



İSTANBUL MEDENİYET ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
BİLİM TARİHİ VE FELSEFESİ ANABİLİM DALI

**On Üçüncü ve On Dördüncü Yüzyıllarda İslam
Medeniyetinde Şifreleme Yöntemleri**

Yüksek Lisans Tezi

Afra Akyol

Haziran 2023



İSTANBUL MEDENİYET ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
BİLİM TARİHİ VE FELSEFESİ ANABİLİM DALI

**On Üçüncü ve On Dördüncü Yüzyıllarda İslam
Medeniyetinde Şifreleme Yöntemleri**

Yüksek Lisans Tezi

Afra Akyol

Danışman

Dr. Öğr. Üyesi Taha Yasin Arslan

Haziran 2023

TEZ JÜRİSİ ONAYI

Afra AKYOL tarafından hazırlanan "On Üçüncü ve On Dördüncü Yüzyıllarda İslam Medeniyetinde Şifreleme Yöntemleri" başlıklı bu yüksek lisans tezi, Bilim Tarihi ve Felsefesi Anabilim Dalı'nda hazırlanmış ve jürimiz tarafından kabul edilmiştir.

JÜRİ ÜYELERİ

İMZA

Tez Danışmanı:

Unvanı Adı Soyadı: Dr. Öğr. Üyesi Taha Yasin Arslan

Kurumu: İstanbul Medeniyet Üniversitesi

Üyeler:

Unvanı Adı Soyadı: Prof. Dr. Tuncay Zorlu

Kurumu: İstanbul Teknik Üniversitesi

Unvanı Adı Soyadı: Dr. Öğr. Üyesi Zeynep Tuba Oğuz Ceyhan

Kurumu: İstanbul Medeniyet Üniversitesi

Tez Savunma Tarihi: 27/07/2023

BEYANLAR

Yazım ve Kaynak Gösterme Kılavuzu Beyanı

Danışmanlığımda yazılan bu tezin APA yazım ve kaynak gösterme kılavuzunda belirtilen kurallara uygun olarak yapılandırıldığı ve bu kılavuzun metin içi kaynak gösterme standartlarının bu tezde tutarlı olarak uygulandığı tarafımdan incelenerek teyit edilmiştir.

İmza

Dr. Öğr. Üyesi Taha Yasin Arslan

Etik İlkeler Sadakat Beyanı

Hazırladığım bu tezin tamamen kendi çalışmam olduğunu, akademik ve etik kuralları gözeterek çalıştığımı ve her alıntıya kaynak gösterdiğimi beyan ederim.

Afra Akyol

ÖNSÖZ

Bu çalışma, on üçüncü ve on dördüncü yüzyıllarda İslam medeniyetinde yazılmış kriptoloji eserleri kapsamında ele alınan şifreleme yöntemlerini konu almaktadır. Bu dönemde kullanılan şifreleme yöntemleri, bir sınıflandırma dahilinde Arapça ve Türkçe olarak örneklendirilerek kriptoloji tarihi alanındaki çalışmalara bir katkı sunmayı açıklamaktadır.

Danışmanım Dr. Öğr. Üyesi Taha Yasin Arslan ile tez konusu olarak kriptoloji çalışmak istediğimizde, konu ile ilgili yaptığımız araştırmamız sonucu Şam Arap Dili Akademisi'nden Muhammed Mrayati, Yahya Meer Alam ve Muhammed Hasan At-Tayyan tarafından hazırlanan “Arabic Origins of Cryptology” isimli altı ciltlik kitap serisine ulaştık. İlk olarak 1987 senesinde *‘ilm el-te’miye ve istihrāc el-mu‘ammā ‘ind el-‘Arab* ismi ile Arapça olarak yayımlanan bu seri, İstanbul Süleymaniye Yazma Eserler Kütüphanesi başta olmak üzere dünya üzerindeki farklı kütüphanelerde bulunan 15 adet kriptoloji konulu el yazmasını içermektedir. 2002 senesi itibarıyla İngilizceye tercüme edilmeye başlanan ve esasen M. Mrayati ve ekibi tarafından dokuz cilt olarak yayımlanması planlanan bu serinin, henüz altı cildi yayımlanmıştır. İngilizce olarak yayımlanan serinin her bir cildi, keşfedilen el yazmalarının tahlili, İngilizce tercümeleri ve dizgileri olmak üzere üç bölümden oluşmaktadır. Birinci ciltte, bahsi geçen bölümlere ek olarak kriptolojinin İslam medeniyetindeki genel gelişimi de ele alınmıştır.

Bu serinin ikinci, üçüncü ve dördüncü cildini oluşturan İbn ‘Adlān, İbn Duneynır ve İbnu’d-Dureyhim isimli müelliflerin çalışmaları, serinin diğer ciltlerini oluşturan müelliflerin çalışmalarını da kapsayıcı ve üzerine ekleyici özellikte olduğundan çalışmamız 13. ve 14. yüzyıllarda İslam medeniyeti üzerine yoğunlaşarak hazırlanmıştır. Bununla birlikte çalışmamızda sadece düz yazıda kullanılan şifreleme yöntemleri ele alınmış olup şiirsel şifreleme yöntemleri şiirin yapısal ve dilbilimsel konularını gerektirdiğinden bu çalışmanın dışında bırakılmıştır.

Çalışmamızın başında İslam medeniyetinde yazılmış eserleri orijinal metninden çalışmak istemekle birlikte Arapça bilginimizin bu eserleri okuyup anlayabilecek düzeyde yeterli olmamasından dolayı bahsi geçen altı ciltlik eserdeki İngilizce tercümelemlerle çalışmamıza başladık. Süreç içerisinde Arapça bilginimizi ilerletmiş olmakla birlikte konunun gidişatı

zaten belirlenmiř olduđu iin bu alıřmamız eserlerin tercümeleri ile tamamlanmıřtır. Bununla beraber ileri düzey Arapa gramer bilgisinin gerektiđi yöntemlerin örneklendirilmeleri profesyonel yardım alınarak hazırlanmıřtır.

Bu vesile ile yüksek lisans eđitimimin bařından tez yazım sürecinin sonuna kadar ilgi ve desteđini esirgemeyen, tecrübelerini paylařmaya her daim hazır olan, biz öđrencilerine rahat soru sorma imkânı sađlayan ve daha ileriye hedeflememiz iin bizleri yüreklendiren danıřmanım Dr. öđr. Üyesi Taha Yasin Arslan’a tüm yardımları iin ok teřekkür ederim. Bu süre zarfında derslerinden olduka istifade ettiđim, bilim tarihine daha geniř bir perspektiften bakmamı sađlayan Prof. Dr. İhsan Fazlıođlu’na ve derslerine katılma isteklerimi nezaketle kabul eden İstanbul Medeniyet Üniversitesi Bilim Tarihi ve Felsefesi Anabilim dalında hocalarıma da teřekkürü bor bilirim.

ÖZET

On Üçüncü ve On Dördüncü Yüzyıllarda İslam Medeniyetinde Şifreleme Yöntemleri

Akyol, Afra

Yüksek Lisans Tezi, Bilim Tarihi ve Felsefesi Anabilim Dalı

Danışman: Dr. Öğr. Üyesi Taha Yasin Arslan

Haziran 2023, 199 Sayfa

Bu çalışmanın amacı, bugün günlük yaşamımızın bir parçası haline gelen kriptolojinin arka planını 13. ve 14 yüzyıllarda İslam medeniyetinde kullanılan şifreleme yöntemleri bağlamında incelemektedir. Bu dönemde kullanılan yöntemlerin bir sınıflandırması sunulurarak Arapça ve Türkçe olmak üzere iki dilde hazırlanan örnekler ile daha anlaşılır kılınması amaçlanmıştır.

Geçmişten günümüze kadar gelen süreçte bir mesajın, istenmeyen kişiler tarafından okunma ihtimaline karşı gizliliğinin güvence altına alınması, çok çeşitli girişimlerle mümkün kılınmaya çalışılmıştır. Amaç, gizliliği mümkün olan en yüksek seviyede sağlamak olsa da kimi zaman mesajın okunmasını çok kısa bir süre geciktirmek bile oluşabilecek muhtemel zararları engelleyebilecek bir öneme sahip olmuştur. Tüm bu girişimler çeşitli şifreleme yöntemlerinin geliştirilmesinin ve buna bağlı olarak şifreli metnin ele geçirilip mesajın içeriğini anlamaya yönelik çalışmaların yolunu açmıştır.

Bilindiği kadarı ile ilk olarak Kindî tarafından *Risāle fî istihrāc el-mu‘ammā* isimli eserde sistematik bir şekilde ele alınan şifreleme ve şifre çözümleme yöntemleri, bu alanda yapılan diğer çalışmalarla birlikte geliştirilerek bir disiplin haline gelmiştir. Bugün kriptoloji olarak adlandırdığımız bu bilim alanı, içinde yaşadığımız dünya için bir tür modern silahlanma yöntemi olarak kabul edilmektedir.

Anahtar Kelimeler: Kriptoloji, İslam medeniyetinde şifreleme yöntemleri, İbn ‘Adlān, İbn Duneynīr, İbnu’l-Dureyhim

ABSTRACT

Encryption Methods in the 13th-14th Century Islamic World

Akyol, Afra

Master's Thesis, Department of the History of Science and Philosophy

Supervisor: Assistant Professor Dr. Taha Yasin Arslan

July 2023, 199 Pages

The aim of this study is to analyse the background of cryptology becoming a part of our daily life in the context of encryption methods used in the Islamic world in the 13th and 14th centuries. In Arabic and Turkish, by presenting the methods used in this period within a classification and by providing examples of both languages, it is aimed to make them more comprehensible.

Since the past until now, a great variety of initiatives have been done to keep the confidentiality of a message secure against the possibility of being read by unauthorised people. Although the aim was to ensure the highest possible level of confidentiality, time to time postponing the reading of the message even for a very short period, gained importance to avoid possible damages that may occur. All these initiatives promoted the improvement of various encryption methods and correspondingly the efforts to attain the ciphertext to decipher it. As much as it is known, the methods of encryption and decipherment addressed systematically by Kindî in the work named *Risāle fî istihrāc el-mu‘ammā* have become a discipline by means of the improvements done in this field. This science currently named cryptology is regarded as a form of modern armament method for the world we live in.

Keywords: Cryptology, encryption methods in the Islamic world, Ibn ‘Adlān, Ibn Dunaynīr, Ibn al-Durayhim

İÇİNDEKİLER

İÇİNDEKİLER.....	v
TABLolar LİSTESİ	xi
RESİMLER LİSTESİ	xiii
ŞEKİLLER LİSTESİ	xiii
KISALTMALAR	xiv
GİRİŞ.....	1
BÖLÜM I ON ÜÇÜNCÜ YÜZYILA KADAR İSLAM MEDENİYETİNDE KRİPTOLOJİNİN GELİŞİMİ	5
1.1. DOKUZUNCU YÜZYILA KADAR KRİPTOLOJİNİN GELİŞİMİ.....	5
1.2. DOKUZUNCU VE ON İKİNCİ YÜZYILLAR ARASINDA İSLAM MEDENİYETİNDE KRİPTOLOJİNİN GELİŞİMİ	9
1.2.1. İslam Medeniyetinde Kriptolojinin Gelişimini Sağlayan Faktörler	10
1.2.1.1. Tercüme Hareketleri	10
1.2.1.2. Dil Bilim Çalışmaları.....	12
1.2.1.3. Matematik Çalışmaları.....	14
1.2.1.4. Yönetim Faaliyetleri	16
1.2.2. Kriptolojide Öne Çıkan İsimler	16
1.2.2.1. Kindî	16
1.2.2.1.1. Kriptoloji Eseri	19
1.2.2.2. İbn Vehb	23
1.2.2.2.1. Eseri	23
1.2.2.3. A ve B'nin Yazarı	27
1.2.2.3.1. Eseri	27
2. BÖLÜM II	32

ON ÜÇ VE ON DÖRDÜNCÜ YÜZYILLARDA İSLAM MEDENİYETİNDE KRİPTOLOJİNİN GELİŞİMİ.....	32
2.1. ON ÜÇ VE ON DÖRDÜNCÜ YÜZYILLARDA İSLAM MEDENİYETİNİN GENEL DURUMU.....	32
2.2. KRİPTOLOJİDE ÖNE ÇIKAN İSİMLER	34
2.2.1. İbn ‘Adlān	34
2.2.1.1. Eseri	35
2.2.2. İbn Duneynīr	40
2.2.2.1. Eseri	41
2.2.3. İbnu’-d-Dureyhim	47
2.2.3.1. Eseri	48
3. BÖLÜM III.....	58
ON ÜÇÜNCÜ VE ON DÖRDÜNCÜ YÜZYILLARDA İSLAM MEDENİYETİNDE KULLANILAN ŞİFRELEME YÖNTEMLERİ	58
3.1. YÖNTEMLERİN AÇIKLAMALARI	58
3.1.1. Anlamın Gizlenmesine Dayalı Şifreleme Yöntemleri	58
3.1.1.1. Yerine Koyma Yöntemi.....	58
3.1.1.1.1. Harf Konulması	58
3.1.1.1.2. Sembol Konulması.....	62
3.1.1.1.3. Sayı Konulması.....	67
3.1.1.1.4. Kelime Konulması	68
3.1.1.1.5. Dallı Harf Konulması	68
3.1.1.1.6. Sembolik Resim Konulması	69
3.1.1.2. Yer Değiştirme Yöntemi.....	69
3.1.1.2.1. Harflerin Çevresindeki Harflere Göre Yerlerinin Değiştirilmesi	69
3.1.1.2.2. Harflerin Kendi Pozisyonuna Göre Değiştirilmesi.....	70

3.1.1.3.	Ekleme ve Çıkarma Yöntemi.....	71
3.1.1.3.1.	Fazladan Harf ya da Sembollerin Eklenmesi.....	71
3.1.1.3.2.	Harflerin Tekrarlanması.....	72
3.1.1.3.3.	Harf Çıkarılması	72
3.1.1.4.	Birleştirme ve Ayırma Yöntemi	73
3.1.1.4.1.	Ayrı Yazılan Harflerin Birleştirilmesi	73
3.1.1.4.2.	Birleşik Yazılan Harflerin Ayrılması.....	74
3.1.2.	Şifrenin Gizlenmesine Dayalı Şifreleme Yöntemleri	74
3.1.2.1.	Kurgulayarak Şifreleme	74
3.1.2.1.1.	Harflerin Bir Kategori ile İlişkilendirilmesine Dayalı Yöntemler	74
3.1.2.1.2.	Harflerin Sayısal Değerlerinin Kullanılarak Bir Metnin İçerisine Yerleştirilmesi.....	78
3.1.2.1.3.	Mesajların Başka Bir Bağlam İçerisine Yerleştirilmesine Dayalı Yöntemler	78
3.1.2.1.4.	Harflerin Sayısal Değerlerine Denk Yeni Kelimeler Üretilmesi .	80
3.1.2.2.	Bir Araç Kullanarak Gizleme	80
3.1.2.2.1.	Parmak İşaretleri ile Şifreleme	80
3.1.2.2.2.	Katlanmış Kâğıt ile Şifreleme	81
3.1.2.2.3.	Satranç Tahtası ile Şifreleme	82
3.1.2.2.4.	Delikli Tahta ile Şifreleme.....	82
3.1.2.2.5.	Renkli Boncuklar ile Şifreleme	83
3.2.	YÖNTEMLERİN ARAPÇA ÖRNEKLERİ	83
3.2.1.	Anlamanın Gizlenmesine Dayalı Şifreleme Örnekleri	84
3.2.1.1.	Harf ile Yerine Koyma Örnekleri	84
		89
3.2.1.2.	Sembol ile Yerine Koyma Örnekleri	92

3.2.1.3.	Sayı ile Yerine Koyma Örnekleri	95
3.2.1.4.	Kelime ile Yerine Koyma Örnekleri.....	97
		99
3.2.1.5.	Dallı Alfabe ile Yerine Koyma Örneği.....	100
		101
3.2.1.6.	Sembolik Resimler ile Yerine Koyma Örneği	102
3.2.1.7.	Harflerin Çevresindeki Harflere Göre Yer Değiştirme Örnekleri	104
3.2.1.8.	Harflerin Kendi Pozisyonuna Göre Yer Değiştirmesi Örneği	108
3.2.1.9.	Fazladan Değer Ekleme Örnekleri.....	108
3.2.1.10.	Harf Tekrarlama Örneği.....	109
3.2.1.11.	Harflerin Çıkarılması Örnekleri.....	109
		111
3.2.1.12.	Ayrı Yazılan Harfleri Birleştirme Örneği	111
3.2.1.13.	Birleşik Yazılan Harfleri Ayırma Örneği	112
3.2.2.	Şifrenin Gizlenmesine Dayalı Şifreleme Örnekleri	112
3.2.2.1.	Bir Kategori ile İlişkilendirme Örnekleri.....	113
		123
		125
		132
3.2.2.2.	Harflerin Sayısal Değerlerinin Bir Metnin İçerisine Yerleştirilmesi Örneği	136
3.2.2.3.	Mesajın Başka Bir Bağlam İçerisine Yerleştirilmesi Örnekleri ...	137
3.2.2.4.	Harflerin Sayısal Değerlerine Denk Yeni Kelimelerin Üretilmesi Örneği	139
		139
3.3.	ARAPÇA ÖRNEKLERİN TÜRKÇEYE UYARLANMASI	139

3.3.1.	Anlamların Gizlenmesi Dayalı Şifreleme Örnekleri.....	140
3.3.1.1.	Harf ile Yerine Koyma Örnekleri	140
		141
3.3.1.2.	Sembol ile Yerine Koyma Örnekleri	148
3.3.1.3.	Sayı ile Yerine Koyma Örnekleri	151
		152
3.3.1.4.	Kelime ile Yerine Koyma Örnekleri.....	152
		155
3.3.1.5.	Dallı Alfabe ile Yerine Koyma Örneđi.....	156
3.3.1.6.	Sembolik Resimler ile Yerine Koyma Örneđi	157
		159
3.3.1.7.	Harflerin Çevresindeki Harflere Göre Yer Deđiştirme Örnekleri	160
3.3.1.8.	Harflerin Kendi Pozisyonuna Göre Yer Deđiştirmesi Örneđi	164
3.3.1.9.	Fazladan Deđer Ekleme Örnekleri.....	165
3.3.1.10.	Harf Tekrarlama Örneđi.....	166
3.3.1.11.	Harflerin Çıkarması Örnekleri	166
3.3.1.12.	Ayrı Yazılan Harfleri Birleştirmeye Örneđi	168
3.3.2.	Şifrenin Gizlenmesine Dayalı Şifreleme Örnekleri	169
3.3.2.1.	Bir Kategori ile İlişkilendirme Örnekleri.....	169
		170
		176
		181
		184
3.3.2.2.	Harflerin Sayısal Deđerlerinin Bir Metin İçerisine Yerleştirilmesi Örneđi	186
3.3.2.3.	Mesajın Başka Bir Bağlam İçerisine Yerleştirilmesi Örnekleri ...	187

3.3.2.4.	Harflerin Sayısal Değerlerine Denk Yeni Kelimelerin Üretilmesi	
Örneği	188	

SONUÇ	190
--------------------	------------

KAYNAKÇA.....	194
----------------------	------------

TABLÖLAR LİSTESİ

Tablo 1: İbn ‘Adlân’a Göre Harflerin Bulunma Sıklıklarının Gruplandırılması	36
Tablo 2: Arap Harflerinin Ebced Sistemindeki Sayısal Karşılıkları.....	60
Tablo 3: Arapçada Harflerin Bulunma Sıklığı Yüzdeleri	64
Tablo 4: Düzenli Bir Kurala Bağlı Olarak Arap Harflerini Eşleştirme	85
Tablo 5: Düzenli Bir Kurala Bağlı Olmayarak Arap Harflerini Eşleştirme	86
Tablo 6: Arap Harflerinin Sayısal Değerlerinin Tekrar Harflere Dönüştürülmesi ...	87
Tablo 7: Arap Harflerinin Sayısal Değerlerinin Değiştirilerek Tekrar Harflere Dönüştürülmesi	89
Tablo 8: Arap Harflerinin Düz ve Ters Okunuşları	91
Tablo 9: Arap Harflerinin Semboller ile Temsil Edilmesi.....	93
Tablo 10: Arap Dilinde Sıklıkla Birlikte Kullanılan Bazı Harfler ve Örnekte Temsil Edildikleri Semboller	94
Tablo 11: Arap Harflerinin Ebced Sistemindeki Sayısal Değerleri.....	95
Tablo 12: Arap Harflerinin Rastgele Sayısal Değerler ile Temsil Edilmesi.....	96
Tablo 13: Arap Harflerinin Ebced Sistemindeki Sayısal Değerlerinin Okunuşları ..	97
Tablo 14: Arap Harflerinin Kuş İsimleri ile Temsil Edilmesi	99
Tablo 15: Arap Harflerinin Dallı Alfabenin Harfleri ile Temsil Edilmesi	101
Tablo 16: Arap Harflerinin Meyve ve Sebze Emojileri ile Temsil Edilmesi.....	103
Tablo 17: Yazılışları Benzer olan Arap harflerinin ortak bir harf ile temsil edilmesi	110
Tablo 18: Bazı Arap Harflerinin Ortak Bir Harf Tarafından Temsil Edilmesi.....	111
Tablo 19: Arap Harflerine Karşılık Gelen Kategori İsimleri	114
Tablo 20: Bir Kısıtlamaya Bağlı Kalmadan Yapılan Şifrelemede Kullanılan Kelimeler	115
Tablo 21: Bir Kısıtlamaya Bağlı Kalarak Yapılan Şifrelemede Kullanılan Kelimeler	117
Tablo 22: Normal Alfabe Dizilişine Göre Kullanılan Kelimeler.....	119
Tablo 23: Sayısal Alfabe Dizilişine Göre Kullanılan Kelimeler	121
Tablo 24: Arap Harflerinin Arazi Ölçü Birimleri ile Temsil Edilmesi.....	123
Tablo 25: Arap Harflerinin Dinar Para Birimi ile Temsil Edilmesi	125
Tablo 26: Arap Harflerinin Haftanın Gün ve Saatleri ile Temsil Edilmesi	129

Tablo 27: Arap Harflerinin Kitap İsimleri ile Temsil Edilmesi.....	132
Tablo 28: "علي" Mesajındaki Harflerin Sayısal Değerlerine Karşılık Kelime Üretme	139
Tablo 29: Türk Alfabesindeki Harflere Farazi Olarak Atanan Sayısal Değerler....	140
Tablo 30: Düzenli Bir Kurala Bağlı Olarak Türk Alfabesindeki Harflerini Eşleştirme	141
Tablo 31: Düzenli Bir Kurala Bağlı Olmayarak Türk Alfabesindeki Harflerini Eşleştirme.....	141
Tablo 32: Türk Alfabesindeki Harflerin Sayısal Değerlerinin Tekrar Harflere Dönüştürülmesi	143
Tablo 33: Türk Alfabesindeki Harflerin Sayısal Değerlerinin Değiştirilerek Tekrar Harflere Dönüştürülmesi.....	145
Tablo 34: Türk Alfabesindeki Harflerin Düz ve Ters Okunuşları	147
Tablo 35: Türk Alfabesindeki Harflerin Semboller ile Temsil Edilmesi.....	149
Tablo 36: Türk Alfabesindeki Harflerin Rastgele Sayısal Değerler ile Temsil Edilmesi	152
Tablo 37: Türk Alfabesindeki Harflere Atanan Sayısal Değerlerin Okunuşları.....	153
Tablo 38: Türk Alfabesindeki Harflerin Kuş İsimleri ile Temsil Edilmesi	155
Tablo 39: Türk Alfabesindeki Harflerin Dallı Alfabe ile Temsil Edilmesi	157
Tablo 40: Türk Alfabesindeki Harflerin Meyve ve Sebze Emojileri ile Temsil Edilmesi	159
Tablo 41: Yazılışları Benzer Olan Türk Alfabesindeki Harflerin Ortak Bir Harf ile Temsil Edilmesi	167
Tablo 42: Türk Alfabesindeki Bazı Harflerin Ortak Bir Harf Tarafından Temsil Edilmesi	168
Tablo 43: Türk Alfabesinin Harflerine Karşılık Gelen Kategori İsimleri	170
Tablo 44: Bir Kısıtlamaya Bağlı Kalmadan Yapılan Şifrelemede Kullanılan Kelimeler	171
Tablo 45: Bir Kısıtlamaya Bağlı Kalarak Yapılan Şifrelemede Kullanılan Kelimeler	173
Tablo 46: Normal Alfabe Dizilişine Göre Kullanılan Kelimeler.....	174
Tablo 47: Sayısal Alfabe Dizilişine Göre Kullanılan Kelimeler	176
Tablo 48: Türk Alfabesindeki Harflerin Arazi Ölçü Birimleri ile Temsil Edilmesi	177
Tablo 49: Türk Alfabesindeki Harflerin Para Birimi ile Temsil Edilmesi	179

Tablo 50: Türk Alfabesindeki Harflerin Haftanın Gün ve Saatleri ile Temsil Edilmesi	181
Tablo 51: Harflerinin Kitap İsimleri ile Temsil Edilmesi.....	184
Tablo 52: “Üç” Mesajındaki Harflerin Sayısal Değerlerine Karşılık Kelime Üretme	189

RESİMLER LİSTESİ

Resim 1: Kindî'nin Risāle fî istihrāc el-mu‘ammā isimli risalesinde yapmış olduğu şifreleme yöntemleri sınıflandırması	21
Resim 2: İbnu'd-Dureyhim'in Miftāh el-Kunūz fî idāh el-marmūz isimli risalesindeki dallı harf şekilleri	54
Resim 3: İbnu'd-Dureyhim'in Miftāh el-Kunūz fî idāh el-marmūz isimli risalesinde vermiş olduğu şifreli metin örneği.....	56
Resim 4: Ayrı Yazılan Harflerin Birleşik Yazılması	112
Resim 5: Ayrı Yazılan Harflerin Birleştirilmesi	169

ŞEKİLLER LİSTESİ

Şekil 1: Kriptolojinin İki Temel Alt Dalı	1
Şekil 2: Kriptolojinin Temel Çalışma Prensipleri	2
Şekil 3: Şifreleme Yöntemlerinin Sınıflandırılması	57

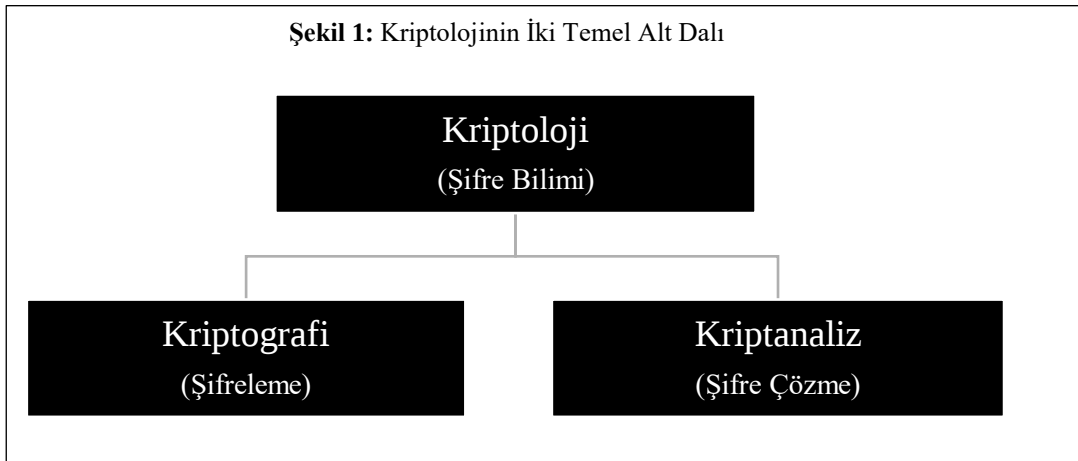
KISALTMALAR

A ve B'nin yazarı.:	A ve B risalelerinin yazarı
Bkz.:	Bakınız
M.Ö.:	Milattan Önce
M.S.:	Milattan Sonra
Ö.:	Ölüm / Vefat
s.:	Sayfa
vr.:	Varak numarası

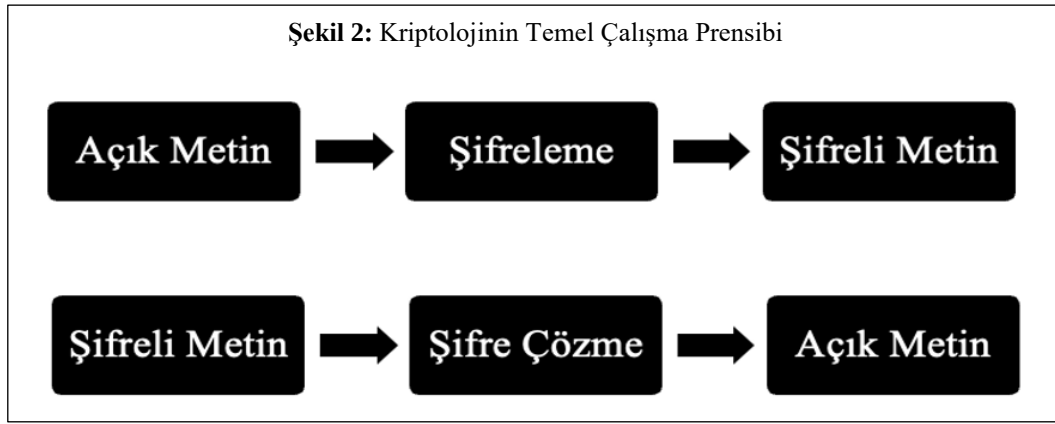
GİRİŞ

Her insan, başkalarınca öğrenilmesini istemediği birtakım bilgilere sahiptir. Bu bilgileri yalnızca istediği kişilerle paylaşma isteği ya da ihtiyacı, insan doğasının temel özelliklerinden biri olarak görülebilir. Başka bir ifade ile üç veya daha fazla kişinin bir arada bulunması durumunda, bir bilginin sadece istenilen kişilerle paylaşılacak istenmesi, doğal bir durum olarak görülmekte ve bu durum da gizli paylaşımı doğurmaktadır. Bu şekildeki paylaşım, istenmeyen kişiler tarafından duyulmayacak bir ortamda yapılabileceği gibi böyle bir ortamın mümkün olmadığı şartlarda, istenmeyen kişilerden gizlenerek de yapılabilir. Bununla birlikte gizli bir paylaşımın, insanın sahip olduğu güçlü merak duygusundan ötürü istenmeyen kişiler tarafından öğrenilmek istenmesi de anlaşılabilir bir durum olarak görülebilmektedir. Bu bağlamda gizli mesajlaşmanın ve bu mesajların içeriğini elde etme teşebbüsleri, kriptoloji olarak adlandırılmakta ve insanlığın başlangıcına kadar götürülebilmektedir. Burada sözü edilen kriptolojinin sözlü kriptoloji geleneği olarak düşünülmesi gerektiği de unutulmamalıdır.

Kriptoloji ya da şifre bilimi, Yunanca gizli, saklı anlamına gelen *kryptos* ile bilim anlamına gelen *logos* kelimelerinin birleşiminden oluşmaktadır. Bir taraftan, bilginin yalnızca istenilen kişilere iletilmesini, bu kişilerce saklanmasını ve bu bilginin istenmeyen kişilerin eline geçmesi ihtimaline karşı anlaşılmasını engellemeyi amaçlayan kriptoloji, diğer taraftan anlaşılmaz halde elde edilen bilginin anlaşılmasını sağlayan çözümlemeyi amaçlamaktadır. Bu durum bilgide hak sahibi olan kişileri korumakla birlikte haksızca ya da herhangi bir sebeple bilgiye ulaşmaya çalışan kişilerin de bilgiye ulaşımına imkân vermektedir. Buradan yola çıkarak kriptolojinin, kriptografi ve kriptanaliz olarak adlandırılan iki ayrı uç alandan oluştuğunu söyleyebiliriz.



Kriptografi köken itibariyle *kryptos* ve yazmak anlamına gelen Yunanca *graphein* kelimelerinden türetilmiştir. Şifreleme bilimi olarak da adlandırılan kriptografi, açık bir metni istenmeyen kişiler tarafından anlaşılmayacak bir hale dönüştürme işlemine denir. Gizlilik, erişilebilirlik ve bütünlük gibi bilgi güvenliği konularını sağlamak için kullanılan yöntemleri kapsamaktadır. Bu yöntemler bilginin istenmeyen kişiler tarafından anlaşılmasını önleyerek gönderici ve alıcısını korumayı amaçlamaktadır (Akleyek, Akyıldız ve Çimen, 2012: 8). Kriptanaliz ya da şifre çözme ise ele geçirilen şifreli yani anlamsız bir metinden açık metni (şifresiz metni) elde etme yöntemlerine denilmektedir. Unutulmamalıdır ki şifrelerin çözülmesi için şifrelerin nasıl tasarlandığının da iyi derecede bilinmesi gerekmektedir dolayısıyla şifre çözümlemede başarılı olma yolunun şifreleme yöntemlerine hâkim olmaktan geçtiği söylenebilir (Akleyek ve diğerleri, 2012: 8).



Sözlü kriptoloji tarihi insanlık tarihi ile başlatılabilirken kayıtlı kriptoloji tarihi, kesin delil bulmanın diğer bilimlere nazaran daha zorlayıcı olabileceği göz önünde bulundurularak, M.Ö. yaklaşık 1900 yılında yaşayan bir kâtibin efendisinin hayatını anlatması ile başlatılmaktadır. Bununla birlikte şifre ve kodların kullanımı, iki bin yıldan fazla bir süredir siyasetten savaşımlara, toplum yapısından bilimsel gelişmelere kadar birçok alanda etkin bir şekilde kullanılmakta hatta kimi zaman sonucu belirleyen bir rol oynamaktadır. Gizli bir şekilde iletilen mesajlar vesilesiyle savaşlar kazanılmış ya da kaybedilmiş, imparatorluklar kurulmuş ya da yıkılmış, insanların hayatları kurtulmuş ya da son bulmuştur. Bu kadar ciddi sonuçlar doğurması, şifre yazıcılar ve şifre çözümleyiciler arasında sonu gelmeyen bir mücadelenin var olmasına neden olmuştur (Frery ve Pincock, 2021:8). Bu çekişmeyi “entelektüel silahlanma yarışı” olarak tanımlayan Simon Singh,

şifreyi yazan ve çözümleyen kişiler arasındaki ilişkiyi tıpkı bir bakteri ile antibiyotik arasındaki ilişkiye benzetmektedir. Bir bakteri kendisindeki bir zayıflığın tespit edilip ona uygun bir antibiyotik geliştirilene kadar hayatını sürdürebilmekte ve ancak evrim geçirip antibiyotiğe karşı direnç kazanırsa tekrar çoğalabilmektedir. Bakteriler gibi şifrelerin de zayıf bir yönünün tespit edilmesi o şifre için öldürücü bir silah geliştirmek anlamına gelmektedir. Bunun nedeni işlevselliğini kaybeden bir şifrenin artık ölü bir şifre konumuna geçecek olmasıdır. Hazırlandığı andan itibaren kendisini çözümlemeye çalışan herkesin saldırısı altında olan şifreler, sürekli olarak evrim geçirip zayıf taraflarını güçlendirmek zorundadırlar (Singh, 2002: 2). Bu anlamda tarih boyunca yapılan ve günümüzde hala geliştirilerek devam eden pek çok teşebbüs bulunmaktadır. Yaklaşık 4000 yıl önce başlayan bu süreç günümüz teknolojisinde cep telefonları, internet siteleri, banka işlemleri ve silah sistemleri gibi önemli bilginin olduğu her yerde kullanılır hale gelmiştir. Bugün elektronik sistemlerin doğru kişiyi tanınması, kriptoloji sayesinde mümkün olabilmektedir.

Bu çalışma, kriptolojinin bugüne gelen olgunluğunun yüzyıllara dayanan arka planını daha iyi anlamak ve bu süreçte İslam medeniyetinde yapılmış katkıları ele almak amacıyla yapılmıştır. Bununla birlikte dönem olarak 13. ve 14. yüzyıllara odaklanılarak mevcut birikimin bu dönem içerisinde ne şekilde devam ettiği sorusuna cevap aranmak istenmiştir.

Tezimiz, giriş ve sonuç bölümü hariç üç ana bölümden oluşmaktadır. Birinci bölümde, kayıtlı kriptolojinin doğuşundan dokuzuncu yüzyıl İslam medeniyetine kadar gelen kriptoloji bilgisinden ve kullanımından bahsedilmiştir. İslam medeniyetinde 9. yüzyıl ile başlayan kriptoloji geleneğinin 13. yüzyıla kadar olan gelişimi de bu bölümde ele alınmıştır. Bu bağlamda, İslam dünyasında kriptolojinin gelişmesini teşvik eden unsurlar hakkında bilgi verildikten sonra oluşan kriptoloji geleneğinin kökenine dair bilgi edinmek ve bu gelişimin nasıl ilerlediğini görmek amacıyla bu döneme ait üç şifre bilimcisinin ve eserlerinin tanıtımı yapılmıştır. İlk olarak, bilindiği kadarıyla yazılan ilk kriptoloji kitabı olma özelliği taşıması ve konuya ait özgün bilgiler içermesi bakımından büyük önem taşıyan Kindî'nin *Risāle fî istihrāc el-mu'ammā* isimli eserinin incelemesi yapılmıştır. İkinci olarak, İbn Vehb tarafından ele alınan *el-Burhān fî Vucūhi'l-Beyān* isimli eserin ve üçüncü olarak bilinmeyen bir müellif tarafından yazılan iki ayrı risalenin tanıtımına yer

verilmiştir. Bu iki risale, içerdği şifreleme yöntemlerinin yanı sıra bu bilimle uğraşan kişilere verilen tavsiyelerle de dikkat çekmektedir.

Tezin ikinci bölümü, kriptolojinin 13. ve 14. yüzyıllarda İslam medeniyetindeki gelişimini ele almaktadır. 13. ve 14. yüzyıllarda İslam medeniyetinin genel durumu hakkında kısa bir bilgi verdikten sonra bu dönemde yaşamış, üç şifre bilimci İbn ‘Adlān, İbn Duneynīr ve İbnu’d-Dureyhim tanıtılmış ve konu ile ilgili yazdıkları eserlerin incelemeleri yapılmıştır. Bu eserler, bir önceki dönemin mevcut kriptoloji geleneğini devam ettirmesi ve eklenen yeni özelliklerle birlikte kullanılan yöntemlerin nasıl geliştirildiğini göstermesi açısından önem taşımaktadır.

Tezin üçüncü bölümünün amacı, 13. ve 14. yüzyıllarda İslam medeniyetinde kullanılan şifreleme yöntemleri için bir sınıflandırma sunmaktır. Bu sınıflandırma, en temelde “anlamın gizlenmesi” ve “şifrenin gizlenmesi” ayrımı gözetilerek hazırlanmış olup yöntemlerin açıklama ve örneklerine de yer verilmiştir. Örnekler, orijinaline yakın olması amacıyla ilk olarak Arapça ve daha iyi anlaşılması için Türkçeye uyarlanması şeklinde iki ayrı dilde hazırlanmıştır.

Çalışmamızda ana kaynak olarak, Muhammed Mrayati, Yahya Meer Alam ve Muhammed Hasan At-Tayyan tarafından hazırlanan ve KFCRIS & KACST tarafından yayımlanan “Arabic Origins of Cryptology” isimli kitap serisinin 1. 2. 3. 4. ve 6. ciltleri kullanılmıştır. Bununla birlikte David Kahn’ın “The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet” isimli eseri, kriptolojinin tarihsel gelişimi hakkında sunmuş olduğu bilgilerle teze katkı sağlamıştır.

BÖLÜM I ON ÜÇÜNCÜ YÜZYILA KADAR İSLAM MEDENİYETİNDE KRİPTOLOJİNİN GELİŞİMİ

1.1. DOKUZUNCU YÜZYILA KADAR KRİPTOLOJİNİN GELİŞİMİ

Kayıtlı kriptoloji tarihi, yaklaşık 4000 yıl önce Nil nehrinin kıyısında bulunan Menet Khufu adlı küçük bir kasabada yaşayan bir kâtibin, efendisinin hayatını anlattığı hiyerogliflerle başlatılmaktadır. Bu hiyeroglifler modern dünyanın bildiği şekilde gizli bir yazı sistemi olmasa da metnin bazı yerlerinde alışılmışın dışında sembol kullanımı, kriptolojinin temel unsurlarından biri olan yazının kasıtlı bir şekilde dönüştürülmesini içermesinden dolayı önemlidir. Buradaki amacın kelimelerin gerçek anlamlarını gizlemekten ziyade yazıta bir itibar kazandırmak, gizemini artırmak ve daha önemlisi Mısırlıların yoldan geçenlere bu yazıtları okutarak orada yatan ölülerine bu kutsamaları bahşetmek olduğu düşünülmektedir (Kahn, 1973: 64-65).

Öteki dünya üzerine yoğunlaşan Mısır güçlendikçe, saygı duyulan kişilerin mezarlarını ve buna bağlı olarak bu mezar yazıtlarında kullanılan farklı sembol ve dönüşümleri artırmıştır. Ancak bu tür yazıtların sayısı çoğaldıkça ziyaretçilerin ilgileri de zamanla azalmıştır. Bu ilgiyi tekrar canlandırmak isteyen Mısırlılar, ziyaretçileri meraklandırmak ve yazıtları okumaya teşvik etmek için bu yazıtları kasıtlı olarak anlaşılmasız hale getirmeye başlamışlardır. Buna rağmen bu durum, ziyaretçilerin ilgilerini geri getirmek için etkili olmamış, bu sebeple mezar kriptolojisi bir süre sonra sona ermiştir (Kahn, 1973: 65-66). Burada önemli olan nokta, yazının dönüşümüne artık gizliliğin de eklenerek kriptografinin üretilmesi olmuştur. Fakat buradaki asıl amaç, yazının anlaşılmasını olabildiğince uzun değil, mümkün olan en kısa bir süre için geciktirmek olduğundan bu durum yarı kriptoloji olarak da adlandırılabilir. Buna rağmen bu yazıtlar, bugünkü gelişmiş kriptoloji biliminin doğuşu olarak kabul edilmektedir (Kahn, 1973: 66).

Kriptoloji bilimi, tarihinin ilk üç bin yılında, istikrarlı bir gelişme göstermemiş, birçok yerde bağımsız olarak ortaya çıkmış ancak medeniyetlerin yok olması ile bu girişimler de kaybolmuştur (Kahn, 1973: 66). Büyük ve kadim medeniyetlerden biri olan Çin’de bilindiği kadarıyla kayda değer bir kriptolojik gelişme olmamıştır. Bunun nedeninin, o

dönemde çoğu mesajın ezberlenip sözlü olarak iletilmesinin veya Çin dilinin ideografik¹ yapısının, mevcut şifreleme yöntemlerini işlevsiz hale getirmiş olduğu düşünülmektedir. Ancak kriptografi olmasa da bir steganografi² tekniği olarak, mesajların pirinç kağıtlara yazılıp balmumu ile kaplanarak yutulması ya da vücudun başka bir yerinde gizlenerek iletildiği bilinmektedir (Mollin, 2005: 8). Bununla birlikte mesajın ince bir ipek parçası üzerine yazılıp küçük bir top içerisine sıkıştırılması ve daha sonra bu topun cila ile kaplanıp yutulması da kaynaklarda geçmektedir (Singh, 2001: 10).

Pratikte çok sayıda gizli iletişim biçiminin kullanıldığı tahmin edilen Hint medeniyetinde ise iki katkının öne çıktığı görülmektedir. Birincisi, parmaklar yardımıyla yapılan ve bugün işaret dili olarak bilinen iletişim biçimidir. Parmakların eklem kısımları ile sesli harflerin, diğer kısımları ile sessiz harflerin temsil edildiği bu yöntem, Nirābhāṣa olarak adlandırılmaktadır. İkincisi, şifre çözümlemenin politik amaçlarla kullanımında yazılı tarihte ilk örneğine sahip olmalarıdır. M.Ö. 4. yüzyılın sonunda Kautilya (ö. M.Ö. 293) tarafından devlet olma sanatı üzerine yazılan *Arthaśāstra* isimli kitapta, ticaretlerinde gerekli olan bilgileri elde etmek için çeşitli şifre çözümleme önerilerinden bahsedilmiştir. Kitap, bu önerilerin uygulanabilmesi için herhangi bir yöntem içermese de bu tür yöntemlere ulaşılabileceği mesajını vermesi açısından önemli görülmektedir (Mollin, 2005: 8).

Kriptoloji, kutsal metinlerle de çok ilişkili olmuştur. M.Ö. 500-600 civarında Yahudi katiplerin basit yerine koyma yöntemine dayanan ve “Atbash” olarak adlandırılan bir şifreleme yaptıkları bilinmektedir (Madhekar ve diğerleri, 2015: 28). Bu yöntem, İbrani alfabesindeki ilk harfin son harfle, ikinci harfin sondan ikinci harfle ve bu şekilde devam ederek alfabedeki harflerin yerlerinin değiştirilmesine dayanmaktadır. Atbash şifrelemesi, Eski Ahit’te Yeremya 25:26 ve 51:41 olmak üzere iki yerde kullanılmış, Babil kelimesi “Sheshac”, Kashdim kelimesi ise “leb kamai” olarak şifrelenmiştir. İncil’de tespit edilen şifrelemeler ise Abgad ve Albam olarak adlandırılan iki yöntemdir. Abgad, alfabedeki her harfin yerine kendisinden sonra gelen harfin konulması ile uygulanmakta ve bu yöntemin muskalarda kullanıldığı bilinmektedir (Blake, 2010: 116-117). Albam ise alfabedeki harflerin ikiye ayrılması ve ilk yarıdaki harflerin sırayla

¹ Doğrudan bir şeyi ya da bir fikri temsil eden işaret ya da semboller. Harf değildirler.

² Mesajın varlığının gizlenmesine dayanan steganografi, Yunanca gizli anlamına gelen “steganos” ve yazı anlamına gelen “graphia” kelimelerinden oluşmaktadır. Kriptolojiden farklı olarak mesajın içeriğinin değil, varlığının gizlenmesi amaçlanmaktadır.

kendilerine karşılık gelen ikinci yarıdaki harflerle yer değiştirilmesine dayanmaktadır (Al Cimino, 2017: 23-24). İncil’de kullanılan bu şifreler, uzun metinlerden ziyade belirli kelimelerden oluşmaktadır (Blake, 2010: 116-117).

Öte yandan Akad, Arap, İbrani ve Yunan dili gibi bazı dillerin harflerine çeşitli sayı değerleri verildiği ve harflerin sayı olarak da işlev gördüğü bilinmektedir. Bununla birlikte sayıların, insanların bilmediği düşünce ve güçleri taşıdığına olan inanç, harflerin sayısal değerleri üzerine kurgulama yapılmasının yolunu açmıştır. Bu sisteme dayanan yöntem, Yahudilerde Gematria, Yunanlılarda ise İsosephi adı ile uygulanmaktadır. En eski Gematria örneklerinden birisinin Asur kralı II. Sargon ile ilgili olduğu bilinmektedir (Blake, 2010: 122). Harflere sayı değerlerinin verilmesi, bir kelimeyi oluşturan harf dizisinin sayısal bir yorumunun yapılabileceği ya da sayıların bazı kelimelere delalet edebileceği düşüncesini de doğurmuştur. Böylece aynı sayısal değere sahip kelimeler arasında çeşitli ilişkiler kurulmaya çalışılmıştır. Yahudi bilginler, bu yöntemleri kahinlikle ilgili hesaplarda kullanarak gizli anlamlar bulduklarını iddia etmişlerdir. Özellikle Talmud ve Midraş metinlerinde bu yöntem sıklıkla kullanılmıştır (Ifrah, 2000, s. 252-253).³ M.Ö. 1. yüzyılda ise bugün Irak’taki Uruk kentinde, katiplerin kendi isimlerinin harflerini sayı olarak şifrelediği bilinmektedir (Cawthorne, 2018: 14). Sayılar kullanılarak yapılan başka bir şifreleme yöntemi, Yunan tarihçi Polybius (M.Ö. 120) tarafından tasarlanan, 5x5 bir kareden oluşan yerine koyma şifrelemesidir. Şifreleme yapmak için karenin sütun ve satırları 1’den 5’e kadar numaralandırılmakta ve alfabedeki harfler sırayla bu karelere yazılmaktadır. Böylece her harf, satır ve sütundaki olmak üzere iki rakamla temsil edilmektedir. Şifrenin çözümlenmesi, belirtilen satır ve sütunlardaki kesişen harflerin tespit edilmesi ile yapılmaktadır (Kondo ve Mselle, 2013: 31). Polybius mesajın uzak mesafelere kolaylıkla iletilebilmesi için ise sayıların meşaleler aracılığı ile temsil edilmesini önermiştir. Bu yöntemle örneğin “e” rakamını temsil eden 15 sayısı, sağ elde bir, sol elde 5 meşale tutularak iletilmektedir (Kahn, 1973: 72).

Yunan tarihçi Herodot (M.Ö. 425) *Tarih* adlı eserinde “gizlenmiş yazı” anlamına gelen bazı steganografi tekniklerinden bahsetmiştir. Herodot, bir kölenin saçlarının tıraş edilip mesajın dövme ile kafa derisine yazıldığından ve saçları tekrar uzadığında kölenin mesajın iletilmesi gereken yere gönderildiğinden bahsetmiştir. Herodot’un anlattığı başka bir teknik ise balmumu tabletinin üstündeki mum çıkartılarak içindeki tahtaya mesaj

³ Ayrıntılı bilgi için bkz. Ifrah, 248-262.

yazılması ardından üzerine tekrar mum dökülerek mesajın gizlenmesidir. Böylece tablet yazı yazmak için pürüzsüz bir yüzey olarak görünmekte ve dikkat çekmemektedir (Anderson, Kuhn, & Petitcolas, 1999, s. 3).

Kriptoloji, askerî alanda ilk olarak Spartalılar tarafından kullanılmıştır. M.Ö. 5. yüzyılda, en eski şifreleme aleti olarak bilinen skytale'i kullandıkları bilinmektedir. Bu aleti kullanmak için öncelikle ince ve uzun bir papirüs ya da parşömen şeridin alınması ve silindir bir sopa etrafına sıkıca sarılması gerekmektedir. İletilecek olan mesaj, sopa üzerine sarılı parşömen ya da papirüs şeridin üzerine yazılarak sopadan çekilmelidir. Daha sonra üzerine bir anlam ifade etmeyen harfler de eklenerek açık halde alıcıya gönderilmelidir. Mesajın okunabilmesi için kâğıdın tekrar daha önce şifreleme yapılırken kullanılan sopa ile aynı ebatlara sahip bir sopaya sarılması gerekmektedir. Bu sayede harfler aynı hizaya denk gelerek mesajın anlamlı bir hal almasını sağlamaktadır (Kahn, 1973: 71-72, Singh, 2001: 12). M.Ö. 404 yılında Pers ülkesinden gelen bir haberci, Spartalı Lysander'e belindeki kemerini vermiş ve sarmalı bu kemere sararak okumasını istemiştir. Bu sayede Lysander (ö. M.Ö. 395), Persli asker ve devlet adamı olan Pharnabazus'un (ö. M.Ö. 387) kendisine bir saldırı planladığını öğrenmiştir. Böylece Lysander savunma için gerekliliği hazırlık yapabilmiş ve saldırıya başarılı bir şekilde karşı koyabilmiştir (Singh, 2001: 12-13). Kuşatmaya karşı, nasıl savunma yapılacağına dair ilk el kitabını yazan Yunan yazar Aeneas Tacitus (M.Ö. 4.yy) ise eserinde, kendisinden önce kullanılanlar ve kendi tasarladıkları dahil olmak üzere toplam yirmi farklı gizli yazışma türüne yer verdiği bilinmektedir (Hulme, 1898: 24). Bunların arasında domuz mesanesine, bacaklara sıvanmış yapraklara, zırh kanadının altına dikilen papirüse, atın dizginlerine, köpek tasmalarına yazı yazılması ve kadınların kâğıttan yapılan, gerçek olmayan küpeler takması ile mesajların iletilmesi şeklinde teknikler bulunmaktadır. Bir yazı aracı olarak mürekkepten de bahseden Tacitus, harflerin görünmez olması için üstüne beyaz bir madde kullanılması gerektiğini belirtmiştir. Mesajın okunması için ise bu beyaz maddenin suya konup silinmesi gerekmektedir (Macrakis, 2014, s. 10-11). Büyük Plinius⁴ da *Naturalis Historia* adlı eserinde süt ve sütleğen cinsi bir bitki sıvısının bu amaçla kullanıldığından bahsetmiştir (Macrakis, 2014, s. 3). Tacitus ayrıca bir yazılı metnin harflerinin altına ya da üstüne küçük delikler açarak mesajların iletilebileceğine de değinmiştir (Mollin, 2005: 9).

⁴ Gaius Plinius Secundus Maior (ö. M.S. 79).

Romalı tarihçi Suetonius, *De Vita Caesarum* adlı eserinde Sezar⁵'ın basit yerine koyma yöntemiyle şifreleme yaptığından bahsetmiştir. Bu yöntemle göre alfabe'deki her harf, o harften sonra gelen üçüncü harfin yerine konur. Sezar, bu şifrelemeyi sadece iç işlerinde değil aynı zamanda *Galya Savaşları* adlı eserinde belirttiği üzere askerî işlerinde de kullanmıştır (Mollin, 2005: 10-11). Sezar muhtemelen, bahsedilen ve bugün “Sezar Şifrelemesi” olarak bilinen bu yöntemin mucidi olmasa da bu şifreleme türü günümüze Sezar ile tanınır hale gelmiştir (Holden, 2017: 2). Eserinde esir halde bulunan Cicero'ya⁶ nasıl mesaj gönderdiğini de anlatan Sezar, Roma harfleri yerine Yunan harflerini koyarak basit yerine koyma yöntemini uyguladığından bahsetmiştir (Singh, 2001: 14).

Kriptoloji, varlığının ilk zamanlarından itibaren bir yönüyle büyü, kehanet, beddua gibi doğa üstü güçlerle ilgili yazıların kritik kısımlarını gizlemeye de hizmet etmiş ve kimi zaman Yahudi kabalasıyla da karıştırılmıştır. Özü itibarıyla her iki sistem de tanınmış olmayan ve görünüşe göre anlamsız olan işaretlerden bir anlam çıkarmaya çalışmaktadır. Kuşların uçuşlarından, yıldız ve gezegenlerin konumlarından, insan elindeki çizgilerden, koyunların iç organlarından, fincandaki posadan ya da şifreli mesajdan bir anlam çıkarma çalışmalarının hepsi bilinmeyen biliniyor kılma teşebbüsleridir. Kriptoloji ve kehanet arasındaki bu yüzeysel benzerlik, insanların zihninde bu bilimin büyücükle ilgili bir okültizm biçimi olduğuna dair bir inancın oluşmasına ve bu bilime karşı mesafeli durmalarına neden olmuştur. Bununla birlikte Batı Roma İmparatorluğunun çöküşüyle sanat ve bilimde yaşanan durgunluk kriptolojiye de yansımıştır (Kahn, 1973: 74-75).

Sekizinci yüzyıla gelindiğinde, Halil b. Ahmed⁷ yapmış olduğu çalışmalar ile şifre çözümleme alanına kayda değer bir katkı sağlamıştır. Bulduğu kombinasyon hesaplama formülü, belirli sayıda harften oluşan kelimelerin sayısının hesaplanması ve kelimelerin muhtemel kombinasyonların tespiti açısından önemli olmuştur. Halil b. Ahmed'den kısa bir süre sonra ise Kindî ile İslam medeniyetinde bir nevi bir kriptoloji geleneğinin başladığını söyleyebiliriz (Alam, Mrayati ve at-Tayyan 2002: 54-56).

1.2. DOKUZUNCU VE ON İKİNCİ YÜZYILLAR ARASINDA İSLAM MEDENİYETİNDE KRİPTOLOJİNİN GELİŞİMİ

⁵ Gaius Iulius Caesar (ö. M.Ö. 44).

⁶ Marcus Tullius Cicero (ö. M.Ö. 43).

⁷ Ebü Abdurrahmân el-Halîl b. Ahmed b. 'Amr b. Temîm el-Ferâhîdî (ö. 175/ 791).

Elimizdeki kaynaklar İslam medeniyetinde kriptoloji geleneğinin dokuzuncu yüzyılın ilk yarısından itibaren oluşmaya başladığını göstermektedir. Bilindiği kadarıyla Kindî'nin şifre çözümü üzerine yazdığı eser ile başlayan bu süreç ardından gelen pek çok teşebbüsle gelişerek devam etmiştir. Bu dönemde yoğunlaşan tercüme hareketlerine paralel olarak dil bilim ve matematik alanında yapılan çalışmalar, kriptolojiye dolaylı olarak katkı sağlayarak gelişmesi için uygun zemini hazırlamıştır. Bununla birlikte etkili bir yönetim sisteminin gerektirdiği ihtiyaçlar da bu bilim ile ilgili çalışmalar için teşvik edici bir unsur olmuştur.

1.2.1. İslam Medeniyetinde Kriptolojinin Gelişimini Sağlayan Faktörler

1.2.1.1. Tercüme Hareketleri

Tarih boyunca her medeniyet, etkileşimde bulunduğu diğer medeniyetlerin tecrübesini belirli oranda kendisine katmıştır. İslam medeniyetinin de kendi gelişim sürecinde diğer medeniyetlerin felsefi ve bilimsel birikimlerine ilgisiz kalması pek mümkün olmamıştır. Hz. Peygamber'in vefatından (11/ 632) sonra dört halife ve Emevîler döneminde yapılan fetihlerle büyük bir coğrafyaya yayılmaya başlayan İslam medeniyeti, Çin'den İspanya'ya kadar genişleyerek Hindistan, Mezopotamya, Mısır gibi antik medeniyetlerin topraklarını da bünyesine katmıştır. Bu sayede birçok yerel kültürle temasa geçen Müslümanlar, zamanla bu kültürleri tanımak istemişlerdir (Dağbaşı, 2013: 177-178). Bunun yanı sıra İslam medeniyetinin kısa sürede bu kadar büyük bir coğrafyaya yayılmış olması, şehir yönetimi, sağlık sorunları ve teolojik tartışmalar gibi birçok sosyal ihtiyaç ve problemleri de beraberinde getirmiştir. Bu tür meselelere çözüm bulma arayışı da tercüme faaliyetlerinin başlamasına ve çeşitli bilimlerin gelişimine yol açmıştır (Gutas, 2020: 108-114).

Emevîler, yönetimi devraldıkları zaman idari, ticari ve toplumsal ilişkilerin yürümesi için Yunanca bilen memurlara ihtiyaç duymuşlardır. Bu durum o dönemde Yunancadan Arapçaya çeviriyi günlük hayatın bir parçası haline getirmiştir (Aslan, 2013:171). Bununla birlikte bu dönemde Nesturi ve Suriyeli Ortodoks Hristiyanlar, Aristoteles'in mantığı, Batlamyus'un astronomi ve kozmolojisi, Hipokrat ve Yunan tıbbı hakkında

Süryanice eserler kaleme almışlardır⁸ (Lindberg ve Shank, 2013: 35). Ancak böyle çoklu bir dil ortamında her ne kadar Yunanca ve Süryaniceden Arapçaya çeşitli çeviriler yapılmış olsa da bu çeviriler daha çok yönetimdeki sürekliliği sağlayabilmek adına yöneticilerin kişisel çabaları doğrultusunda gerçekleşmiştir (Gutas, 2020: 33-34). Emevîlerin daha ziyade fetihlerle meşgul olup devlet yapılanmasını ön planda tutmaları, bu dönemde yapılan çevirileri yetersiz kılmıştır (Aslan, 2013:172).

Abbasi dönemine gelindiğinde, özellikle Me'mûn yönetimiyle birlikte tercüme hareketleri bilinçli bir şekilde organize edilen ve iktisâdî olarak desteklenen bir etkinlik halini almaya başlamıştır. Sınırların genişlemesi ve ticari ilişkilerin artmasıyla farklı inanç, düşünce, kültür ve gelenekler Müslüman toplumunu daha çok ilgilendirmeye başlamıştır (Burgu, 2017: 117-118). Bu durum, Müslümanların kendi inanç esaslarını, ispatlı bir şekilde izah etme ve inkârcı akımlara karşı muhafaza etme ihtiyacını da doğurmuştur. Özellikle Mu'tezile ekolünün mantiki ve felsefî delillere olan ihtiyacı, tercüme hareketlerinin hız kazanmasında önemli bir rol oynamıştır (Burgu, 2017: 12). Bu dönemde Hristiyan alimlerin İslam dininden detaylı bir şekilde haberdar oldukları ve Müslümanlarla çeşitli teolojik tartışma ve polemiklere girdikleri, bunun sonucunda Müslümanların da kendi tartışma tekniklerini geliştirmek istedikleri bilinmektedir (Kalın, 2017: 64-65). Gutas, tercüme hareketlerini hızlandıran en önemli etkenlerden birisinin de kâğıt yapım teknolojisinin Müslümanlar tarafından öğrenilmesi olduğunu öne sürmektedir. Öyle ki kâğıt, Abbasi döneminin ilk on yılı içerisinde yazı yazılan diğer materyallerin yerini hızlı bir şekilde almıştır (Gutas, 2020: 25).

Tercümelere olan istek ve ihtiyaçlar Beytül'Hikme'nin⁹ kurulmasına yol açmıştır. Buradaki çalışmalar, sadece sistemli bir şekilde yapılan tercümelerle ile sınırlı kalmayıp özümseme ve üretim faaliyetleri de söz konusu olmuştur (Burgu, 2017: 24). Bu sayede İslam medeniyetine mensup bilginler, farklı dillerde yazılmış birçok eski ve çağdaş medeniyetin eserlerinden haberdar olmuşlardır. Bir zaman sonra o dönemde artık kullanılmayan dillerde yazılmış eserleri bile tercüme etmek istemişlerdir. Bu durum, bu bilginleri çeşitli dilleri öğrenmeye ve bu dillerin alfabelerini sınıflandırmaya teşvik etmiştir. Bununla birlikte çok sayıda simya, büyü, din ve felsefe eserinde şifre ile yazılmış

⁸ Bir örnek olarak bkz. Severus Sebokth (ö. 666/667)

⁹ Abbasi halifesi Me'mûn'un 830'da Bağdat'ta kurmuş olduğu ilim ve araştırma merkezidir. Ayrıntılı bilgi için bkz. <https://islamdusunceatlasi.org/beytul-hikme/3636>

kısımlar bulunmaktaydı. Bu kısımların anlaşılabilir olarak çevirilerin tamamlaması isteği şifreleri çözümü ihtiyacını doğurmuştur. Örneğin Zünnûn el-Mısrî (ö. 245/859) *Hall el-rumûz ve ber' el- 'askām fî kaşf 'uşûl el-lugāt ve el- 'aqlām* isimli eserinde eski alfabeleri, İbn Vahşiyye (ö. 10. yy) *Şevk el-mustehām fî ma'rifet rumûz al-aqlām* isimli eserinde Hint, Yunan, Mısır gibi medeniyetlerin de alfabeleri dahil olmak üzere toplam 93 farklı alfabe, Ebu'l-Kāsim el-İrākî (ö. 12 veya 13. yy) ise *Hall el-rumûz ve feth ekfāl el-kunûz* adlı eserinde eski medeniyetlerin şifreleme için kullandıkları alfabeleri ele almıştır (Alam ve diğerleri, 2002: 44-45).

Sonuç itibarıyla İslam medeniyetinin teşekkül ve sonrası döneminde, eski medeniyetlerin bilgi birikiminden yararlanmak amacıyla, bıraktıkları birçok eserin tercümesi yapılmıştır. Tüm bu süreç zarfında alimler, aktif kullanılan ya da kullanılmayan birçok alfabe ile hatırı sayılır oranda şifreli kısımlarla karşılaşmışlardır. Bu durum alimleri, şifreleri çözümlemeye teşvik ederek kriptolojinin bir bilim olarak temellerinin atılmasına yol açmıştır. Nitekim Kindî, birçok antik bilim insanının kitaplarında bilinmeyen semboller kullandığı için şifre çözümü bilginin, en büyük faydaları sağladığını ifade etmiştir (Alam ve diğerleri, 2002: 120).

1.2.1.2. Dil Bilim Çalışmaları

İslam medeniyetinin kısa sürede geniş bir coğrafyaya yayılması, Arapça bilmeyen toplulukları da medeniyetin bir mensubu haline getirmiştir. Bu toplulukların etkileşimleri sonucunda oluşan kültürel çeşitlilik ve değişimler, bir süre sonra Arap dilinin kullanımına da yansımıştır. Bu süreçte Arapçanın çok geniş bir kitle tarafından öğrenilmeye başlanması, konuşma dili ve Kur'an-ı Kerim'i okuyuş hatalarını da bir o kadar artırmıştır. Genel dil hataları ile ayetlerin kıraatlerinde yapılan hatalar sonucu ortaya çıkan farklı anlamların önüne geçilerek Arapçayı muhafaza etme ve dilin doğru bir şekilde öğrenilmesini sağlama amacı Arap dili üzerine çeşitli çalışmaların önünü açmıştır (Ayyıldız, 2019: 160-161).

Bir diğer husus ise İslam dininin iki ana kaynağı olan Kur'an-ı Kerim ve Hadis-i şerifleri doğru anlamının ilk aşamasının, Arapçanın iyi bir seviyede öğrenilmesi gerektiğinin fark edilmesi olmuştur (Dereli, 2020: 77). Arapçanın tüm İslami ilimlerin anahtarı konumunda

görülmesi, alimleri bu dili incelemeye ve dil bilgisi kurallarını ortaya koymaya teşvik etmiştir (Dereli, 2020: 73).

Arap dilinin iç yapısı ile ilgili tüm bu çalışmalar kriptolojinin İslam medeniyetinde gelişmesi açısından önemli bir zemin hazırlamıştır. Şifre yazma ve şifre çözme üzerine olan metinler detaylı olarak incelendiği zaman ses bilgisi, istatistiksel dilbilimi, şekil bilgisi, sözcük bilgisi, söz dizim kuralları, anlam bilimi, ölçü bilimi gibi dilbilimin alt dalı olan konularla yakın ilişkisi dikkat çekmektedir (Alam ve diğerleri, 2002: 47). Kindî, İbn Vehb, İbn ‘Adlân, İbn Duneynîr ve İbnu’d-Dureyhim eserlerinde harflerin birbirleri ile birleşme ve birleşmeme durumlarını bir şifre çözme yöntemi olarak ele alırken İbn ‘Adlân ve İbnu’d-Dureyhim bu bilgi seviyesini biraz daha ileriye götürerek dilbilim kuralları hakkında bilgi sahibi olmayı, şifreyi çözümleyici için şart bir nitelik olarak belirtmişlerdir (Alam ve diğerleri, 2003a: 40, 2003b: 52).

İslam medeniyetinin yetiştirdiği büyük bir dilbilim uzmanı olan Halil b. Ahmed, nahiv ilmini bir sistem altında toplamış, aruz ilmini ise yeni bir ilim dalı olarak ortaya koymuştur. Aynı zamanda matematikçi ve müzikolog olan Halil bin Ahmed, Arapçadaki kelimeleri kapsamlı bir şekilde sıralayabileceği bir sözlük oluşturmak istemiştir. Bunun sonucunda ilk Arapça sözlük olma özelliğini taşıyan *Kitâbü’l-‘Ayn* isimli eserini yazmıştır (Topuzoğlu, 1997: 309-312). Bir kelimenin kökünün en az iki en fazla beş harften oluşabileceğini belirterek işe başlayan Halil bin Ahmed, 28 harfli Arap alfabesinde anlamlı ve anlamsız olarak oluşturulabilecek 2, 3, 4 ve 5 harfli kelimelerin hesaplamasını yaparak kombinasyon hesaplama formülünü bulmuştur. Kombinasyon analizi olarak bilinen bu hesaplama ile olası kelimeler kümesi elde edildiği için sonlu sayıdaki kelimeleri yönetmesi daha kolay olmuştur (Rashed, 2015: 150-151). Celaledin Suyiti¹⁰ *el-Müzhir* adlı eserinde Hamza el-İsfahânî’den¹¹ alıntı yaparak Halil bin Ahmed’in *Kitâbü’l-‘Ayn*’da Arapçadaki 2, 3, 4 ve 5 harfli kelimeleri dört kategoride tekrarsız olarak toplam 12.305.412 olarak hesapladığını aktarmıştır. İsfahânî bu sayıyı çözümleyerek iki harfli 756, üç harfli 19,656, dört harfli 491.400 ve beş harfli 11.793,600 tane kelime olduğunu belirtmiştir. Bu alıntı günümüze ulaşan *Kitâbü’l-‘Ayn*’da geçmese de eserin başka bir nüshasında ya da Halil bin Ahmed’in şu an kayıp olan başka bir kitabında geçtiği düşünülmektedir. Sonuç itibariyle bu bilgiler, Halil bin Ahmed’in

¹⁰ Ebû’l- Fazl Celâlüddîn Abdurrahmân b. Ebî Bekr b. Muhammed el-Hudayrî es-Süyûtî eş-Şâfiî (ö. 911/1505).

¹¹ Ebû Abdillâh Hamza b. el-Hasen el İsfahânî (ö. 360/971’den önce).

halefleri tarafından bize aktarılmış ve kurmuş olduğu bu sistem ardından gelen dil bilimci ve matematikçiler tarafından geliştirilerek kullanılmaya devam etmiştir (Rashed, 2015: 152).

Kombinatör analizinin uygulama alanlarından biri de kriptoloji olmuştur. Bu sayede bir dilde n harfli anlamlı ya da anlamsız veya bazı harflerin belli olması kaydıyla kaç farklı kelimenin yazılabileceği ya da boşluksuz olarak yazılmış bir şifreli metnin bir satırında kaç farklı bölümlene yapılabileceği gibi hesapların yapılmasını mümkün kılmaktadır.

1.2.1.3. Matematik Çalışmaları

İslam dini Allah'a iman, namaz, oruç, hac ve zekât olmak üzere beş temel esas üzerine kurulmuştur. Allah'a iman İslami bilimleri öğrenmeyi gerektirirken geri kalanlar dünyaya ait bilimlerin öğrenilmesini gerektirmektedir. Namazlar ancak belirli vakitlerde ve kibleye yönelerek kılınmaktadır. Oruç için güneşin doğuş ve batış vaktinin gözlemlenmesi gerekmektedir. Hac yapabilmek için yine belirli vakitlerin tespit edilmesi ve Mekke'ye ulaşım için yol bilgisine ile ulaşım araçlarına ihtiyaç duyulmaktadır. Zekât ise iyi bir matematik bilgisi kullanılarak hesaplanabilmektedir (Hamidullah, 2016: 293/294). Bunların yanında günlük ve medeni hayatın bir parçası olan alışveriş yapma, bina inşa etme, miras paylaşımı, vergi hesaplama, takvim belirme, sulama ve tarım faaliyetleri gibi gereklilikler, matematiksel bilimlere olan ihtiyacı daha çok artırmıştır. Nitekim Hârizmî¹² (ö.850), Halife Me'mun'a¹³ ithaf ettiği ünlü eseri *Kitabu'l Muhtasar fi hisâbi'l-cebr ve'l-mukabele*'nin girişinde, eserini insanların günlük hayat içerisinde ihtiyaç duyduğu çeşitli konulardaki hesaplamaları kolaylaştırmak için kaleme aldığını ifade etmiştir (Cebbar, 2018:157). Kendinden önce dağınık ve ilişkisiz halde bulunan unsurları tek bir kitapta toplayarak bir araya getiren Harezmi, cebirin konularını sistematik bir şekilde ele almıştır (Cebbar, 2018:159). Kitabında aritmetiksel sayı tanımı ile bu sayının konumlu ve on tabanlı sayı sisteminde ifade ediliş tarzını açıklayan Harezmi, daha sonra cebirsel sayı tanımına geçmiş ve geliştirmiş olduğu sistemde sayının üç türünü göstermiştir (Fazlıoğlu, 1997: 224-227). Daha sonra gelen Sâbit bin Kurre, Ebu Kâmil, Kereci, Mâhânî (ö. 261/874 veya 271/884) gibi isimler kendi çalışmalarını

¹² Ebû Ca'fer Muhammed b. Mûsâ el Hârizmî (ö. 232/847'den sonra).

¹³ Ebû Ca'fer (Ebû'l- Abbâs) Abdullah el-Me'mûn b. Hârûn er-Reşîd (ö.218/ 833).

Harezmi'nin çalışmalarıyla birleştirilerek cebir ilmini genişletmişlerdir (Fazlıoğlu, 1993: 195-201).

Bununla birlikte Harezmi, *Kitâbü'l-Hisâbi'l-Hindî* adlı başka eserinde, Hint rakamları ile ondalık sayı sistemini İslam medeniyetine tanıtmıştır (Fazlıoğlu, 1997: 224-227). Hint hesap yönteminin 10 tabanlı, konumsal¹⁴ ve 9 rakam ile sıfırı içeriyor olması, işlem kabiliyetini ve yapılan işlemin denetlenebilirliğini artırmış böylece Hint hesap yönteminin diğer hesap yöntemlerine göre çok daha avantajlı olmasını sağlamıştır. Yunan ve Roma sayı sistemleri, konumsal olmayan yani sayının değerinin bulunduğu konuma bağlı olmayıp sabit olduğu sistem yapısına sahiptirler. Bu durum, büyük sayıların temsil edilmesini zorlaştırmakla beraber hata riskini de bir o kadar artırmaktaydı. Bununla birlikte bu sistem, sayıların kullanım alanlarını da sınırlamaktaydı. Ancak İslam medeniyetinde böylesi bir matematiğin gelişmesi hem şifreleme hem de şifre çözümü için bazı yöntemlerin ortaya çıkmasına imkân sağlamıştır. Hint rakamları ve konumsal sayı sistemi kullanılmadan, harflerin bulunma sıklıklarının hesaplanması gibi analitik yöntemlerin uygulanması çok zahmetli olurdu. Alfabadeki tüm harflerin bulunma sıklıklarının hesaplanmasına dayanan frekans analiz yönteminin kullanılması için açık metnin dilinde yazılmış yeterli uzunluktaki bir metnin incelenip, her harfin kaç kere kullanıldığının sayılması ve sıralanması gerekmektedir. Bu hesaplama Roma rakamları ile yapılacak olsaydı, örneğin 974 kere kullanılan “K” harfinin CMLXXIV ya da DCCCCLXXIV şeklinde yazılması gerekmekteydi. Bu yazım şeklinin alfabadeki her harf ve şifreli metindeki her sembole uygulanması bir de bulunan bu değerlerin sıralanması süreci çok daha külfetli hale getirirdi. Bilindiği kadarıyla ilk defa Kindî tarafından *Risāle fî istihrāc el-mu‘ammā* adlı eserinde açıklanan ve “Frekans Analizi” olarak bilinen bu yöntem, basit yerine koyma yöntemi ile oluşturulan şifreleri kırmada çok etkili olmuştur.

Bu dönemde kullanılan şifreleme yöntemlerine bakıldığında ise harflerin temsil ettiği sayı değerlerine çeşitli aritmetik işlemler uygulanarak oluşturulan yöntemler dikkat çekmektedir. Bazı müellifler harflerin denk olduğu sayı değerlerine çarpma ve bölme işlemleri uygulanarak elde edilen değerlerin yeniden harfe dönüştürülmesinden bahsetmişlerdir. Bu yöntemin uygulanabilmesi için bir sayının sayısal değerinin kaç farklı

¹⁴ Sayının bulunduğu konumun sayı değeri için önemli olduğu sistem.

şekilde elde edilebileceğinin hesaplanması gerekmektedir. 28 harfli bir alfabe için 28 farklı sayısal değer söz konusudur. Her bir değer için ortalama 6 farklı işlem yapılacak olsa toplamda 168 farklı hesaplama yapılması gerekmektedir. Dolayısı ile bu yöntem, dört işlemin pratik bir şekilde uygulanabildiği Hint hesap sisteminin bir ürünü olarak düşünülmektedir. Bu bağlamda İslam medeniyetinde yapılan cebir ve aritmetik alanındaki çalışmaların, şifreleme ve şifre çözümü yöntemlerinin gelişmesine dolaylı olarak katkı sağladığı görülmektedir.

1.2.1.4. Yönetim Faaliyetleri

İslam medeniyetindeki kültürel ve entelektüel zenginlik büyük oranda toplumun refah ve huzur içerisinde olmasının bir sonucudur. Abbasi halifeleri iyi organize olmuş varlıklı bir toplum inşa etmeye önem vermişler böylece kanunları sıkı tutarak yozlaşmanın önüne geçmek, vatandaşlarını korumak, düşük vergilerle de ticaret ve endüstriyi teşvik etmek istemişlerdir. Tüm bunlar etkili bir yönetim sistemine bağlı olduğu için güvenli iletişim, çeşitli şifrelerin kullanımı ile sağlanmıştır (Singh, 2001: 20).

Etkili bir yönetimin sağlanabilmesi için gerekli olan haberleşme, yazışma, kayıt, gibi unsurların devlet idaresine dair özel bilgiler içermesi şifreleme ve şifre çözümü tekniklerinin gelişmesini teşvik etmiştir. Diğer taraftan, bu alandaki bazı eserlerin devletin idari kısmında bulunan kişilerin isteği üzerine ele alınmış olması da dikkat çekmektedir. Kindî, İbn 'Adlân ve İbnü'd-Dureyhim de bu tür bir motivasyonla eserlerini yazdıklarını ifade etmişlerdir (Alam ve diğerleri, 2002: 64).

1.2.2. Kriptolojide Öne Çıkan İsimler

1.2.2.1. Kindî

Tahmini olarak 215/ 801 senesinde Kûfe'de doğduğu düşünülen Ebu Yûsuf Ya'kûb bin İshâk bin es-Sabbâh el- Kindî, saygın bir Arap kabilesi olan Kinde 'ye mensuptur. Babasının Basra valisi olmasından dolayı ilk gençlik yıllarını burada geçirmiş, daha sonra Bağdat'a gitmiş ve vefatına kadar burada yaşamıştır (Corbin, 2010: 279).

Bulunduđu şehirlerin entelektüel faaliyetler bakımından zengin olması Kindî'nin eğitim hayatına katkıda bulunarak zamanın düşünce akımlarından daha kolay bir şekilde haberdar olmasını sağlamıştır. Abbâsîlerin altın çağını yaşadığı bir dönemde İslam medeniyetinde ilk Müslüman filozof olarak anılma özelliğine sahip olmuş ve Müslümanları felsefe ile tanıştıtararak dönemin fikrî tartışmalarında felsefenin önemini göstermeye çalışmıştır (Kaya, 2011: 91-92). Özellikle Aristoteles'in eserlerini incelemiş ve içselleştirdiğı felsefesinin kavramlarını geliştirmede önemli adımlar atmıştır (Kaya, 2002: 41-58). Kindî, hem felsefî düşüneyi bütüncül bir şekilde benimsemeye hem de İslam akidesine bağlı kalmaya çalışarak bu iki sistemi uzlaştıracı bir tutum içerisinde olmuştur. Öte yandan Kindî'nin bu bütüncül yaklaşımıyla beraber tercüme faaliyetleri sırasında çok fazla felsefî esere maruz kalması, sisteminin tam olarak tespitinin yapılmasını zorlaştırmış ve bazı açılardan farklı şekillerde yorumlanmasına sebep olmuştur. Aşağıdaki satırlar Kindî 'nin felsefeye yaklaşım tarzını açık bir şekilde göstermektedir:

Hak bilirligin gereğı olarak bize düşen, hakiki ve ciddi konularda kendilerinden büyük ölçüde yararlandıklarımız şöyle dursun, basit ve küçük ölçüde yararlandıklarımızı dahi karalamamaktır. Her ne kadar bazı gerçekleri görememişlerse de bize intikal eden düşünce ürünleriyle onlar, bizim atamız ve ortağımız sayılırlar. (...) O halde bize gerçeğı büyük ölçüde getirenler bir yana, onu azıcık olarak ulaştıranlara da şükür borcumuz büyük olmalı. (...) Nereden gelirse gelsin, isterse bize uzak ve karşıt milletlerden gelsin, gerçeğın güzelliğini benimsemekten ve ona sahip olmaktan utanmamalıyız. (...) (Kaya, 2011: 96).

Sadece felsefe ile kalmayıp fizik, metafizik, tıp, matematik, astronomi, ahlâk, kriptoloji, psikoloji, kimya, optik, siyaset, meteoroloji, astroloji ve kehanet gibi alanlarla da ilgilenmiş ve eserler vermiştir (Kaya, 2011: 96).

Bununla birlikte Kindî'nin İslam dünyasındaki ilimler tasnifini yapan ilk iki kişiden biri olduğunu düşünülmektedir. İlimleri dinî ve insanî olarak ikiye ayıran Kindî, insan çabasıyla elde edilen bilginin insanî, sadece peygamberlere gelen vahyin ise dinî bilgi olduğunu söylemiştir. Ancak dinî bilginin, insan çabasına dayanmayıp doğrudan Allah'ın öğretmesi ile elde edilen bir bilgi türü olduğu için daha üstün olduğunu ifade etmiştir (Türker, 2019: 63-73). Farklı bilgi alanlarının kendine özgü metotları olması gerektiğini vurgulamış, örneğın matematikte ikna değil, ispat metodunun kullanılması gerektiğini

belirtmiş, ikna metodunun kullanılması durumunda, bu bilginin bilimsel değil zannî bir bilgi olacağını savunmuştur (Kaya, 2011: 97). Kindî aynı zamanda birçok müzik terimini de Arapçaya kazandırmıştır. Arap musikisini belirli bir seviyeye getirerek bu musikinin kurallarını aktaran ilk kişi olmuştur (Turabi, 2002: 58-59).

Halife Me'mûn'a ithaf ederek yazdığı *Risâle ile'l-Me'mûn fi'l-ille ve'l-ma 'lûl* isimli eserinden, Me'mûn'un gözünde saygın bir konuma sahip olduğu anlaşılan Kindî, (Kaya, 2011: 92) İslam dünyasının ilk ilimler akademisi olarak kabul edilen Beytül Hikme'de görevlendirilmiştir (Erdem, 2013: 58). Kindî'nin Beytül Hikme'deki çalışmaları ve katkıları ayrı bir çalışmanın konusu olsa da kısaca Yunancadan yapılan tercümelerin kontrol edilmesi ve hataların düzeltilmesi için denetmenlik yaptığı söylenebilir. Bir eseri baştan sona tercüme edecek kadar Yunanca bilmediği fakat halihazırda tercümesi bitmiş eserleri kontrol ettiği, Arapça terim karşılıklarını yazıp yorumladığı ve özetlediği bilinmektedir. Ayrıca o dönemde birçok felsefe eseri Arapçaya yeni tercüme edildiğinden kavramların daha iyi anlaşılması için Kindî'nin felsefi bir dil geliştirmeye çalıştığı da görülmektedir (Köroğlu, 2021: 898).

Yazmış olduğu eserlerden Me'mûn'dan sonra gelen Halife Mu'tasım döneminde tanınırlığının daha çok arttığı anlaşılmaktadır. Mu'tasım, oğlu Ahmed'in hocası olarak Kindî'yi görevlendirmiş, Kindî de bazı eserlerini Ahmed'e ithaf ederek yazmıştır. Bu eserlerden bir tanesi de bu çalışmada ele alınan kriptoloji üzerine yazmış olduğu eseridir. Ancak zamanla çeşitli çevrelerin baskı ve eleştirilerine maruz kalarak kütüphanesinesine el konulduğu bilinmektedir. Kindî 'nin Bağdat'ta yaklaşık 252/866 senesinde vefat ettiği tahmin edilmektedir (Kaya, 2002: 41-58).

Kindî'nin, bir kısmını halifelere bir kısmını da dostlarına ithaf ettiği 277 eseri olduğu söylenmektedir. Bu eserlerin tam listesi İbn Nedim'in *Fihrist*'inde bulunmaktadır (Kaya, 2011: 93). On ikinci yüzyılda Arapçadan Latinceye çevrilen kitaplar arasında Kindî'nin de birkaç eseri bulunmaktadır (Ülken, 2020: 64).

1.2.2.1.1. Kriptoloji Eseri

Kindî, pek çok antik felsefeci ve bilim insanının eserlerinde bilinmeyen semboller bulunduğu için şifre çözümüleme biliminin kişiye en büyük avantajları sağladığını ve bu bilimi bilmeyen kişilerin kendi alanlarında iyi seviyelere ulaşamayacaklarını ifade etmiştir. Kindî bu eseri yazma amacının, kısa zamanda anlaşılması zor olan eserlerin kolaylıkla anlaşılması sağlamak için ilimle meşgul olan kimselere yardımcı olmak olduğunu belirtmiş ve eserini Halife el-Mu'tasım'a ithaf etmiştir (Alam ve diğerleri, 2002: 118-120). *Risāle fî istiḥrāc el-mu'ammā* isimli eserini yazma nedenini bu şekilde belirttikten hemen sonra şifre çözümüleme algoritmalarını anlatmaya başlayan Kindî, düz yazı içerisinde bulunan şifrelerin çözülmesi için niceliksel ve niteliksel olmak üzere iki yöntemden bahsetmiştir.

Niceliksel yöntem, çözümüleme yapılacak metnin dilinde sıklıkla kullanılan harflerin belirlenmesini içermektedir. Sesli harflerin bir dilin asıl unsurunu oluşturduğunu belirten Kindî, nasıl altın metalinden taç, bilezik, kolye gibi farklı cisimler oluşturuluyor ise sesli harflerden de farklı kelimelerin oluşturulduğunu ve bu sebeple de sesli harflerin kullanım sıklıklarının sessiz harflerden daha fazla olduğunu ifade etmiştir (Alam ve diğerleri, 2002: 122). Şifreyi çözmeye başlamadan önce açık metnin diline ait uzun bir metnin ele alınması ve bu metne göre alfabedeki her harfin bulunma sıklıklarının hesaplanıp bu sıklığa göre sıralanması gerektiğini belirtmiştir. Daha sonra çözülmek istenen şifreli metinde kullanılan semboller de aynı şekilde bulunma sıklıklarına göre sıralanarak açık metindeki harflerin bulunma sıklıklarıyla eşleştirilmelidir (Alam ve diğerleri, 2002: 124). Frekans analizi olarak bilinen ve Kindî 'ye atfedilen bu yöntem, özellikle tek alfabeli yerine koyma yöntemi ile hazırlanmış şifreleri kırmada çok etkili olmuştur.

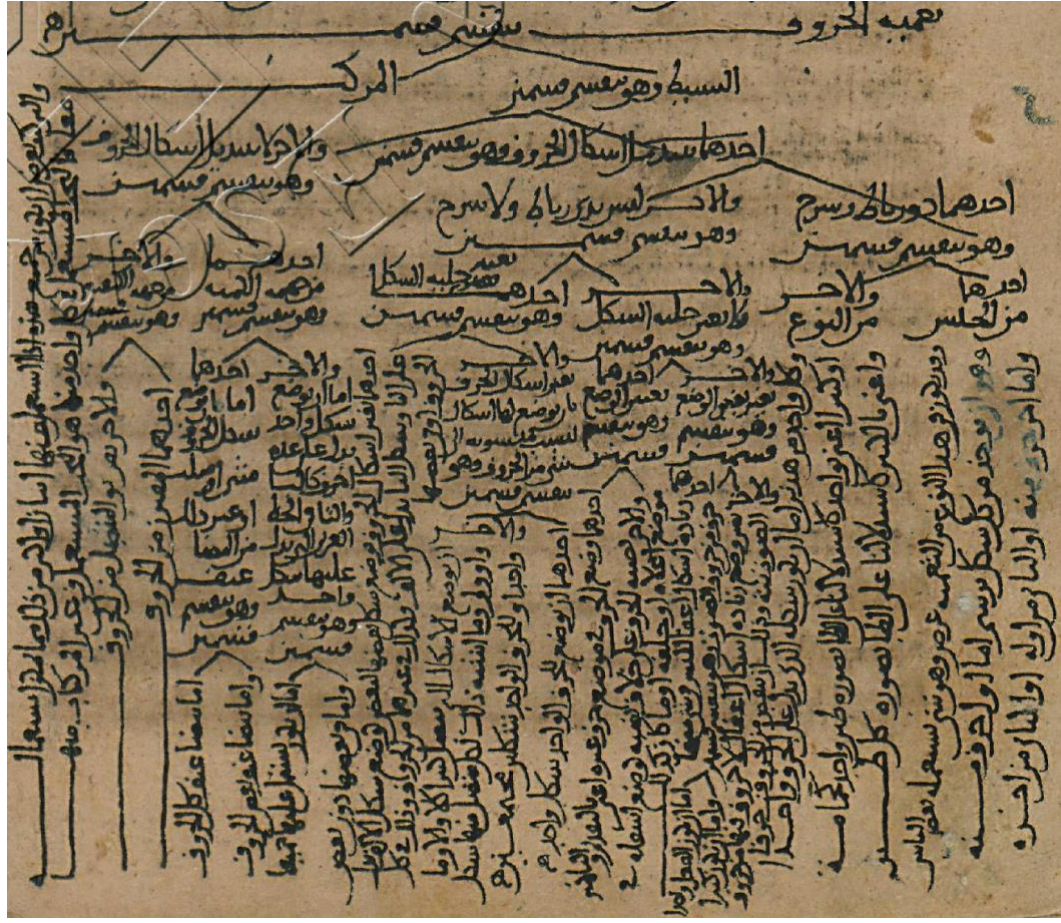
Alfabedeki her harfin yeteri kadar kullanılmadığı şifreli metinlerde ise şifreyi çözme yöntemi farklılaşmaktadır. Bu tür metinlerde frekans analizi yönteminin artık güvenilir bir araç olmayacağına dikkat çeken Kindî, niceliksel yöntem yerine dilin yapısal özelliklerinin kullanıldığı, harflerin birleşme veya birleşmeme durumlarına dayanan niteliksel yöntemin kullanılması gerektiğini belirtmiştir (Alam ve diğerleri, 2002: 124-126). Bu durumda harflerin birbirleriyle birleşme veya birleşmeme özelliklerinin iyi bir şekilde öğrenilmesi gerekmektedir. Şifreli metinde öncelikle sık kullanılan harfler tespit edildikten sonra, bu harflerle birleşen ve birleşmeyen harfler göz önünde bulundurularak

önündeki ve arkasındaki harfler tespit edilmeye çalışılmalıdır. Birleşmeyen harfler zaten metnin içerisinde dağılmış vaziyette olacaklardır ancak ayrılmayıp birlikte kullanılanlar ise çıkarım yapmaya yardımcı olacaklardır (Alam ve diğerleri, 2002: 126).

Bununla birlikte Kindî, sıklıkla birlikte kullanılan سم, عل, كم, لو, ثم, أو, عن, مم, لم, ما gibi iki harfli ve كما, على gibi üç harfli kelimelerin bilinmesinin önemli olduğunu vurgulayarak şifre çözmede bu kelimelerden yararlanılması gerektiğini belirtmiştir. Şifreleri çözmede başka bir yardımcı unsur olarak, onursal unvanlar gibi kullanılması muhtemel kelimelere de değinen Kindî, çoğunlukla metinlerin başında kullanılan “Bismillahirrahmanirrahim” ifadesinin şifreli metinlerde genellikle tercih edilmeyeceğine dikkat çekmiştir (Alam ve diğerleri, 2002: 128).

Şifre çözme yöntemlerinin ardından Kindî’nin diğer bir özgün çalışması ise şifreleme yöntemlerini sınıflandırması olmuştur. Kindî, yöntemleri ağaç diyagramı halinde alt gruplara ayırarak numaralandırmış her birinin açıklamasını yapmıştır. Kindî’nin bilindiği kadarıyla daha önce benzeri yapılmamış bu çalışması, okuyucuya sunduğu katkı ve kolaylık açısından büyük bir öneme sahiptir. Kendisinden yaklaşık üç yüz elli sene sonra yaşamış olan İbn Duneynî de bu yöntemlere yenilerini ekleyerek eserinde yer vermiştir.

Resim 1: Kindî'nin *Risāle fî istihrāc el-mu'ammā* isimli risalesinde yapmış olduğu şifreleme yöntemleri sınıflandırması



Kaynak: Süleymaniye Kütüphanesi, Ayasofya 4832, vr. 212b.

Şifreleme yöntemlerini, basit ve birleşik şifreleme olmak üzere ikiye ayıran Kindî, birleşik şifrelemenin basit şifreleme yöntemlerinin kombinasyonu ile oluşturulduğunu belirtmiş ve daha fazla detaylandırmamıştır. Basit şifreleme yöntemlerini ise ayrıntılı olarak sınıflandırarak açıklamalarına yer vermiştir.

Kindî basit şifreleme yöntemlerini, şekillerini koruyan ve şekillerini değiştiren harfler olmak üzere iki ana bölüm altında incelemiştir. Harflerin şekillerinin korunduğu şifreleme yöntemlerinde adında da anlaşıldığı üzere açık metinde kullanılan harfler kullanılmaktadır. Bu başlık altında; Harflerin tekrarlanması, ortak bir harf ile temsil edilmesi, doğası gereği ayrı yazılan harflerin birleştirilmesi ve doğası gereği birleşik yazılan harflerin ayrılması şeklinde dört ayrı yöntem belirlemiştir. Bu yöntemlerin metnin

bir kısmına veya tamamına uygulanabileceğini de ifade etmiştir (Alam ve diğerleri, 2002: 132).

Kindî, harflerin şekillerinin değiştirildiği yöntemleri ise, harflerin ilişkilendirilerek şifrelenmesi ve ilişkilendirilmeyerek şifrelenmesi şeklinde ikiye ayırmıştır. İlişkilendirilerek yapılan şifreleme yöntemleri, harflerin bir kategoriye ait isimlerle ilişkilendirilmesine dayanmaktadır. İlişkilendirilme yapılmadan uygulanan şifreleme yöntemi altında ise yerine koyma ve yer değiştirme şifreleme türlerini incelemiştir. Yer değiştirme yönteminin, harflerin konumunun veya açısının değiştirilmesi, bazı harflerin eklenmesi veya çıkartılması şeklinde dört farklı biçimde uygulanabileceğini belirtmiştir. Harflerin konumunun değiştirilebilmesi için çeşitli alternatifler sunmuş, ekleme ve çıkarmada ise sesli harflerin kullanılmamasını şart koşmuştur. Yerine koyma yöntemini ise, açık metnin harflerinin ya da çeşitli sembollerin kullanılması olarak ikiye ayırmıştır. Böylece şifrelenecek metindeki harflerin yerine ya dilin gerçek alfabesindeki harflerin ya da sembollerin konarak şifreleme yapılabileceğini belirtmiştir. Kindî'nin mevcut dilde sıklıkla birlikte kullanılan ikili ve üçlü harfler için de ortak bir sembol kullanma düşüncesi, şifrenin çözümlenmesini zorlaştırması bakımından oldukça dikkate değer bir noktadır (Alam ve diğerleri, 2002: 132-140).

Kindî, basit şifreleme yöntemlerini açıkladıktan sonra eserin kısa ve öz anlatım amacını aşacağından bu yöntemlerin birleştirilmesiyle oluşturulan birleşik şifreleme yöntemlerini detaylandırmayacağını ifade etmiştir (Alam ve diğerleri, 2002: 142).

Kindî daha sonra bu yöntemlerin çözümlenmelerine ilişkin çeşitli tavsiyelerde bulunmuştur. ¹⁵Açıklanan tüm çözümlenme algoritmaları uygulandığı halde şifre hala çözümsüz kalırsa bunun birleşik şifreleme olduğu sonucuna varılmasını ve algoritmaların tek tek birbiri ile eşleştirilerek denenmesi gerektiğini belirtmiştir. Başka bir ifade ile birleşik şifrelerin çözümlenmesi için, deneme yanılma yoluyla hangi algoritmaların uygun olduğunu tespit etmek gerekmektedir. Kindî, frekans analizinin tüm bu yöntemler arasında güçlü bir rehber olduğuna da ayrıca dikkat çekmiştir (Alam ve diğerleri, 2002: 164).

Son bölümde harflerin bulunma sıklıklarını ele alan Kindî, Arap harflerinin kullanım sıklıklarını azalan sıraya göre sıralamış ve bu sıralama için yedi sayfadan oluşan bir metinden yararlandığını ifade etmiştir (Alam ve diğerleri, 2002: 166-168). Kindî harflerin

¹⁵ Ayrıntılı bilgi için bkz. Alam, Mrayati ve at-Tayyan, 2002: 146-162.

kombinasyonlarını da ele almış ve harfleri “esas harfler” ve “değişken harfler” olmak üzere iki kısma ayırmıştır. Ek olarak kullanılmayan esas harfleri¹⁶ ya hiçbir şekilde birleşmeyen ya da sadece önünden veya sadece sonundan birleşen harfler olarak tanımlamıştır. Değişken harflerin ise bazen esas bazen ek harf olarak kullanılabileceğini belirtmiş ve hem önünden hem sonundan birleşen ya da sadece önünden veya sadece sonundan birleşen harfler olarak tanımlamıştır¹⁷ (Alam ve diğerleri, 2002: 172). Kindî eserini 16 temel harfin, hangi harflerle ve hangi pozisyonlarda birleşip birleşmediği bilgisini vererek sonlandırmıştır.¹⁸

1.2.2.2. İbn Vehb

Hakkında yeteri kadar bilgi bulunmayan Ebu el-Hüseyin İshak ibn İbrahim ibn Süleyman ibn Vehb el-Kâtib’in, hayatının büyük bir kısmını hicretin dördüncü yüzyılında (10. yy) geçirdiği tahmin edilmektedir.

Vehb’ler yazarlık mesleği ile tanınan isimlerdendi. Bu durum, yazarlığın onlar arasında nesilden nesile aktarıldığını göstermektedir. Bununla birlikte Vehbler’den bazılarının siyaset ve devlet yönetimi ile de ilgilendikleri ve Abbasiler döneminde, Emevîler döneminde olduğundan daha fazla tercih edildikleri bilinmektedir. Öyle ki Vehbler’in bu hayli saygın statüleri, Ebû Temmâm (ö. 231/ 846), Buhtürî (ö. 284/897) ve Rûmî (ö. 283/896) gibi büyük Abbasi şairlerine methiyeler yazdırmıştır (Alam, Mrayati ve at-Tayyan, 2007: 73).

1.2.2.2.1. Eseri

İbn Vehb, *el-Burhân fî Vucûhi’l-Beyân* isimli eserine, yazılı şifrelemenin sözlü yapılan şifrelemeden daha uygun ve güvenli olduğunu belirterek başlamıştır (Alam ve diğerleri, 2007: 94). Arap alfabesindeki 29 harfin 18 tane şekli olduğunu ve çeşitli noktalamalarla farklı harflerin belirgin hale getirildiğini belirtmiştir. Bazı şifrelerin, harflerin sayısına bazılarının ise şekillerinin sayısına dayandırılarak oluşturulduğuna dikkat çekmiş ve şifreleme yöntemlerini “terceme” ve “te’miye” olmak üzere iki türe ayırmıştır (Alam ve

¹⁶ ث، ج، ح، خ، د، ذ، ر، ز، ش، ص، ض، ط، ظ، ع، غ، ق

¹⁷ ي، و، ه، ن، م، ل، ك، ف، س، ت، ب، ا

¹⁸ Ayrıntılı bilgi için bkz. Alam, Mrayati ve at-Tayyan, 2002: 172-202.

diğerleri, 2007: 96). Alimler, “terceme” terimi; kriptoloji, basit yerine koyma ve şifre çözümü olmak üzere üç farklı anlamda kullanılmaktadır (Alam ve diğerleri, 2002: 24). İbn Vehb’in bu terimi, bir harfin yerine başka bir harfin ya da harf biçimine benzemeyen bir sembolün konulduğu “basit yerine koyma” anlamında kullandığı görülmektedir (Alam ve diğerleri, 2007: 98).

Diğer şifreleme türü olan te’miye ise anlaşılır halde yazılmış bir metni, belirli yöntemler kullanarak anlaşılmaz hale dönüştürme sürecini ifade etmek için kullanılmaktadır. İbn Vehb bu şifreleme türünü aşağıdaki şekilde üç kısma ayırmaktadır.

1. Her harfin bir kavramla ilişkilendirilerek şifrlenmesi: Harfleri temsil etmek için kategorilere ait isimler kullanılır.
2. Harflerin belirlenen bir kurala göre yerlerinin değiştirilerek şifrlenmesi: Açık metindeki harflerin belirli bir düzene göre yerleri değiştirilerek anlamsız bir metin elde edilmeye çalışılır.
3. Gereksiz harf ekleme ya da çıkarma yoluyla şifreleme: İbn Vehb bu şifrelemenin, açık metne gereksiz harfler eklenmesi, sık kullanılan iki harfli kelimelere tek bir sembol verilmesi veya benzer yazım şekline sahip harflerin ortak bir harf altında yazılması şeklinde üç farklı türde uygulanabileceğini belirtmiştir. Bu yöntemlerin uygulamalarının sayılamayacak kadar çok olduğunu ifade eden İbn Vehb, şifre çözümü yöntemlerini açıklamaya geçmiştir (Alam ve diğerleri, 2007: 98-102).

İbn Vehb’e göre eğer şifreli metin yeteri kadar uzun ise, ilk olarak harflerin yerine kullanılan tüm sembollerin tek tek sayılması ve bulunma sıklıklarına göre sıralanması gerekmektedir. Bu noktada okuyucusuna aşağıdaki dört olası durumu sunmuştur.

Şifreli bir metinde kullanılan sembollerin sayısı;

- a. 29 ise, her harfi temsil etmek için bir sembol kullanıldığına
- b. 29’dan fazla ise, gereksiz semboller kullanıldığına
- c. 29’dan az ve 18’den fazla ise, noktasız hali ile yazımı ortak olan bazı harfler için ortak bir sembol kullanıldığına
- d. 18 ise, noktasız hali ile yazımı ortak olan tüm harfler için ortak bir sembol kullanıldığına delalet etmektedir.

Tüm sembollerin metinde kaç kez kullanıldığı sayılarak en fazla bulunma sıklığına sahip olan sembolden en aza doğru bir sıralama yapılır. İbn Vehb bu kısımda, kolaylık olması bakımından Arap harflerinin bulunma sıklıklarını azalan sıraya göre sıralamıştır (Alam ve diğerleri, 2007: 104). Bununla birlikte niceliksel çözümleme yöntemi olan frekans analizinin, tüm harflerin yeteri kadar kullanıldığı metinler için geçerli olduğuna ve kısa metinler için bu yöntemin işlevselliğini kaybedeceğine değinmiştir. Şifreli metnin kısa olma durumunda ise metni çözmek için Arap harflerinin birleşme ve birleşmeme özelliklerini içeren niteliksel yöntemin kullanılması gerektiğini ifade etmiştir. İbn Vehb'e göre kısa bir metni çözmek için yapılan sezgiye dayalı tahminde, iki harf arasında kalınırsa birleşmeyi kabul edip etmediklerine bakılmalıdır. Her iki harf de birleşebilen özellikteyse, bu harflerin metnin başka kısımlarında da geçtiği yerlere bakılmalı ve bir anlam ifade edip etmedikleri kontrol edilmelidir. Harfler birlikte bir anlam kazanana kadar bu eşleştirmeler devam etmelidir. İbn Vehb, bir dilde sıklıkla kullanılan iki harfli kelimelerin de şifrelenmiş harfleri ortaya çıkarmada çok fazla işaret sunduğuna dikkat çekmiştir. Bazen bu iki harfli kelimeler için tek bir sembolün kullanıldığını da hatırlatan İbn Vehb, böyle bir durumda zorda kalmamak için Arap dilinde çok sık kullanılan iki harfli kelimelerin bulunma sıklıklarına göre sıralamasını yapmıştır. Bununla birlikte şifre çözümlemede, başlangıç ifadeleri olarak kullanılan dua, unvan ve saygı ifadelerinin çok önemli bir ipucu olduğunu ve harfleri ortaya çıkarmada kolaylık sağladığını ifade etmiştir (Alam ve diğerleri, 2007: 106).

İbn Vehb, kriptoloji hakkında eser veren diğer müelliflerden farklı olarak şifreleri çözümlemeye yardımcı olması için harflerin çıkış noktalarına da değinmiştir. Harflerin 13 tane çıkış noktası olduğunu belirterek nereden ve hangi şekilde çıktıklarını aşağıdaki şekilde tarif etmiştir:

م, ب, و ve ف harfleri dudaktan,
ظ, ث ve ذ harfleri dil ucunu üst ön dişlerin etlerine dokundurarak,
د, ت ve ط harfleri dili dış köklerine kilitleyerek,
س, ص ve ز harfleri dil yüzeyini hafif bir şekilde derinleştirerek,
ن, ر ve ل harfleri dil ucundan,
ض harfi dilin sağ ya da sol her iki tarafından,
ج, ي ve ش harfleri dilin kenarı ve ortası arasında yayılarak,

ك harfi dilin köküne doğru,
ق harfi dil kökündeki en uç noktadan,
خ ve غ harfleri boğazın ağza en yakın kısmından,
ع ve ح harfleri boğazın orta kısmından,
ء (hemze) ve ه harfleri boğazın en uç kısmı olan göğüs kafesinin önünden,
ن harfi ise üst damaktan çıkmaktadır (Alam ve diğerleri, 2007: 108).

İbn Vehb, bu tür harflerin birlikte bulundukları zaman birbirine benzeme eğiliminde olduklarına dikkat çekmiş ve çıkış noktaları birbirine yakınlaştıkça telaffuzlarının güçleştiğini ifade etmiştir (Alam ve diğerleri, 2007: 110). Arapça konuşmanın büyük bir kısmının nispeten daha kolay olan dil ve dudak bölgelerinden çıkarılan harflerden oluştuğunu belirtmiş, bu harflerin bir veya ikisi olmadan, neredeyse dört veya daha fazla harften oluşan isim ya da fiil olmadığını söylemiştir. Bu özelliğin boşluk kullanılarak hazırlanmış bir şifreli metni çözümlemeye önemli bir ipucu olarak kullanılabileceğini de eklemiştir (Alam ve diğerleri, 2007: 116). İbn Vehb'in harflerin birleşme özelliklerini çıkış noktaları ile açıklayarak ele almış olması, bu özelliğin daha kalıcı bir şekilde öğrenilmesini istediğini göstermektedir.

İbn Vehb şifre çözümleme için son bir ipucu daha vererek, şifreli metni oluşturan kelimelerin harf sayılarını incelemeyi de tavsiye etmiştir. Şifreli metindeki kelimeler genel olarak üç veya dört harfli kelimelerden oluşuyorsa, metnin gereksiz harfler kullanılmadan oluşturulduğunu, çoğunlukla dört, altı ve sekiz harfli uzun kelimelerden oluşuyorsa, şifrenin büyük ihtimalle gereksiz harfler eklenerek oluşturulmuş olabileceğine dikkat çekmiştir. Buna gerekçe olarak Arapçada isimlerin köklerinin çoğunlukla beş, fiillerin ise dört harften oluştuğunu belirtmiştir (Alam ve diğerleri, 2007: 116). İbn Vehb eserinin son bölümünü ise şiirsel şifrelerin çözülmesi üzerine ayırmıştır. Fakat şiirsel şifreler bu çalışmanın konusu olmadığı için burada ele alınmamıştır.

1.2.2.3. A ve B'nin Yazarı

Bu çalışmada ana kaynak olarak kullanılan “Arabic Origins of Cryptology” isimli serinin 6. cildinin 1. bölümünde, müellifi belli olmayan ve aynı kişi tarafından yazıldığı bilinen iki risale bulunmaktadır. Bir karışıklığa sebebiyet vermemek adına risalelerden birincisi “A risalesi”, ikincisi “B risalesi”, yazar ise “A ve B'nin yazarı” olarak adlandırılacaktır. Kronolojik yaklaşım, A ve B'nin yazarının bu çalışmaya konu olan risalelerinin, kendisine atıfta bulunan İbn Duneynîr'in risalesinden daha önce yazıldığını göstermektedir. Bunun yanı sıra, A ve B'nin yazarının, şifreleme için İbn Tabataba'nın kullandığı “terceme” terimini kullanması, İbn Tabataba'dan önce bu terimin kullanılmadığı da göz önünde bulundurulursa, A ve B'nin yazarının risalelerini İbn Tabataba'nın (ö. 322/ 934) kriptoloji üzerine yazdığı eserinden daha sonra yazmış olduğu düşünülmektedir. Bu ipuçları, A ve B'nin yazarının 10. 11. ya da 12. yüzyıllarda yaşamış olabileceğine işaret etmektedir. Öte yandan İbn Duneynîr dışında başvurulabilecek güvenilir kaynaklarda yazar hakkında herhangi bir atıfa rastlanmamıştır. İbn Duneynîr, Kindî ve İbn Tabataba 'ya ismi ile atıf yaparken bahsi geçen A ve B'nin yazarı için bir isim kullanmamış olması yazarın kimliğinin belli olmadığına işaret etmektedir (Alam ve diğerleri, 2007: 5-6).

1.2.2.3.1. Eseri

Eser, kolay ve karmaşık şifrelerin çözülmesi üzerine iki ayrı risaleden oluşmaktadır. Yazar, beş bölümden oluşan A risalesine, kişinin şifre çözümü işine büyük bir sabır ve tam bir kararlılık halinde, kendisini adayarak başlaması gerektiğini ifade ederek giriş yapmıştır. Yazara göre, bu süreçte hevesi kırılmış ruh halinin kişiye faydası olmayacağı için ümitsizliğe düşülmemelidir ve zihin fazla yorulmamalıdır. Bununla birlikte zaman zaman rahatlamak için verilen ipuçlarına tekrar göz atılmalı ancak buna rağmen hala bir sonuç alınamazsa bu şifrenin yazarın B risalesinde ele aldığı şifre türlerinden biri olduğu sonucuna varılması gerekmektedir (Alam ve diğerleri, 2007: 34).

Yazar ikinci bölümde, çözümleme algoritması frekans analizi yöntemine dayanmayan şifreleri ele almıştır. Bu bölümde bir şifre çözümleyicinin karşılaşılabileceği yer değiştirme, harf ekleme, harf ayırma gibi bazı şifreleme türlerine örnekler vermiştir. Bu

şifreleme türlerini frekans analizi yönteminden ziyade uygulama yapılarak edinilen deneyim ile çözümlenebilecek şifreler olarak tanımlamıştır. Daha sonra harflerin sayısal değerlerinin dinar para birimi ile temsil edilmesine dayanan bir şifreleme yönteminden bahsetmiştir. Ebced sistemindeki sayısal değerleri 1'den 10'a kadar olan harflerin tam dinar ile, 10 ve katlarına denk olan harflerin çeyrek dinar ile, 100 ve katlarına denk olan harflerin yarım dinar ile ve 1000 sayısına denk olan Ğ harfinin ise 1/8 dinar ile temsil edilebileceğini belirtmiştir (Alam ve diğerleri, 2007: 36-38). Bu yönteme, kendisinden daha sonra yaşadığı tahmin edilen İbn Duneynîr de eserinde yer vermiştir.

Yazar üçüncü bölümde ise frekans analizi yöntemine dayanan çözümleme algoritmalarını ele almıştır. Harflerin yeterli sıklıkta kullanılmadığı metinleri çözmeye çalışmanın faydasız olacağını belirtmiş ve şifreli bir metnin en az on satırdan oluşması gerektiğini ifade etmiştir. Bir önceki bölümde verilen ipuçları ile şifrenin çözülemediği takdirde, şekil bakımından birbirine benzeyen sembollere özellikle dikkat edilerek şifreli metindeki tüm sembollerin sayılması gerektiğini belirtmiştir. Toplam sembol sayısı 28 ise alfabedeki her harf için bir sembol, 29 ise ﻻ harfi için de bir sembol, 30 ise kelimeler arasında kullanılan boşluk için de ayrı bir sembol atandığı sonucuna varılır. Tüm bu semboller metindeki kullanım sıklıklarına göre sıralanır. En yüksek bulunma sıklığına sahip sembolün altına boşluk ya da ﻻ harfi diye not düşülür. ﻻ harfini temsil eden sembolle birlikte sık tekrarlandığı görülen ve sıklık sayısı olarak da ﻻ harfinin sıklığına yakın olan sembolün altına ise ﺝ harfi olarak not düşülür. Kalan harfler de benzer şekilde bulunma sıklıklarına göre sembollerle eşleştirilir. Böylece harfler ve kelimeler yavaş yavaş açığa çıkmaya başlayacaktır. Bunun yanında yazar ﺍﻝ، ﻋﻦ، ﻓﻲ، ﻫﺬﺍ، ﻟﻮ gibi sıklıkla birlikte kullanılan harflerin bilinmesinin boşlukları ortaya çıkarmada oldukça yardımcı olacağını belirtmiştir. Başka bir ipucu olarak da ﺍﻝ takısı tespit edildikten sonra ﺍ، ﺝ، ﺝ harflerinin yan yana geldiği semboller aranarak metinlerde sık kullanılan ﺍﻟﻠﻪ kelimesinden ﺍﻫ harfinin bulunabileceğine değinmiştir (Alam ve diğerleri, 2007: 40-44).

Dördüncü bölümü, okuyucusuna yardımcı olmak için sembol kullanılarak basit yerine koyma yöntemi ile hazırlanmış bir şifrenin çözümlenmesine ayıran yazar¹⁹, beşinci bölümde çeşitli tavsiyelere yer vermiştir. Bu bilimde ne kadar çok pratik yapılırsa o kadar aşinalık kazanılacağını ve böylece şifrelerin eksiksiz bir biçimde çözümlenebileceğini belirtmiştir. Bununla birlikte şifre çözümlemede uzmanlaşmış kişileri, bilgilerini arkadaş

¹⁹ Ayrıntılı bilgi için bkz. Alam, Mrayati ve at-Tayyan, 2007: 44-52.

grubu arasında bahis ve eğlence aracı olarak kullanmamaları gerektiğine dair uyarmıştır. Bu tür şifreler kasıtlı olarak uzun süreli zihinsel çaba harcatmak amacıyla hazırlandığı için kişinin becerilerini boş yere kullanmaması gerektiği tavsiyesinde bulunmuştur. Yazar, eğer kişi böyle bir işe girer ve başarılı olursa da bunun onun statüsüne hiçbir şekilde katkı sağlamayacağını ifade etmiştir. Ancak bu kişilerin, günün birinde yüksek rütbeli devlet yetkilileri tarafından devletin belirli meseleleriyle ilgili olan bir şifreyi çözümlemesi için de davet alabileceğine değinen yazar, bu değerli amacın bahis gibi maceralardan çok uzak olduğunu belirterek birinci risalesini sonlandırmıştır (Alam ve diğerleri, 2007: 54).

Yazar dört bölüm ve bir ekten oluşan B risalesinde ise ileri düzey şifreleme yöntemlerini ve çözümleme algoritmalarını ele almıştır. Birinci bölümde bu bilimin ihmal edilmemesi ve vermiş olduğu bilgilerin özümzenerek dayanak noktası olarak alınması gerektiğinden bahsetmiştir. Bilinmeyen bilinen olarak kalmasına müsaade edilmesini yani kasıtlı olarak gizemli bırakılan kısımlar için zihni yormaya gerek olmadığını belirtmiştir. Şifre çözümlemeye başlarken tam odaklanmak için rahatsız edilmeyecek bir ortamda kesin bir zihinle çalışılması gerektiğini ifade etmiştir. Şifreli metindeki sembollerin sınıflandırılıp sıralamanın bu sürecin bel kemiğini oluşturduğunu belirterek ' ve J harflerini ortaya çıkarmanın çözümlemeyi büyük oranda kolaylaştırdığını vurgulamıştır (Alam ve diğerleri, 2007: 56).

Yazar ikinci bölümde, ' harfi için iki ayrı sembol kullanılarak hazırlanan şifrelerden bahsetmiştir. Daha önce vermiş olduğu çözümleme teknikleri ile şifre hala çözümsüz kalıyorsa ' harfinin iki ayrı sembolle şifrelenmiş olabileceğine karşı uyarıda bulunmuştur. Yazar bu şekilde hazırlanmış şifreler için aşağıdaki yorumlarda bulunmuştur:

Eğer şifreli metin 30 sembolden oluşuyor ve önceki çözümleme tekniklerine yanıt vermiyorsa ' harfinin iki ayrı sembolle temsil edilmiş olabileceği göz önünde bulundurulmalıdır. Bu durumda ' harfinin peşine düşmektense J harfi tespit edilmeye çalışılmalıdır. Böyle bir şifrede, J harfini temsil eden sembolün tüm sembollerden daha fazla kullanıldığı görülecektir. J harfi ile kullanılan semboller göz önünde bulundurularak الله kelimesinin tespit edilmesi, ' harfini temsil eden semboller ortaya çıkarmaya yardımcı olacaktır (Alam ve diğerleri, 2007: 58).

Yazar, sembol sayısının 30'dan fazla olduğu şifreleri de üçüncü bölümde ele almış ve aşağıdaki yorumlarda bulunmuştur:

Eğer şifreli metindeki sembollerin sayısı 30'dan fazla ve kullanım sıklıkları birbirine yakın ise, ١ harfi gibi ٢ harfinin de iki ayrı sembolle temsil edilmiş olabileceği ve böylece şifreli metnin zayıf noktalarının bulanıklaştırıldığı düşünülmelidir. Bu durumda başka bir teknik aranmalı ve tesadüfen ortaya çıkmadıkları sürece ١ ve ٢ harfleri tespit edilmeye çalışılmamalıdır. Bu iki harfe odaklanmak yerine bulunma sıklığı ١ ve ٢ harflerinden sonra gelen bir sembol tespit edilmeli ve bu sembolün ه, و, ن, م ve ي harflerinden biri olduğu varsayılmalıdır. Tahmin edilen harfin çevresiyle uyum sağlayıp sağlamadığı kontrol edilerek, sırayla şifre boyunca bulunduğu yerlere yerleştirilmelidir. Anlamlı ifadeler ortaya çıkarsa sıradaki sembollerle devam edilmeli eğer çıkmazsa sıklığı yüksek olan bir sonraki harf, aynı sembol için tüm metin boyunca kontrol edilerek tekrar denenmelidir (Alam ve diğerleri, 2007: 60).

Yazar dördüncü bölümde tesadüf dışında çözülemeyecek gibi görünen, şifreyi yazan kişilerin muhtemel ihmallerinden kaynaklanan veya kasıtlı olarak gizemli kalması için planlanan şifre türlerine odaklanmıştır. Yazara göre, eğer şifre tüm çözümleme tekniklerine karşı açığa çıkmayacak kadar kapalı kalırsa, bu şifrenin bir tesadüf olmadıkça çözümlenmeyeceği sonucuna varılmalıdır. İki kişi arasında sıkı bir şekilde iletilen her şifreli mesajın, üçüncü bir şahıs tarafından mutlaka ortaya çıkarılacağına dair bir kaidenin olmadığına değinen yazar, özellikle her harf için birden fazla sembolün kullanıldığı şifreli metinlerde ne kadar çok emek harcanırsa harcansın şifrenin çözümlenmesinin imkânsız hale geleceğini ifade etmiştir. Öte yandan yazar, bazı mesajların çözümlenmesindeki gecikmenin ciddi sonuçlara yol açabileceğinin farkında olunmasını da istemiştir. Bununla ilgili olarak mesajın, bir savaş zamanı ordu komutanı tarafından, devlet yöneticisine acil askeri destek talebiyle iletildiği düşünülürse, ihtiyacın karşılanmasındaki herhangi bir gecikmenin yenilgiye sebep olabileceği örneğine dikkat çekmiştir (Alam ve diğerleri, 2007: 62).

Devamında ilk bakışta kolay gibi görünen ancak çözümlenmesi zor olan bazı şifrelere değinmiştir. Bu şifrelerde ١ ve ٢ harfleri yerine üçer farklı harf kullanılırken ث, ت, ب gibi noktasız, haliyle aynı yazılan harfler de ortak bir harf altında birleştirilerek temsil edilmektedirler. Böylece açık metindeki harflerin sayısı ile şifreli metindeki harflerin sayısı eşitlenmiş olacak ve alfabedeki tüm harfler kullanıldığı için şifrenin basit yerine koyma yöntemi ile hazırlanmış olabileceği düşüncesi oluşacaktır. Bu şekilde oluşturulmuş bir şifreli metinde sadece ١ takısı için bile dokuz farklı kombinasyon

bulunduğundan, şifre çözümlenmeye çalışıldığında içinden çıkılması zor bir hale gelecektir. Bulunma sıklıkları yüksek olan harflerin, sıklık oranlarının düşürülüp diğer harflere yakın hale getirildiği bu tür şifreler için frekans analizi yönteminin uygulanması ciddi zorluklara neden olacaktır. Yazarın bu kısımda bahsettiği, sık kullanılan harflerin birkaç harfle temsil edilerek bulunma sıklıklarının diğer harflerle birbirine yakınlaştırılması, şifrelerin açığa çıkmasını zorlaştırmak adına oldukça kayda değer bir özelliktir. Yazarın da söylediği gibi bu yöntem, tüm harflerin kullanılmasından dolayı şifreyi çözmeye çalışan kişiyi, şifrenin kolay bir yöntemle oluşturulduğuna dair yanılgıya düşürecek ve kafasının karışmasına neden olacaktır. İbn Duneynîr daha sonra yazarın bu satırlarına atıfta bulunarak yazımı benzer olan harflerin ortak bir harf altında temsil edilmesini, anlam belirsizliğine yol açacağı için bu yöntemi onaylamadığını ifade etmiştir (Alam ve diğerleri, 2007: 64).

Yazar alfabedeki harfleri, bulunma sıklıklarına göre yüksek, orta ve düşük olmak üzere üç ayrı kategoriye ayırdığı ek ile b risalesini tamamlamıştır. Yazarın kendisinden daha sonra yaşadığı tahmin edilen İbn ‘Adlân’ın da harflerin bulunma sıklıklarını aynı şekilde üç kategoriye göre ayırması dikkat çekmektedir (Alam ve diğerleri, 2007: 66).

BÖLÜM II

ON ÜÇ VE ON DÖRDÜNCÜ YÜZYILLARDA İSLAM MEDENİYETİNDE KRİPTOLOJİNİN GELİŞİMİ

2.1. ON ÜÇ VE ON DÖRDÜNCÜ YÜZYILLARDA İSLAM MEDENİYETİNİN GENEL DURUMU

İslam medeniyetinin 13. ve 14. yüzyıllarını kapsayan dönemi, siyasi tarihin en karışık dönemlerinden biri olarak karşımıza çıkmaktadır. Bu dönemde Haçlı kuvvetlerinin yanı sıra Moğol istilasının oluşturduğu istikrarsız ortam İslam kültür ve medeniyetini olumsuz yönde etkilemiştir. Moğollar 52 sene gibi kısa bir sürede Karakurum'dan başlayarak Anadolu ve Avrupa'ya varan bir istila süreci gerçekleştirmişler, bu süreçte Hârizmşahlar, Anadolu Selçuklular ve Abbasiler gibi önemli devletleri mağlup ederek İslam topraklarının büyük çoğunluğunu ele geçirmişlerdir (Açıl, 2019: 35).

Böyle kritik bir dönemde Memlukler, iktidarı ele geçirip Mısır'da ayrı bir devlet olarak ortaya çıkmış ve iki ayrı taraftan gelen Haçlı ve Moğol saldırılarını bertaraf etmişlerdir. Böylece Irak bölgesindeki siyasi ve kültürel üstünlük Memlukler sayesinde Mısır ve Suriye'ye geçmiştir (Özgüdenli, 2020: 225-229). Memlukler dönemi, bilimsel çalışmalar bakımından İslam medeniyetinin en parlak dönemlerinden biri olarak kabul edilmektedir. Gerek Haçlı gerek Moğol istilasını altında olan pek çok âlim, Memluklerin hakimiyeti altında bulunan bölgelere sığınmıştır. Devlet idarecilerinin de ilmi çalışmaları desteklemesi, Kahire ve Şam'ın iki önemli bilim merkezi haline gelmesini sağlamıştır (Yiğit, 2004: 90-97). Bu dönemde dinî ve pozitif ilimlerin gelişmesi için eğitim-öğretim kurumları inşa edilmiş, talebelerin tüm ihtiyaçları karşılanmış ve hocalara maddi destek sağlanmıştır (Keleş, 2010: 151-152). Öyle ki Memlukler dönemi “ansiklopediler çağı” olarak da bilinir hale gelmiştir (Yiğit, 2004: 90-97).

Diğer taraftan Moğolların bir kısmının Hülâgu liderliğinde 1256 senesinde Ceyhun Nehri'ni aşıp Horasan'a girmesiyle başlayan ilerleyişi Azerbaycan, İran, Irak ve Anadolu topraklarının bir bölümünü kapsayan İlhanlı devletinin kurulması ile sonuçlanmıştır. (Haykıran, 2015: viii) Moğolların başından beri uyguladıkları istila ve tahrip hareketleri İlhanlı devletinin kurulmasıyla bir durulma devresine girmiştir (Haykıran, 2015: 65).

Bununla beraber yapılan arařtırmalar, İlhanlıların pek çok medrese ve mescidin tamirini saęlayarak eęitim faaliyetlerini devam ettirme gayretinde olduklarını göstermektedir. Hülâgü Han ile bařlayan imar süreci, ardından gelen dięer hükümdarlar ile artarak devam etmiř ve Gâzân Han ile zirveye ulařmıřtır (Haykıran, 2015: 97)

Bu dönemde yapılan en önemli adımlardan biri Merâğa rasathanesinin kurulması olmuřtur. Nasîrüddin Tûsî'nin (ö.1274) Hülâgu'dan aldıęı maddi destekle kurduęu bu rasathane, gözlem aletlerinin çeřitlilięi, çalışan âlimlerin sayısı ve üstünlüęü bakımından önceki kurulanlardan daha üstün olduęunu göstermektedir (Bakkal, 2019: 121). Tûsî'nin *Zîc-i İlhanî* adlı meřhur eseri de 12 yıl boyunca burada yapılan gözlem ve hesaplamalar neticesinde yazılmıřtır (Unat, 2013: 399). Tusî, aynı zamanda İslam medeniyetinin çeřitli bölgelerinden getirttięi kitapları toplayarak rasathane iesinde büyük bir kütüphane de kurmuřtur. Rasathane, sadece astronominin deęil akli ve nakli ilimlerde de alıřmaların yürütüldüęü bir kurum haline gelmiřtir. Burada çalışan âlimler arasında Kutbüddîn-i řîrâzî, Necmeddin Ali b. Ömer el-Kâtibî, Müeyyidüddin el-Urdî ed-Dımařkî, Fahreddîn el-Merâęî, İbn Ebü'ř řükr el-Kurtubî ve Fahreddîn el-Ahlâtî gibi isimler bulunmaktadır (řirinov, 2012: 437-442).

Bu dönemde İslam coęrafyasının dięer bölgelerinde de astronomi, tıp, matematik, optik, coęrafya, kimya, kartografya alanlarında aktif alıřmalar yürütülmüř ve özgün eserler ortaya konmuřtur.²⁰ Bununla birlikte bu dönemde yařanan veba salgınına da ayrıca deęinmek faydalı olacaktır. Salgınların, yoğun nüfus kaybı ile psikolojik, sosyal ve ekonomik açıdan çeřitli yıkımlara sebep olduęunun göz önünde bulundurulması, yapılan alıřmaların deęerini daha açık bir řekilde ortaya koymaktadır. Kısaca dönemin tüm siyasi alkantılarına ve sonucunda getirmiř olduęu hastalık ve kıtlık gibi hayati sorunlarına raęmen 13. ve 14. yüzyılların, bilimsel gelişmeler açısından önceki yüzyıllardan devralınan disiplinlerin sistemli bir hale getirildięi ve yeni bilimsel atılımların devam ettięi bir dönem olduęunu söyleyebiliriz (Sezgin, 2015: 42 ve 53).

Dönemin řifreleme yöntemlerine baktıęımızda ise önceki dönemlerden devralınan uygulamaların çeřitlendirilerek geliştirildięi görülmektedir. Öncelikle sayıların kullanımının oldukça yaygınlařtıęı ve özellikle harflerin ebced sistemindeki sayısal deęerlerinin farklı yöntemler ierisinde kullanılarak pratik bir hale getirildięi görülmektedir. Bununla birlikte bu sayısal deęerlere çeřitli aritmetik işlemler

²⁰ Ayrıntılı bilgi iin bkz. Sezgin, 2015: 41-64.

uygulanarak şifreleme yapılması da ayrıca dikkat çekmektedir. Bu dönemde uygulanan yöntemlerde dikkate değer bir diğer unsur, İbn Duneynîr'in önerdiği şekliyle harflerin sayısal değerlerinin bir astronomi metni içerisine uyarlanması yöntemidir. Yöntemin uygulanması için astronomi ve aritmetik bilgisinin gerekli olduğunu belirtmesi ise astronominin bu dönemde gelişip yaygınlaşmasının bir yansıması olarak görülebilir.

Daha önce A ve B'nin yazarında çok kısıtlı bir şekilde gördüğümüz metin steganografisinin kullanımı, bu dönemde İbn Duneynîr ve İbnu'd-Dureyhim tarafından pek çok alternatif sunularak farklı şekillerde uygulanmıştır. Özü itibari ile mesajın kurgulanarak başka bir metin içerisine yerleştirilmesine dayanan bu yöntemin, oldukça geliştirildiği görülmektedir. İslam medeniyetine mensup önceki müellifler tarafından ele alınmayan teknik steganografi ise bu dönemde karşımıza çıkmaktadır. Bu yöntemde araç olarak satranç tahtası, delikli tahta, renkli boncuklar, katlanmış kâğıt ve parmak işaretleri kullanılmıştır. Buna ek olarak uygulanması her ne kadar basit yerine koyma yöntemine dayansa da İbnu'd-Dureyhim'in dallı alfabe yöntemi ile yeni bir alfabe oluşturması ve harfler yerine sembolik resimlerin kullanılabileceğinden bahsetmesi de diğer dikkat çekici yöntemler arasındadır. Son olarak İbn 'Adlân'ın kelimeler arasındaki boşlukların şifrelenmesi ve tespit edilmesini ayrıntılı bir şekilde ele alması, bu dönemde boşluksuz şifrelemenin yaygın bir şekilde kullanıldığına işaret etmektedir.

Sonuç itibari ile bu dönemde basit şifreleme yöntemlerinin daha detaylandırıldığı, birleşik şifreleme yöntemlerinin ise yenilerinin eklenerek geliştirildiğini söyleyebiliriz.

2.2. KRİPTOLOJİDE ÖNE ÇIKAN İSİMLER

2.2.1. İbn 'Adlân

'Afîf al-Dîn 'Alî ibn 'Adlân ibn Hammâd ibn 'Alî al-Mavşilî al-Nahvî al-Mutarcim 583/1187 senesinde Musul'da doğmuş ve eğitimini Bağdat'ta almıştır. Aralarında Ebu'l-Beķā el-Ukberî'nin de bulunduğu bazı hocalardan söz dizimi kurallarını öğrenmiştir. Eğitiminden sonra -aynı zamanda vefat ettiği yer olan- Kahire şehrindeki Salih Camii'nde bir süreliğine Arapça dersleri vermiş ve birçok öğrenci yetiştirmiştir. Zekâsıyla ünlü İbn 'Adlân, büyük bir şair olmasının yanında edebiyat alanında da önde gelen isimler arasında kabul edilmektedir. Bu alandaki kapsamlı bilgisinin onu şifre çözümü alanında birden

fazla eser vermeye uygun hale getirdiği düşünülmektedir. 666/1268 senesinde vefat ettiği düşünülen İbn ‘Adlān, seksen yıldan fazla süren ömründe, parıldayan zekâsı, söz dizimdeki kapsamlı bilgisi ve şifre çözümlemedeki ustalığı ile öne çıkmıştır. Buna rağmen kaynaklarda kendisine atfedilen kitapların sayısı yalnızca üç ile sınırlandırılmaktadır. Ancak bu teze konu olan *el-Mu’ellef lil-malik el-Eşref* isimli eserinin 20. kuralında referans olarak verdiği *el-Mu’lem* isimli kitabının bilinen kaynaklarda geçmemesi, İbn ‘Adlān’ın bazı eserlerinin kayıp olduğunu düşündürmektedir (Alam, Mrayati ve at-Tayyan,2003a: 13).

İbn ‘Adlān’ın bilinen çalışmaları aşağıdaki gibidir;

- 1- *al-intihāb li-keşf el-abyāt el- müşkilāt el-i ‘rāb.*
- 2- *‘uqlat el-muctāz fī ḥall el-alcāz.*
- 3- *el-Mu’ellef lil-malik el-Eşref.*
- 4- *el-Mu’lem.*

2.2.1.1. Eseri

İbn ‘Adlān’ın şifre çözümleme ilkelerini anlatmak amacıyla ele almış olduğu *el-mu’ellef lil-malik el-Eşref fī ḥall al-taracim* isimli eseri, giriş, 20 kural ve sonuç bölümü olmak üzere üç ana bölümden oluşmaktadır. İbn ‘Adlān eserini, Şam emiri Ebu’l-Feth el-Meliku’l-Eşref Muzafferuddîn Mûsâ b. el-Meliki’l-Âdil Muhammed b. Eyyûb’e (ö. 1237) ithaf ettiğini ifade etmiştir (Alam ve diğerleri, 2003a: 36).

İbn ‘Adlān eserin giriş bölümünde, şifre çözümleme uzmanının araçlarını; zekâ, sağduyu, uyanıklık, dil bilimi bilgisi, söz dizimi bilgisi, biçim bilimi bilgisi, deyim bilgisi, ölçü ve kafiye bilgisi, harflerin bulunma sıklıklarının bilgisi, birleşen ve birleşmeyen harflerin bilgisi, en az ve en sık kullanılan kelimelerin bilgisi, sık kullanılan iki ve üç harfli kelimelerin bilgisi, başlangıç ifadeleri ile onursal unvanların bilgisi, kelime boşlukları ve şifreleme yöntemlerine aşina olma şeklinde sıralamıştır (Alam ve diğerleri, 2003a: 40). Ardından basit yerine koyma ve yer değiştirme yöntemlerini kısaca tanıtmıştır. Yerine koyma yöntemi için bir tanesi sembol, iki tanesi harflerle hazırlanmış olan toplam üç tane şifre alfabesi örneği vermiştir. Özellikle sembolle oluşturulan alfabelerin örnekleri, diğer eserlerde yeterince anlatıldığı için daha fazla detaylandırmayacağını ifade etmiştir (Alam ve diğerleri, 2003a: 42-44).

İbn ‘Adlān eserin ikinci bölümde şifre çözümleme yöntemlerini aşağıda belirtildiği şekilde 20 kural altında ele almıştır. Birinci kuralda harfler, sık kullanılanlar, yaygın olarak kullanılanlar ve nadir olarak kullanılanlar olmak üzere üç kategoriye ayrılmıştır. Her kategorideki harfler de kendi aralarında azalan sıraya göre aşağıdaki şekilde sıralanmıştır (Alam ve diğerleri, 2003a: 48).

Tablo 1: İbn ‘Adlān’a Göre Harflerin Bulunma Sıklıklarının Gruplandırılması

Bulunma Sıklığı	Harfler
Yüksek	ن، ي، و، ه، م، ل، ا
Orta	ج، ح، ق، س، د، ك، ب، ت، ف، ع، ر
Az	ظ، غ، ط، ز، ث، خ، ض، ش، ص، ذ

İkinci kuralda ise sık kullanılan iki ve üç harfli kelimelerin kullanım sıklıkları azalan sıraya göre aşağıdaki gibi sıralanmıştır (Alam ve diğerleri, 2003a: 50).

İki harfli sık kullanılan kelimeler:

يا، لو، أو، هي، (son ikisi eşit bulunma sıklığına sahip) قد، عن، لم، في، ما، أن، إِنْ، مَنْ، مِنْ، لا
(Son ikisi eşit bulunma sıklığına sahip) ذَا كي، رَبِّ، ذو، كِي، ثم، إذ، هم،
مُدْ، هُنْ، وا (son dördü eşit bulunma sıklığına sahip)

Üç harfli sık kullanılan kelimeler:

عَمَّا، متى، كما، إذا، لَمَّا، أَمَّا، يَهَا، لَهَا، أَنَا، عَلَى، إِلَى

Üçüncü kuralda çözülecek şifreli bir metnin uzunluğunun en az 90 harf olması gerektiğini belirtilmiş ve şifreli bir metnin nasıl yorumlanması gerektiğini anlatılmıştır. İbn ‘Adlān’a göre, ilk olarak metindeki sembollerin sınıflandırılmaları ve bulunma sıklıklarına göre ayrılmaları gerekmektedir. Sonra bulunma sıklığı yüksek olan harfler, sık kullanılan iki ve üç harfli kelimeler için anlamlı hale gelene kadar tek tek denenmelidir. Eğer bu harflerle kendi içinde ve çevresiyle anlamlı bir kelime oluşmaz ise bulunma sıklığı orta olan harflere geçilmeli ve sırayla bu harfler denenmelidir. Ancak bu harf grubunda, ikinci tekil şahısla kullanıldıklarında kullanım sıklıkları artan ت ve ك harflerine öncelik verilebilir. Eğer bu harf grubuyla da istenilen sonuç elde edilemezse bu sefer az sıklıkta kullanılan harflere başvurulmalıdır (Alam ve diğerleri, 2003a: 52-56).

Dördüncü kural ise şifreli metinlerdeki boşluklara ayrılmıştır. Şifreli metinde boşluğun çözülmesi iki şekilde yapılabilir. Bu durumda ya metinde en çok tekrar eden sembol tespit edilmeli, ya da kelimelere sınır koyan semboller gözlemlenmelidir. Bu aşamada kelimelerin başında ve sonunda bulunabilen harflerin bilgisine hâkim olunması gerekmektedir. Bununla birlikte kelimelerin içerisine bilerek ya da yanlışlıkla konulmuş boşluklara da ayrıca dikkat edilmelidir (Alam ve diğerleri, 2003a: 58).

Beşinci Kuralda belirlilik takısı olan ال’in çözülmesi ele alınmış ve bu kuralın şifre çözmede önemli bir ipucu olduğu vurgulanmıştır. Şifreli bir metinde boşluklar belirlendikten sonra kelimelerin başında sıklıkla kullanılan iki sembol gözlemlenirse, bunlar ۱ ve ۲ harfi olarak varsayılabilir.

Ancak şifrede boşluk kullanılmamış ise ﺍﻝ takısını bulmak için ikinci kuralda sıralaması verilen iki harfli kelimelerin göz önünde bulundurulması gerekmektedir. İbn ‘Adlān bu noktada ﺍﻝ takısının tek bir sembol olarak şifrelenmesine de değinmiş ve bu şekilde hazırlanmış bir şifrenin çözülmesinin daha zor bir hale geleceğini ifade etmiştir. Bu durumda kelimelerin başında sıklıkla tekrar eden tek bir sembol aranması ve anlamının önceki ve sonraki bağlam ışığında tahmin edilmeye çalışılması gerektiğini belirtmiştir (Alam ve diğerleri, 2003a: 60-62).

Altıncı kuralda, belirlilik takısı olan kelimelerin sayısal tanımı üzerinde durulmuştur. Belirlilik takısı bulunan bir kelime, son harf ﻱ olmadığı sürece, bu kelimenin belirlilik takısı dışında en az iki olmak üzere çoğunlukla yedi veya sekiz harften oluştuğu belirtilmiştir. Nadir kullanılan ve daha fazla harften oluşan kelimelere de örnek verilerek bu bilgilerin metindeki boşlukları tespit etmede oldukça faydalı olduğuna değinilmiştir (Alam ve diğerleri, 2003a: 64).

Yedinci kuralda, kelimenin başında belirlilik takısından önce gelen harfin و ve ب ك ف harflerinden biri olmak zorunda olduğu üzerinde durulmuş ve bu harflerin sadece tek olarak değil, herhangi ikisinin beraber olarak da belirlilik takısından önce gelebileceğine dair örnekler verilmiştir (Alam ve diğerleri, 2003a: 66).

Sekizinci kural, şifre çözme için önemli ipuçları sunan başlangıç ifadeleri ve onursal unvanlar ile ilgilidir. İbn ‘Adlān bu kuralın bahsedilmesi gereken ilk kural olması gerektiğini ancak unuttuğu için ancak sekizinci kuralda ele alabildiğini ifade etmiştir (Alam ve diğerleri, 2003a: 66).

Dokuzuncu kuralda, bazı kelimelerin başında bulunan وﺍ, ﺑﺎ ve ﻛﺎ harflerinin ﺍﻝ takısı ile karıştırılmaması adına farkındalık oluşturulmak istenmiştir (Alam ve diğerleri, 2003a: 68). Onuncu kural ise sonu ﻝ ile biten bir kelime tespit edildiğinde bir önceki harf için ﺍ ve ﺋ harflerine öncelik verilmesi gerektiği ile ilgilidir (Alam ve diğerleri, 2003a: 70).

On birinci kuralda, art arda gelen ya da arasına bir veya iki harf alarak tekrar eden harflerden oluşan kelimelere örnekler verilmiştir. Bu tür olasılıklara aşina olmanın şifreli metni çözmede kolaylık sağlayacağını ifade eden İbn ‘Adlān, bu konuya daha detaylı olarak el-İmam el-Mustansır için yazdığı el-Mu‘lem adlı eserinde yer verdiğini söylemiştir (Alam ve diğerleri, 2003a: 72-78). On ikinci kuralı boşluk bulunmayan şifreli metinlerin çözümlenmesine ayıran İbn ‘Adlān, okuyucusundan ilk olarak metnin yeterli uzunlukta olduğundan emin olmasını istemektedir.

İbn ‘Adlān şifreli metindeki sembol sayısı ile o dilin alfabesinin harf sayısının eşit olması durumunda, boşluk kullanılmadan bir şifreleme yapıldığı kararına varılabileceğini belirtmiştir. Bu çalışmaya konu olan müellifler arasında boşluk kullanılmadan hazırlanmış şifreleri ayrı bir başlık altında ele alıp detaylandıran tek kişi İbn ‘Adlān olmuştur. Bunun yanında İbn ‘Adlān’ın boşluğun daha kolay tespit edilebilmesi için ث harfi dışındaki tüm harflerin ardışık olarak kaç kez tekrar edebileceğine değinmesi kendisinin Arap dilindekiengin bilgisini göstermektedir (Alam ve diğerleri, 2003a: 80-84).

On üç ve on dördüncü kuralda, kişiyi birçok zihin işinden kurtaracağı ifade edilen kelimenin başında ve sonunda iki kez tekrar eden harfler hakkında bilgi verilmiştir (Alam ve diğerleri, 2003a: 86).

On beşinci kuralda ise özellikle boşluk kullanılmadan hazırlanmış şifreli metinlerde anlam bulanıklığına sebep olabilecek olan tekrar eden hecelerden oluşan kelimelere değinilmiştir. On altıncı ve on yedinci kuralda, şiirsel şifrelerin çözülmesi ile kafiye konusunu ele alınmıştır (Alam ve diğerleri, 2003a: 88-98).

On sekizinci kuralda, İbn ‘Adlān’ın şifre çözümleme adımlarını daha detaylı bir şekilde okuyucusu ile paylaştığı görülmektedir. İlk olarak şifre çözümlemenin zorlu bir iş olduğunu hatırlatarak giriş yapan İbn ‘Adlān, şifreli metinde öncelikle iki, üç ve dört harfli kelimelerin ortaya çıkarılması gerektiğini söylemiştir. Bunun için üçüncü kuralda bahsetmiş olduğu gibi kelimenin ilk harfi bulunduktan sonra ikinci harfin yerine kullanım sıklıklarına göre sırayla diğer harfler konulmalı ve anlamı kontrol edilmelidir. Üç ve dört harfli kelimeler için de daha önce bahsettiği ipuçları uygulanmalı ve hâlihazırda çözümlenmiş olan harflerle uyuşup uyuşmadığı da göz önüne alınarak bu kelimeler ortaya çıkarılmaya çalışılmalıdır (Alam ve diğerleri, 2003a: 100).

İbn ‘Adlān on dokuzuncu kuralda, kelimelerin sonunda bulunan ﻯ harfine değinmiştir. Özellikle şimdiki zaman fiillerinde ﻯ harfi bol miktarda kullanıldığı için şifreyi çözerken bu harfin ﻱ harfi ile sıklıkla karıştırılabileceğine dikkat çekmiştir (Alam ve diğerleri, 2003a: 102). İbn ‘Adlān son kural olan yirminci kuralda ise şifre çözümlemeye dair genel tavsiyelerde bulunmuştur. Şifreyi çözecek olan kişinin, şifreyi hazırlayan kişinin uzmanlık derecesini ve mesajın yazılma amacını da tespit etmeye çalışmasının önemli olduğunu belirtmiştir. Böylece şifreyi çözmeye çalışan kişi, şifreyi hazırlayan kişinin uzmanlık derecesi ile orantılı olarak karmaşık olasılıkların arttığını varsayacak ve aynı

şekilde şifreye karşı daha uyanık olacaktır. Şifrenin yazılma amacının anlaşılması ise o bağlama uygun çağrışımları ortaya çıkarıp ayrıntıları yakalamayı kolaylaştıracaktır (Alam ve diğerleri, 2003a: 102).

İbn ‘Adlān bu eseri özet niteliğinde hazırladığını ve bu nedenle bazı çözümleme yöntemlerine yer vermediğini belirtmiş meraklısını da bu yöntemleri detaylandırmış olduğu el-Mu‘lem adlı kitabına yönlendirmiştir. Buna rağmen bu kısalıktaki bir eser için vermiş olduğu bilgiler İbn ‘Adlān’ın kapsamlı dil bilgisini göstermektedir. İbn ‘Adlān uzman olmayan kişilere boş olarak görünecek şekilde, beyaz kâğıt üzerine şifreleme yapmaktan da bahsetmiş ancak bu tür ilginç şifrelemeleri ayrı bir çalışma altında ele almak istediğini belirtmiştir. Buradan yola çıkarak, İbn ‘Adlān’ın steganografi hakkında da bilgi sahibi olduğunu anlaşılmaktadır. İbn ‘Adlān eserin son bölümünde okuyucusuna örnek olması için 1229 yılında kendisi için şifrelenen bir metnin çözülmesine yer vermiştir. Şifrede her harf bir kuş türü ile temsil edilmiştir. İlk olarak şifredeki sembolleri saymakla işe başlayan İbn ‘Adlān daha sonra boşluğu ve diğer harfleri tespit etmeye çalışırken yaptığı yorumları okuyucusu paylaşmış ve eserini sonlandırmıştır (Alam ve diğerleri, 2003a: 104-112).

2.2.2. İbn Duneynîr

Hayatı hakkında fazla bilgi bulunmayan İbn Duneynîr el-Laḥmî, 583/1187 senesinde Musul’da doğmuştur. Tam ismi İbrāhîm ibn Muḥammed ibn İbrāhîm ibn ‘Alî ibn Hibat Allāh ibn Yūsuf ibn Naṣr ibn Aḥmed olup, Sultan Kābus ibn al-Munḍir ibn Ma’ al-Semā’nın oğlu olduğu bilinmektedir. Selāhaddîn Eyyûbî’nin oğlu el-Melik el-Zāhir Gāzî’nin (ö.1216) Halep valiliği döneminde yaşamıştır. Kendisini övgü ile andığı emir Asad ad-din Ahmed ibn Abdullah al-Muhrani ve Eyyûbî Sultanı Nasir ad-Din Muhammed ibn Eyyup için çalıştığı bilinmektedir. Suriye ve Mısır arasında seyahat etmiş ve orada bazı yönetici ve tanınmış kimselerden övgüyle bahsetmiştir. Hayatı 627/ 1229 senesinde Baniyas yakınlarında kendisine işkence eden Sultan al-Aziz Osman ibn al-Melik al-Adil sebebiyle son bulmuştur. Kaynaklara göre İbn Duneynîr şiir ve kriptoloji olmak üzere aşağıda gösterildiği gibi iki alanda eser vermiştir (Alam, Mrayati ve at-Tayyan, 2005: 3-4).

Şiir alanında kendi şiirlerinden oluşan Divan ile kafiye üzerine yazılmış olan *el-Kāfī fī 'ilm el-ḳavāfī* isimli eser olmak üzere iki eser yazdığı,

Kriptoloji alanında ise günümüzde kayıp olan *el-Şihāb el-necim fī 'ilm vaḍ' el-terācim* ile bu tezde ele alınan *Maḳāsīd al-fuṣūl el-mutercime 'an ḥall el-terceme* isimli eser olmak üzere iki eser yazdığı bilinmektedir.

2.2.2.1. Eseri

Maḳāsīd al-fuṣūl el-mutercime 'an ḥall el-terceme isimli eser toplam 66 bölümden oluşmaktadır. İlk 35 bölüm düzyazıdaki şifrelemeler, kalan 31 bölüm ise şiirsel şifrelemeler üzerine yazılmıştır. İbn Duneynîr eserinin giriş bölümünde, düz yazıdaki şifrelerin çözümlenmesine varsayımlarla ulaşıldığını ancak bu sanatı yöneten düzenli kurallar olduğundan, kişinin bu varsayımlara gelişigüzel olarak değil akıl yürütme ile ulaşması gerektiğini vurgulamıştır. Bu sanatta başarıya ulaşmak için harflerin bulunma sıklığına, birbirleri ile birleşip birleşmeme durumlarına ve eser boyunca ele alacağı şifre çözümlene yöntemlerine aşına olunması gerektiğini belirtmiştir. Bunların yanında bu sanatla uğraşan kişilerde zekâ, gözlem yeteneği, anlayış hassasiyeti, keskin bir sezgi gücü, iyi bir tahmin becerisi ve zihin dinginliği gibi yeteneklerin bulunması gerektiğine dikkat çekmiş aksi halde şifre çözümlenmeye yardımcı olan bu yöntemlerin hiçbirinden faydalanılamayacağına karşı uyarıda bulunmuştur (Alam ve diğerleri, 2005: 70-72). Eserinde Kindî'den oldukça faydalanan İbn Duneynîr, şifre çözümlene yöntemlerini Kindî gibi niceliksel ve niteliksel olmak üzere ikiye ayırarak niceliksel yöntemin harflerin bulunma sıklığına, niteliksel yöntemin ise harflerin birleşme ve birleşmeme özelliklerine dayandığını ifade etmiştir (Alam ve diğerleri, 2005: 72). İbn Duneynîr sesli harflerin kişiye zahmet vermeden, ağızdan hava ile çıktığından, konuşma seslerini temsil ettiklerini ve bu yüzden tüm dillerdeki en yüksek bulunma sıklığına sahip harfler olduklarını belirtmiştir. Fakat Arapçada ﺀ takısının yaygın kullanımından dolayı ﺀ harfinin, bulunma sıklığı en yüksek olan ﺀ harfinden hemen sonra gelerek ﺀ ve ﺀ sesli harflerini geçtiğini eklemiştir. Sessiz harflerin bulunma sıklıklarının ise her dile göre değişiklik göstereceğini ifade eden İbn Duneynîr, her dili ayrı ayrı ele alarak kitabı uzatmak istemediğini bu yüzden sadece Arap dili ile ilgili çözümlene algoritmalarından bahsedeceğini

açıklamıştır (Alam ve diğerleri, 2005: 74).²¹ İbn Duneynîr şifreleme yöntemlerini, Kindî gibi basit şifreleme ve birleşik şifreleme olmak üzere iki ana türe ayırmıştır. Basit şifreleme yöntemlerini Kindî'nin sınıflandırdığı biçimde ele alırken birleşik şifreleme yöntemleri için kendi açıklamalarını eklemiştir.

İbn Duneynîr şifreleme yöntemlerini aşağıdaki şekilde ele almıştır.

Harflerin şifrlenmesi, basit şifreleme ve birleşik şifreleme olmak üzere iki ana türe ayrılmaktadır. Basit şifreleme, harflerin şekillerinin değiştirildiği ve şekillerinin korunduğu iki prensiple uygulanabilmektedir. Harflerin şekillerinin değiştirilmesi de kendi içerisinde “ilişkilendirilerek değiştirme” ve “ilişkilendirme olmadan değiştirme” olmak üzere iki kısımdır.

İlişkilendirilerek değiştirme, harflerin bir kategori ismine ait isimler ile eşleştirilmesi şeklinde uygulanabilmektedir. İlişkilendirme olmadan değiştirme ise yer değiştirme ve yerine koyma yöntemi olarak iki kısma ayrılmaktadır. Basit şifrelemenin ikinci alt başlığı olan harflerin şekillerinin korunduğu yöntem ise harf ekleme, harf çıkarma, harf birleştirme ve harf ayırma olmak üzere dört ana şekilde uygulanmaktadır. Buraya kadar olan tüm yöntemlerin isimleri ve açıklamaları hemen hemen Kindî ile aynı satırları içermektedir (Alam ve diğerleri, 2005: 76-80). İbn Duneynîr devamında açıklamış olduğu basit şifreleme yöntemlerinin niceliksel ve niteliksel çözüm algoritmaları üzerinde durmuştur. İlk olarak şifre çözümlemeyi saygın bir bilim olarak değerlendiren İbn Duneynîr, bu bilimde başarıya ulaşmak için çok fazla alıştırma yapılması gerektiğine dikkat çekmiştir. Bunun yanında Kindî'nin harflerin bulunma sıklığı hesabını, üç sayfa metin üzerinden kontrol ederek doğruluğunu teyit ettiğini ifade eden İbn Duneynîr, Kindî gibi bu yöntemin şifreli metnin çok kısa olması durumunda güvenilir olmayacağını söylemiştir (Alam ve diğerleri, 2005: 86). Bu durumda birleşen ve birleşmeyen harflerin özelliklerinden yararlanılarak çözümleme yapılması gerektiğini belirtmiş ve bunun için harflerin olası kombinasyonlarını ele almıştır (Alam ve diğerleri, 2005: 88). İbn Duneynîr bu harf kombinasyonlarını hem başından hem sonundan birleşenler, sadece başından birleşenler, sadece sonundan birleşenler ve iki taraftan da birleşmeyenler olmak üzere

²¹ İbn Duneynîr kendisinin de belirttiği üzere diğer dillerin incelemesini ayrı olarak ele almasa da ilerleyen bölümlerdeki açıklamalarından Arapçanın yanında Türkçe, Latince ve Moğolca dillerini inceleyip, sıklık sıralarını hesapladığı anlaşılmaktadır.

dört gruba ayırmıştır. Bu özellikleri bir tabloda göstererek, (Alam ve diğerleri, 2005: 90) Kindî'nin fazlalık içeren anlatımını yeterli miktarda kısalttığını ifade etmiştir (Alam ve diğerleri, 2005: 94). İbn Duneynîr basit yerine koyma yönteminin çözümleme algoritmasını, diğer kitabı olan *el-Şihāb el-necim fî 'ilm vaḍ' el-terācim*'de detaylı olarak ele aldığı için bu eserinde yeniden açıklamaya gerek olmadığını belirtmiş (Alam ve diğerleri, 2005: 98) ancak frekans analizi yöntemini açıklarken bu yöntemin algoritmasına da değinmiştir. İbn Duneynîr'e göre, yerine koyma yöntemi ile oluşturulmuş bir şifreli metinle karşılaşıldığı zaman, öncelikli olarak metinde bulunan tüm semboller tespit edilip bulunma sıklıklarına göre sıralanmalıdır. Daha sonra o dilde bulunma sıklığı en fazla olan harf, metinde en çok kullanılan sembolle eşleştirilmeli ve bu eşleştirme tüm harfler bitene kadar devam ettirilmelidir. Metinde anlaşılır manalar ortaya çıkana kadar harf ve sembol kombinasyonları denenerek uygulanmalıdır.

İbn Duneynîr, diğer şifreleme yöntemleri için vermiş olduğu çözümleme ipuçlarını da aşağıdaki şekilde paylaşmıştır:

Harflerin yerlerinin çevresindeki harflere göre değiştirildiği bir şifrelemede, açık metni elde etmek için uyumsuzluğun gözlemlendiği yerlerde kelimenin doğru dizilişi bulunana kadar harflerin tek tek denenmesi gerekmektedir. Harflerin kendi açısına göre değiştirildiği şifrelemede ise harflerin açıları çevrilerek, şekilleri düzeltilmelidir. İbn Duneynîr bu şifreleme türünü algısal iç görüşü yüksek olan bir insanın kaçıramayacağı kadar basit olarak tanımlamıştır (Alam ve diğerleri, 2005: 100).

Eğer şifre gereksiz harfler eklenerek hazırlanmış ise sonradan eklenen harflerin bulunma sıklıkları normalin çok üstüne çıkacaktır. Bu durumda, bu harflerin sonradan kafa karıştırmak için eklendiği sonucuna varılmalıdır. Bu harfler metinden çıkarıldığında zaman, kelimeler anlam kazanıp ve konu bütünlüğü sağlanacaktır (Alam ve diğerleri, 2005: 102). Metindeki bazı harflerin çıkartılarak oluşturulan bir şifrelemede ise tüm sembollerin sayısının hesaplanması gerekmektedir. Eğer sembollerin sayısı alfabedeki harflerin sayısından daha az bulunursa bu yöntemin kullanıldığına karar verilmelidir. Bu durumda daha önce bahsedilen çözümleme yöntemleriyle harflerin bazıları ortaya çıkarılmalı ve metindeki yerlerine yerleştirilmelidir. Böylece anlam bütünlüğünden yararlanılarak kasıtlı olarak çıkarılan harfler tespit edilir (Alam ve diğerleri, 2005: 106). İbn Duneynîr harf birleştirme ve ayırma yoluyla yapılan şifreleme yöntemleri için ise herhangi bir çözümleme algoritması açıklamamıştır.

İbn Duneynîr bir sonraki bölümde, kendisinden şifreli bir mesajın çözülmesinin istendiğinden bahsetmiştir. İlk olarak, sembolleri sınıflandırdığını fakat bir sonuca ulaşamadığını aktaran İbn Duneynîr, mesajın basit şifreleme yöntemlerinin hepsi ile uyumsuz olduğunun farkına vardığını belirtmiştir. İçinden çıkılmaz bir hal aldığına, bazı karakterleri çıkartıp yeniden düzenlediğinde ise mesajın ancak ortaya çıktığını ifade etmiştir. Harflerin şekillerinin ve konumlarının değiştirildiği, aynı zamanda bazı gereksiz harfler de eklenerek hazırlanan bir şifrenin çözülmesinin oldukça zor olduğunu fakat Allah'ın yardımıyla sonuca ulaştığını belirtmiştir (Alam ve diğerleri, 2005: 104). İbn Duneynîr'in aktardığına göre bu şifrenin birden fazla basit yöntemin kombinasyonu ile uygulanan bir birleşik şifreleme türü olduğu anlaşılmaktadır.

Buraya kadar basit şifreleme yöntemlerini ve çözümü algoritmalarını ele alan İbn Duneynîr, bundan sonra birleşik şifreleme yöntemlerini ve çözümü algoritmalarını açıklamaya geçmiştir. İbn Duneynîr, Kindî'nin birleşik şifreleme yöntemlerini açıklamadığına atıfta bulunmuş ve kılavuz işlevi görmesi açısından kendisinin birkaç tane yönteme değineceğini ifade etmiştir (Alam ve diğerleri, 2005: 108). İbn Duneynîr'e göre, eğer bir şifre tüm basit şifre çözümü yöntemlerine karşı hala kapalı kalıyorsa, bu şifre birleşik şifreleme yöntemi ile hazırlanmış olmalıdır. Bu tarz şifrelerin en çetrefilli şifreler olduğunu düşünen İbn Duneynîr, yeterli uzmanlığa sahip olmayan kişiler tarafından çözülmesinin neredeyse imkânsız olduğunu belirtmiştir (Alam ve diğerleri, 2005: 110). İbn Duneynîr, bu başlık altında harflerin bir kategoriye ait isimlerle ilişkilendirilerek kurgulanmasını ele almış ve bu tür şifreleri çözülmemeye karşı meydan okuyan şifreler olarak değerlendirmiştir. Bu yöntem için alfabedeki her harfe karşılık gelen aynı ya da farklı kategorilere ait isimleri içeren bir liste sunmuştur. Bu listenin anlaşılana kadar tekrar edilerek çalışılması gerektiğini vurgulamış ve yöntemin daha iyi anlaşılması için *وَلِي التَّوْفِيقِ* ifadesini kurguladığı bir hikâye içerisine yerleştirerek şifrelemenin nasıl yapılacağını göstermiştir (Alam ve diğerleri, 2005: 110-114).

Eserde öne çıkan bir diğer kurgulamaya dayanan yöntem ise ar, dekar ve hektar gibi arazi ölçü birimlerini harflerin sayısal değerleri ile kullanarak, metne çiftçi ve köylü arasında geçen bir konuşma görüntüsü vermektir. İbn Duneynîr'in metnin köylü ve çiftçi arasında geçen olası bir konuşma gibi kurgulanmasını istemesi, mesajın herhangi bir şifre içerdiğine dair şüphe uyandırmaması açısından önemlidir. Bu kurgulamanın iyi yapılmadığı takdirde şifrenin açığa çıkmasını sağlayan belirgin bir ipucu verilmiş

olacağını da ayrıca eklemiştir (Alam ve diğerleri, 2005: 116). İbn Duneynîr başka bir bölümde, bu yöntemi biraz daha çeşitlendirerek her harf yerine haftanın belirli gün ve saatlerini (Alam ve diğerleri, 2005: 128) ve tam, yarım ve çeyrek dinar gibi parasal değerler konularak yapılan şifrelemelerden de bahsetmiştir (Alam ve diğerleri, 2005: 138). Harf yerine parasal değer koyma yöntemini kendisinden daha önce yaşadığı tahmin edilen A ve B'nin yazarı da eserinde yer vermiştir. Dolayısıyla İbn Duneynîr'in bu yöntemi eserinin başka bir bölümünde atıfta bulunduğu A ve B'nin yazarından almış olması muhtemeldir.

İbn Duneynîr bir başka bölümde ise harflerin ebced sisteminde denk oldukları sayısal değerlerin kullanılması ile şifreleme yapılabileceğinden bahsetmiştir. İlk olarak sayıların, sayısal olarak yazılışlarını tarif eden İbn Duneynîr, bu şekilde oluşturulmuş bir şifrenin çözümlenmesinin gayet kolay olduğunu ifade etmiştir (Alam ve diğerleri, 2005: 124). Bir sonraki bölümde bu yönteme bir aşama daha ekleyerek şifrenin zorluğunu artırmak istemiştir. Bu yeni yöntem, harflerin denk olduğu sayısal değerlere çeşitli çarpma işlemleri uygulayıp bu değerlerin tekrar harflere dönüştürülmesi ile şifrenin daha karmaşık bir hale getirilmesine dayanmaktadır (Alam ve diğerleri, 2005: 126). Yöntem, iki ayrı yerine koyma uygulanması ve aritmetik bir işlem içermesi bakımından oldukça dikkat çekicidir. İbn Duneynîr, harflerin ebced sisteminde denk oldukları değerlerin, parmak işaretleriyle temsil edilerek şifrenmesi hakkında da bilgi vererek, 1'den 11'e kadar olan sayıların gösterimini detaylı olarak tarif etmiştir. Bu sayede şifreli mesajın halihazırda bulunan kişiye el işaretleriyle iletilmesinin de mümkün olduğunu göstermiştir (Alam ve diğerleri, 2005: 118). İbn Duneynîr parmak işaretleri gibi kâğıt dışında başka bir araç kullanılarak yapılan şifreleme yöntemlerini çeşitlendirerek sırasıyla satranç tahtası, delikli tahta ve renkli boncuk gibi materyallerin kullanıldığı yöntemlerinden de bahsetmiştir. Bu yöntemlerin açıklamaları aşağıdaki gibidir:

Satranç tahtasının kullanıldığı şifrelemede, tahtanın her bir karesi bir harfe tahsis edilmektedir. Orada hazır bulunan kişinin göreceği şekilde, satranç taşı sırayla mesajın harflerine denk gelen karelere getirilerek mesajın iletilmesi sağlanmaktadır (Alam ve diğerleri, 2005: 120-122). Delikli tahta ile şifrelemede, öncelikle tahtaya alfabe'deki harf sayısı kadar delik açılması gerekmektedir. Bu yöntemde harfler alfabe'deki dizilişine göre sıralanabilir ya da yeniden düzenlenebilirler. Her iki durumda da şifrenmek istenen harf hangi sıradaki delikle bulunuyorsa ipin o sıradaki delikten geçirilmesi gerekmektedir. Bu

şekilde hazırlanmış bir şifreyi çözümlmek için ipliğin en son geçirildiği delikten ilk geçirildiği deliğe kadar gidilerek harfler tek tek yazılmalı ve tersten okuma yapılarak mesaj açığa çıkarılmalıdır (Alam ve diğerleri, 2005: 132). Bir araç kullanılarak oluşturulan bir başka şifreleme türü ise renkli boncukların kullanıldığı yöntemdir. Bu yöntemde alfabedeki harfler, belirli renkteki boncuklarla eşleştirilmektedir. Şifreleme yapılırken, metindeki harfleri temsil eden boncuklar aynı sırayla ipe dizilmektedirler. İbn Duneynîr, aynı renkteki boncukların farklı harfleri temsil etmesi için boncuklara ayırt edici işaretler eklenmesi gerektiğini belirtmiş fakat kelimeler arasındaki boşlukların nasıl ayırt edileceğine dair bir açıklamada bulunmamıştır. Yöntemin çözümlenmesi ise en fazla kullanılan renkteki boncukların sırayla alfabede en sık kullanılan harflerle eşleştirilmesiyle yapılmaktadır (Alam ve diğerleri, 2005: 134).

İbn Duneynîr, mesajı oluşturulan kelimelerin başka bir bağlam içerisine yerleştirilerek şifrelenmesine de değinmiştir. İletilecek mesajın kelimelerinin yeni oluşturulacak şifreli metnin belirli sıradaki kelimelerine denk gelecek şekilde yerleştirilmesinden veya iletilecek mesajın harflerinin tek tek alınarak, yeni oluşturulacak metnin kelimeleri içerisinde belirli bir sıraya göre yerleştirilebileceğinden bahsetmiştir (Alam ve diğerleri, 2005: 136). Tecrübeli kişiler tarafından çözümlenmesi çok zor olmayan bu yöntem iyi bir kurgu içerisinde sunulması dahilinde metnin herhangi bir şifre içerdiğine dair şüphe uyandırmaması açısından önemli görülmektedir.

İbn Duneynîr, bu çalışmaya konu olan diğer müelliflerden farklı olarak bir şifreyi gezegen ve diğer gök cisimlerinin durumları hakkında bilgi veren bir metin içerisinde iletmeyi de önermiştir. Bu yöntemde harflerin denk oldukları ebced değerleri sırayla metin içerisinde yerleştirilmektedir. İbn Duneynîr bu yöntemle şifreleme yapmak için kişinin aritmetik ve astronomi hakkında bilgi sahibi olması gerektiğini vurgulamıştır (Alam ve diğerleri, 2005: 140). Bu yöntemin, şifrenin bir kurgulamadan ziyade bilimsel bilgi veren bir metin gibi görünmesi de ayrıca önemlidir.

İbn Duneynîr, şifreleme yöntemleri içerisinde kâğıdın farklı bir kullanımına da yer vermiştir. Yöntem, kâğıdın pileli bir şekilde katlanmasına ve mesajın bu kıvrımlara yazılmasına dayanmaktadır. Böylece kâğıt açıldığı zaman mesaj, nokta ve çizgiler halinde görünecektir. Bu şüpheli görünümü ortadan kaldırmak için ise bu nokta ve çizgilerin tam harflere dönüştürülmesini teklif etmiştir. Bunun yanında yöntemin daha önce farklı bir konu hakkında yazılmış olan bir kâğıdın arka kısmına yazılarak da uygulanabileceğini

söylemiştir. Bu sayede kâğıt açıldığında ortaya çıkan nokta ve çizgiler, sayfanın ıslakken katlandığı için bu lekelerin oluştuğu görünümünü verecektir (Alam ve diğerleri, 2005: 130). İbn Duneynîr şiirsel şifrelemeleri ele aldığı kısımda düz yazıda yazılmış şifreler için de uygulanabilecek bazı ipuçları paylaşmıştır. Şifreli bir metinde ' ve ʾ harfinin tespit edilmesinin önemine özellikle değinen İbn Duneynîr birlikte sık kullanılan iki, üç ve dört harfli kelimelerin bilinmesinin şifre çözümleyiciye oldukça kolaylık sağladığını belirtmiştir (Alam ve diğerleri, 2005: 154). Bununla birlikte ʾ takısı ile sıklıkla kullanılan ve ardışık olarak tekrar eden harfler hakkında da bilgi vermiştir (Alam ve diğerleri, 2005: 166). Sonuç itibarıyla Kindî'den yaklaşık 300 sene sonra gelen İbn Duneynîr'in, Kindî'nin eserinden oldukça faydalandığı görülmektedir. Kindî'nin şifreleme yöntemleri sınıflandırmasını ve basit şifreleme yöntemleri açıklamalarını neredeyse hiç değişiklik yapmadan kullanmıştır. Bununla birlikte İbn Duneynîr, Kindî'den farklı olarak birleşik şifreleme yöntemini sadece tanımlamakla kalmamış çeşitlendirerek özgün örnekler sunmuştur. Özellikle mesajın istenmeyen kişi ya da kişiler tarafından ele geçirilmesi durumunda herhangi bir şifre içerdiği konusunda şüphe uyandırmayacak şekilde kurgu ile yapılan şifreleme yöntemlerini ele alması bu konudaki uzmanlığını göstermektedir. İbn Duneynîr'in şiirsel şifrelere de yaklaşık düzyazı şifreleri kadar yer ayırması yaşadığı zamanda şiirin düzyazı kadar yaygın bir şekilde kullanıldığına dair ipucu da vermektedir.

2.2.3. İbnu'd-Dureyhim

Asıl adı 'Alî ibn Muḥammed ibn 'Abd el-'Azîz, lakâbı Tâcu'd-dîn olan İbnu'd-Dureyhim 712/ 1312 senesinin Şaban ayında Musul'da doğmuş ve varlıklı bir yetim olarak büyümüştür. Aralarında Ebû Bekir b. Alemüddin Sencer el-Mevsilî, Zeynüddin ibn Şeyhü'l Uveyne, Şerefeddin Abdullah b. Yûnus, Alâeddin ibnü't-Türkmânî ve Şemseddin el-İsfahânî'nin olduğu bilinen dönemin önde gelen alimlerinden Kur'an, fıkıh, hadis, Arapça dil bilgisi dersleri almıştır (Kaya, 2000: 18-19). Belirli bir yaşa geldiğinde, babasının ardında bıraktığı, devlet yetkililerinin elinde bulunan mirasını devralmaya çalışmış ancak küçük bir kısmını geri alabilmiştir. Eline geçen bu parayı akıllı bir şekilde ticarete değerlendirmiş ve 1332 senesinde Mısır'a gitmiştir (Yarbrough, 2013: 139). Burada Memluk sultanlarıyla yakın ilişkiler kurduğu ancak sattığı bir mal karşılığında devletin kendisine 200.000 dirhem borçlandığı bilinmektedir. İbnu'd-Dureyhim'in bu

miktarı geri alma çabaları, el-Melikü'l-Muzaffer tarafından Şam'a sürülmesine ve kitaplarına el konulmasına sebep olmuştur (748/1347). Daha sonra Şam Emevî Camii'ne müderris olarak atanmış ve bir müddet çeşitli kurumlarda görev yapmıştır. Hayatının son on beş senesini Şam, Halep ve Kahire arasında geçirmek zorunda kalan İbnu'd-Dureyhim'in keskin bir zekâ ile kapsamlı bir bilgi birikimine sahip olduğu söylenmektedir (Kaya, 2000: 18-19). İbnu'd-Dureyhim'in arkadaşı olduğu bilinen Abdillâh es-Safedî (ö.764/ 1363) onun elli seneden kısa süren ömründe seksen civarında eser yazdığını ifade etmiştir. Bununla birlikte Safedî'nin listelediği eserlerin bizzat İbnu'd-Dureyhim'in kendi el yazısıyla yazdığı çalışmalar olduğunu belirtmesi de ayrıca önemlidir. Bu eserler arasında Kur'an-ı Kerim'deki surelerin fazilet ve sırları, hurûf-ı mukataanın yorumu, ibadetlerin sırları, miras hukuku hesapları, İncil ve Tevrat'ın tahrifi, Kahire'deki sinagogların yıkılması, satranç oyunu, şifreleme bilimi gibi farklı konular bulunmaktadır. Mısır'a geri döndüğü 760/ 1359 senesinde Sultan en-Nâsır Hasan tarafından Habeşistan'a elçi olarak görevlendirilmiştir. İbnu'd-Dureyhim'in istemeyerek çıktığı bu yolculuk, 762/1360 senesinde Kûs şehrine varınca vefatı ile sonuçlanmıştır (Alam, Mrayati ve at-Tayyan, 2003b: 3-4, Kaya, 2000: 18-19).

2.2.3.1. Eseri

İbnu'd-Dureyhim, *Miftāh el-Kunūz fî idāh el-marmūz* isimli eserine, şifrelerin formülleştirilmesi ve onların çözümlenmesi üzerine daha önce *idāh el-mubhem fî hall el-mutercem* isimli bir eser yazdığını²² ancak kopyasının elinde bulunmadığını, bu mevcut eserin ise kendisinden yazılması istendiği bu sebeple aklına gelen kurallara yer vereceğini belirterek giriş yapmıştır (Alam ve diğerleri, 2003b: 50).

Şifreli metinleri çözümlemenin çok değerli bir amaç olduğuna değinen İbnu'd-Dureyhim, bu bilim sayesinde eskilerin kitap ve diğer materyallerde miras bıraktıkları sembollerin anlaşılabilirliğini belirtmiş ve ihtiyaç anında bu bilimin vazgeçilmez olduğunu ifade etmiştir. Böyle değerli bir ilme sahip olabilmek için kişinin, çözümlemek istediği metnin dilini, o dilin dil bilgisi kurallarını ve o dilde en yüksek bulunma sıklığına sahip harflerin bilgisinin iyi derecede bilmesi gerektiğini belirtmiştir (Alam ve diğerleri, 2003b: 52). Bu

²² İbnu'd Dureyhim'in bahsi geçen bu iki eser dışında kriptoloji hakkında üç eser daha kaleme aldığı bilinmektedir. Ayrıntılı bilgi için bkz. Alam, Mrayati ve at-Tayyan, 2003b: 4.

noktada İbnu'd-Dureyhim Arapçanın yanında Latince, Ermenice, Moğolca, Türkçe, Farsça, İbranice, Süryanice, Antik Mısırca, Sümerce, Yunanca ve Eski Latince ve iki ayrı Hint alfabesi hakkında çeşitli bilgiler paylaşmış ve sadece Arapça üzerine değil yaşadığı dönemde önemli olan diğer diller üzerine de çeşitli çalışmalar yaptığını göstermiştir (Alam ve diğerleri, 2003b: 54).

İbnu'd-Dureyhim eserin konusuna, yazılış amacına, önemine ve bu bilimi elde etmek için bilinmesi gereken konulara değindikten sonra şifreleme yöntemlerini anlatmaya başlamıştır. Şifreleme yöntemlerini yer değiştirme, yerine koyma, harf ekleme ve çıkarma, çeşitli araçlar kullanma, sayısal alfabe kullanma, kelime kullanma, kategori isimleri ile ilişkilendirme ve sembol veya işaretler kullanma şeklinde aşağıdaki gibi sekiz ayrı başlık altında ele almıştır.

1. Yer değiştirme yöntemi ile şifreleme:

İbnu'd-Dureyhim metnin içerisinde yer alan harflerin yerlerinin belirli ölçütlere göre değiştirilmesini yer değiştirme yöntemi olarak tanımlamıştır. İbnu'd-Dureyhim'in bu yöntem için sunduğu alternatifleri tek kelime içerisinde, İki kelime arasında ve bir kelime grubu içerisinde uygulanabilecek yöntemler olmak üzere üç ana başlık altında incelemek mümkündür²³ (Alam ve diğerleri, 2003b: 56).

2. Yerine koyma yöntemi ile şifreleme:

Alfabedeki harf dizilişinin belirli bir kurala göre değiştirilmesi ile uygulanmaktadır. İbnu'd-Dureyhim yöntemin kurallarının düzenli ve düzensiz olmak üzere iki şekilde oluşturulabileceğinden bahsetmiştir.

- a. Düzensiz kural oluşturularak şifreleme: Şifrelenecek dilin alfabesindeki harflerin dizilişi düzenli bir kurala bağlı olmadan değiştirilir ve belirlenen bir usule göre birbirlerinin yerine konularak şifrelenir. 28 harfli bir alfabe için 28! kadar farklı alfabe oluşturmaya olanak sağlayan bu yöntem, İbnu'd-Dureyhim tarafından neredeyse sayısız şekilde şifre alfabesi oluşturmak mümkün denilerek ifade

²³ Ayrıntılı bilgi için bkz. Alam, Mrayati ve at-Tayyan, 2003b: 56-60.

etmiştir. Bunun yanında harflerin ebced dizilişinin kullanılabileceğine de değinmiştir (Alam ve diğerleri, 2003b: 60-62).

- b. Düzenli kural oluşturularak şifreleme: Şifrelenecek dilin alfabesindeki harflerin dizilişi düzenli bir kurala bağlı olarak değiştirilir ve belirlenen bir usule göre birbirlerinin yerine konularak şifrelenir. İbnu'd-Dureyhim bu kısımda harfleri bir daire etrafında dizilmiş olarak hayal etmiş ve yerine koyma uygulamasının, harflerin ayrı ya da çiftler halinde alınarak yapılabileceğini belirtmiştir. Böylece harfler belirlenen bir sıraya göre kendisinden önce veya sonra gelen harf ya da harf çiftinin yerine konarak şifrelenmektedir (Alam ve diğerleri, 2003b: 62-64).

3. Harf sayısının artırılması ve azalması yoluyla şifreleme:

Açık metindeki harflerin artırılması ya da azaltılması yoluyla uygulanmaktadır. İbnu'd-Dureyhim, belirli bir düzene göre metindeki harflerin tekrarlanması ya da çeşitli harflerin eklenmesi ile metnin karmaşık hale getirilebileceğinden bahsetmiştir. Bununla birlikte tam tersi bir yol izlenerek metindeki bazı harflerin çıkarılması ile de benzer şekilde kafa karışıklığı oluşturulabileceğini belirtmiştir. Bu çıkarma işlemi metindeki belirli kelimelerin tek tek çıkarılması gibi veya bazı harflerin tek bir harf altında temsil edilmesi olarak da uygulanabilmektedir. Bu harfler yazılışları itibariyle benzer olabilir ya da olmayabilirler (Alam ve diğerleri, 2003b: 66).

4. Şifre araçları kullanarak şifreleme:

Kâğıt dışında başka araçlar ile de şifreleme yapılabileceğinden bahseden İbnu'd-Dureyhim, ilk olarak satranç tahtası kullanarak şifreleme yöntemine değinmiştir. Yöntemde satranç tahtasındaki kareler sırayla alfabenin harflerini temsil etmektedir. Mesaj ise satranç taşının sırayla mesajı oluşturan harflerin karelerine denk gelecek şekilde yerleştirilmesiyle iletilmektedir. İbnu'd-Dureyhim'in bu başlık altında ele aldığı ikinci yöntem ise delikli bir tahta yardımı ile şifreleme yapmaktır. Yöntemde ilk olarak bir tahtaya alfabedeki harf sayısı kadar delik açılmalıdır. Daha sonra iplik, mesajın harflerini temsil eden tüm deliklerden sırayla geçirilerek şifrelenmelidir. İbnu'd-Dureyhim bu tür şifrenin çözümlenmesinin, sırayla ipliğin geçtiği deliklerin tespit edilmesiyle yapılacağını ifade etmiştir (Alam ve diğerleri, 2003b: 66-68). İbnu'd-Dureyhim şifreleme yöntemlerinin sonunda geldiğine bu başlığa tekrar dönerek iki yöntem daha eklemiştir.

Bu yöntemler, renkli boncuklar ve kâğıt katlama yöntemi ile yapılan şifrelemelerdir. Renkli boncuklar kullanılarak yapılan şifrelemede, harfler çeşitli renkteki boncukla temsil edilerek tıpkı bir tespih gibi mesajdaki harflerin sırasına göre ipe dizilirler. İbnu'd-Dureyhim ¹ harfinin sarı renkli boncuk ile, ب harfinin mavi renkli boncuk ile, ج harfinin kırmızı renkli boncuk ile, د harfinin yeşil renkli boncuk ile, ه harfinin koyu mavi renkli boncuk ile, و harfinin siyah renkli boncuk ile temsil edildiğini daha sonra aynı renkteki boncukların ikişer olarak kullanılmasından bahsederek, iki tane sarı renkli boncuğun ج harfini, iki tane mavi renkli boncuğun ب harfini temsil ettiğini ve bu düzenin iki siyah renkli boncuğun د harfini temsil etmesine kadar devam ettiğini açıklamıştır. Sonra boncukları üçer üçer alarak üç tane sarı renkli boncuğun ه harfini, üç tane mavi renkli boncuğun و harfini, üç tane siyah renkli boncuğun د harfini temsil ettiğini, bu düzenin dörder ve beşer şekilde de devam ederek kalan harflerin bu şekilde temsil edilebileceğini belirtmiştir. Buna ilave olarak İbnu'd-Dureyhim ipliğin ipekten olmasının ve her bir harf için farklı renkte boncuk kullanılmasının daha iyi olacağını ifade etmiştir. İbnu'd-Dureyhim'in bu başlık altında ele aldığı son yöntem ise katlanmış kâğıt ile şifreleme yöntemidir. Yöntem, kâğıdın üst ve alt ucunun ortada birleştirilmesine ve mesajın bu birleşim noktasına yazılmasına dayanmaktadır. Daha sonra kâğıdın tekrar açılarak mesajın gizlenmesi amaçlanmaktadır (Alam ve diğerleri, 2003b: 80-82).

5. Harf yerine onluk sayı sistemindeki karşılığı konularak yapılan şifreleme:

Yerine koyma kuralının uygulandığı bu yöntemde, harflerin ebced sisteminde denk oldukları sayısal değerlerin bilgisi kullanılmaktadır. İbnu'd-Dureyhim yöntemin aşağıdaki dört farklı şekilde uygulanabileceğini belirtmiştir.

1. Harflerin ebced sisteminde temsil ettiği değerlerin sayı olarak yazılması ile
2. Harflerin ebced sisteminde temsil ettiği değerlerin okunuşlarının yazılması ile
3. Harflerin ebced sisteminde temsil ettiği değerlerin parmak işaretleri ile gösterilmesi
4. Her harf için yeni bir sayısal değer belirlenip, harf yerine bu yeni değer yazılması ile

İbnu'd-Dureyhim bu yöntemi biraz daha geliştirerek harfin temsil ettiği değer korunması şartı ile başka kelimeler üzerinden temsil edilebileceğinden bahsetmiş ve İbn

Duneynır gibi y nteme bir ařama daha ekleyerek harfin temsil ettięi deęere arpma iřlemi uygulayıp bu deęerin tekrar harfler  zerinden temsil edilebileceęini belirtmiřtir (Alam ve dięerleri, 2003b: 68-70).

6. Harf yerine kelime kullanılarak řifreleme:

Yerine koyma kuralının uygulandıęı bu bařlıktaki y ntemler, İbnu'd-Dureyhim'in ele aldıęı řekilde d rt kategoriye ayrılabilir. Birinci kategoride harflerin yerine harflerin okunuřları yazılmaktadır. İbnu'd-Dureyhim bu řifrelemede, harflerin okunuřlarının sırayla bir d z ve bir ters ya da bir ters ve bir d z olarak yazılarak uygulanmasını  nermiřtir.

İkinci kategoride, iletilecek olan mesajın harfleri belirlenen kurala g re yeni oluřturulan bir metnin kelimelerinin ierisine yerleřtirilmektedir. İbnu'd-Dureyhim'in bu řifreleme iin ařaęıdaki řekilde alternatifler sunmuřtur (Alam ve dięerleri, 2003b: 70-72).

- a. Mesajdaki harfler řifreli metindeki her kelimenin ilk harfi olacak řekilde
- b. Mesajdaki harfler řifreli metindeki her kelimenin son harfi olacak řekilde
- c. Mesajdaki harfler řifreli metindeki her kelimenin orta harfi olacak řekilde
- d. Mesajdaki harfler řifreli metindeki her kelimenin ikinci harfi olacak řekilde
- e. Mesajdaki harfler řifreli metindeki her kelimenin   nc  harfi olacak řekilde
- f. Mesajdaki harfler řifreli metindeki tek sıra numaralı harflere denk getirilecek řekilde
- g. Mesajdaki harfler řifreli metindeki ift sıra numaralı harflere denk getirilecek řekilde
- h. Mesajdaki harfler řifreli metindeki her   kelimedenden birinci kelimenin birinci, ikinci kelimenin ikinci,   nc  kelimenin   nc  harfine denk getirilecek řekilde
- i. Mesajdaki harfler řifreli metnin ilk harfine ve ikiřer harf ara olacak řekilde dięer harflerine denk getirilecek řekilde
- j. Mesajdaki harfler řifreli metnin ikinci harfine ve ikiřer harf ara olacak řekilde dięer harflerine denk getirilecek řekilde
- k. Mesajdaki harfler řifreli metnin   nc  ve   n katı olan harf sıralarına denk getirilecek řekilde

Bu şekilde bir şifreleme yapan kişinin, şifreli metindeki hangi harflerin dikkate alınması gerektiğinin doğrudan mesajla iletebileceğini de belirten İbnu'd-Dureyhim, şifreye ١ harfi ile başlanırsa ikinci harflerin, ب harfi ile başlanırsa üçüncü harflerin, ج harfi ile başlanırsa dördüncü harflerin okunması gerektiğini ifade etmiştir. Bununla birlikte İbnu'd-Dureyhim kişinin mesaja doğrudan besmele ile başlayarak metindeki üçüncü harflerin dikkate alınması gerektiği işaretinin verilebileceğini de belirtmiştir (Alam ve diğerleri, 2003b: 72). Üçüncü kategori, her harfe bir kategoriye ait ismin atanmasına dayanmaktadır. İbnu'd-Dureyhim bu isimlerin insan, yıldız, kitap, meyve, ağaç, hayvan, ülke, ilaç isimleri, haftanın gün ve saatleri ve Kur'an-ı Kerim'deki sure isimlerinin olabileceğini ifade etmiştir. Seçilen isimler alfabedeki harflerle eşleştirilerek şifreleme yapılmaktadır. İbnu'd-Dureyhim'in, aynı kategoriye ait isimlerin kullanıldığı bu yöntemi, İbn 'Adlān gibi doğrudan açık metindeki harflerin yerine konulması ile ele aldığı anlaşılmaktadır. Bununla birlikte yöntemin sözlü veya yazılı olarak ya da resim veya semboller kullanılarak oluşturulabileceğini belirtmiştir (Alam ve diğerleri, 2003b: 74). İbnu'd-Dureyhim son kategoride ise harflerin sayısal alfabeyi oluşturan kelime grubunun ve o kelime grubunda bulunduğu harf sırasının dikkate alınması ile bir dallı alfabe oluşturarak şifreleme yapılabileceğinden bahsetmiştir. Harfin sayısal alfabede bulunduğu kelime grubunun sıra sayısı kadar sağ tarafa, bu kelime grubunda kendisinin bulunduğu sıra sayısı kadar da sol tarafa çizik atılarak dallı alfabenin oluşturulabileceğini ifade etmiş ve محمد ابن عم علي ifadesinin bu yöntemle şifrenmesini örnek olarak paylaşmıştır (Alam ve diğerleri, 2003b: 74-76).

Resim 2: İbnu'd-Dureyhim'in *Miftāḥ el-Kunūz fī ṭdāḥ el-marmūz* isimli risalesindeki dallı harf şekilleri



Kaynak: Süleymaniye Kütüphanesi, Esad Efendi 3558, vr. 51b.

7. Kurgulama Yöntemi Kullanılarak Yapılan Şifreleme:

Bu yöntem her harfin yerine o harfle başlayan bir kategoriye ait ismin konulması ile uygulanmaktadır. İbnu'd-Dureyhim ۱ harfinin insan, ب harfinin sebze, ت harfinin tarih veya baharat, ث harfinin kıyafet, ج harfinin deri, ح harfinin tahıl veya demir, خ harfinin ahşap, د harfinin hayvan ya da merhem, ذ harfinin altın, ر harfinin aromatik bitki, ز harfinin cam, س harfinin silah veya balık, ش harfinin ay, saç veya satranç, ص harfinin boya, pirinç veya yün ض harfinin ışık veya bölge, ط harfinin kuş, ظ harfinin karanlık veya geyik, ع harfinin koku, göz veya sayı, غ harfinin koyun, ف harfinin meyveler, ق harfinin köy veya kamış, ك harfinin kitap veya gezegen, ل harfinin süt, م harfinin kasaba, ن harfinin yıldız veya bakır, و harfinin vahşi hayvan, para birimi veya kağıt, ه harfinin böcek, لا harfinin makas ve ي harfinin ise ziynet eşyası için kullanılabileceğini belirtmiştir (Alam ve diğerleri, 2003b: 76). İbnu'd-Dureyhim, Kindî ve İbn Duneynîr'den farklı olarak herhangi bir harfe bağlı kalınmadan, 29 harften sadece birine bağlı kalınarak, normal alfabenin dizilişine bağlı kalınarak ve sayısal alfabenin dizilişine bağlı kalınarak toplamda 32 farklı şifre alfabesinin oluşturulabileceğini belirtmiştir (Alam ve diğerleri, 2003b: 78-80).

8. Harf yerine sembol ve işaret kullanarak şifreleme:

Harfler yerine tasarlanmış sembol veya işaretlerin konulduğu basit yerine koyma yöntemidir. İbnu'd-Dureyhim eserin sonunda bu yöntem ile hazırlanmış iki tane şifre örneğine yer vermiş ve çözümleme aşamalarını paylaşmıştır. Bunula birlikte yöntemi daha karmaşık hale getirmek için kelime içerisine fazladan sembollerin, kelime aralarına ise sembol, nokta veya tire gibi işaretlerin konulabileceğini belirtmiştir (Alam ve diğerleri, 2003b: 82).

İbnu'd-Dureyhim şifreleme yöntemlerini açıkladıktan sonra, şifre çözümlemeye yardımcı olması için Arap dilinin morfolojisine dair bazı bilgiler paylaşmıştır. Bu bölümde kelimelerin uzunluğu, kelimelerin başında tekrarlanan harfler, kelime içerisinde ardışık olarak bulunan harfler ve harflerin birbirleriyle birleşme ve birleşmeme durumları hakkında bilgi vermiştir²⁴ (Alam ve diğerleri, 2003b: 84). İbnu'd-Dureyhim, şifreli bir metinle karşılaşıldığı zaman ilk olarak kullanılan sembol sayısının ve bu sembollerin bulunma sayılarının hesaplanması gerektiğini belirtmiştir. Şifrenin boşluksuz olarak hazırlanmış olma ihtimaline dikkat çekmiş ve böyle bir durumla karşılaşıldığı zaman olası harf kombinasyonlarının kullanılarak boşluğun tespit edilmesinin gerektiğini söylemiştir. Bu aşamayı bir harfin alınıp ikinci harfin boşluk olarak kabul edilmesi ancak anlamlı olmuyorsa, boşluk varsayımının bir sonraki harfe kaydırılması olarak açıklamıştır. Tüm boşluklar tespit edilene kadar bu şekilde devam edilmesi gerekmektedir. Boşluklar tespit edildikten sonra sembollerin bulunma sıklıkları ile açık metnin dilindeki harflerin bulunma sıklıkları birbirleri ile eşleştirilmelidir.

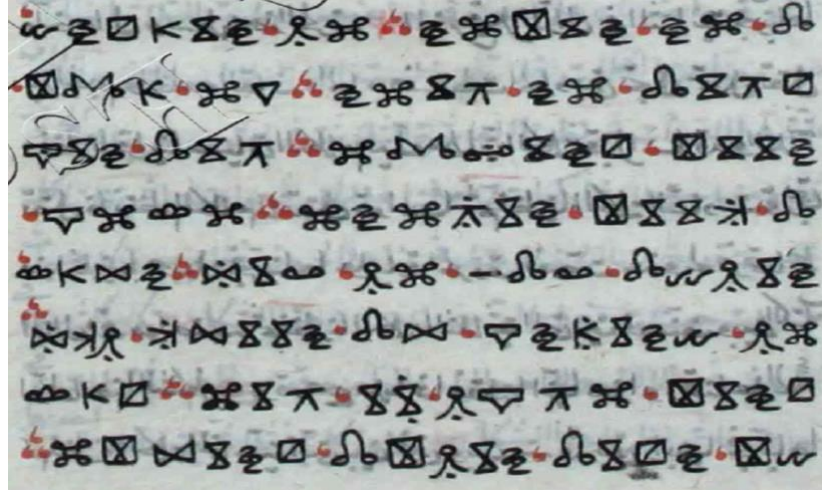
Bu noktada İbnu'd-Dureyhim, Kur'an-ı Kerim'den yararlanarak hesapladığını ifade ettiği harflerin bulunma sıklıklarını azalan sıraya göre paylaşmış fakat şifreli metnin kısa olması ve yeterince harf içermemesi durumunda bu hesaplamanın bir etkisi olmayacağını belirtmiştir. Metin yeterli uzunlukta ise doğru bir şekilde harf eşleştirmeleri yapıldıktan sonra sırayla iki, üç, dört ve beş harfli kelimelere geçilmeli ve çözümlenmeye çalışılmalıdır (Alam ve diğerleri, 2003b: 98-100).

²⁴ Ayrıntılı bilgi için bkz. Alam, Mrayati ve at-Tayyan, 2003b: 84-98.

İbnu'd-Dureyhim son olarak kelimenin başında ال takısından önce gelen ب, ف, ك, و harflerine dikkat çekmiş ve şifre çözümlemeye yeni başlayanların ا ve ت gibi dışıl yapıyı ve ي gibi birinci tekil şahsı ifade eden harflerin olduğu bir şiirle pratik yapmasının faydalı olacağını belirterek şifre çözümleme ipuçlarını bitirmiştir (Alam ve diğerleri, 2003b: 102).

Eserinin son bölümünde harfler yerine semboller konularak hazırlanmış iki tane şifre örneğine yer veren İbnu'd-Dureyhim, önceki bölümlerde paylaştığı çözümleme tekniklerini uygulamalı olarak göstermiştir. İbnu'd-Dureyhim'in vermiş olduğu bu iki örnek, şifreli bir metne nasıl yaklaşılmaması, ilk olarak nereden başlanması ve ne tür yorumlar yapılması gerektiği ile ilgili okuyucuya yol göstermesi açısından oldukça önemlidir. Bunun yanında seçmiş olduğu örneklerden birinin alfabedeki harflerden sadece 21 tanesinin kullanılarak hazırlanmış olması da şifre çözümleyiciyi çetrefilli durumlara karşı hazırlaması açısından dikkate değerdir.

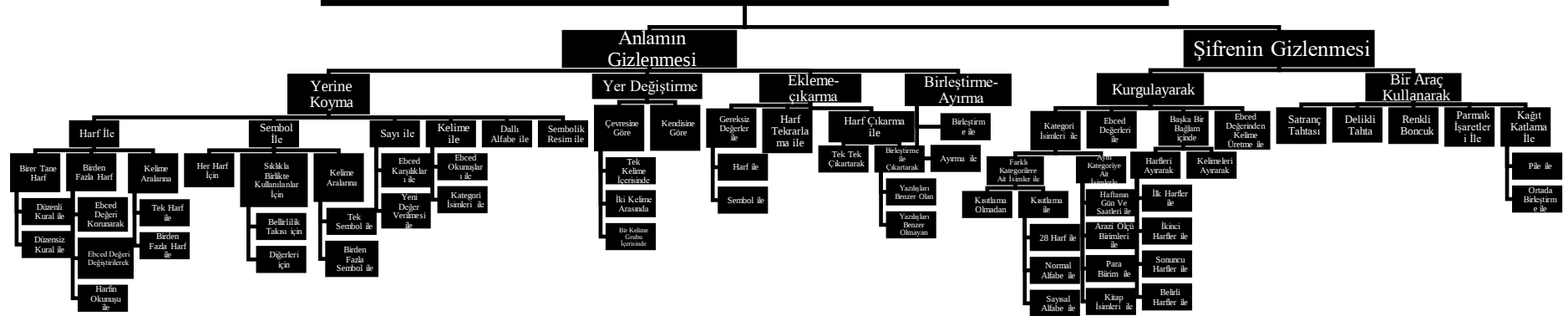
Resim 3: İbnu'd-Dureyhim'in *Miftāh el-Kunūz fī idāh el-marmūz* isimli risalesinde vermiş olduğu şifreli metin örneği



Kaynak: Süleymaniye Kütüphanesi, Esad Efendi 3558, vr. 57b

Şekil 3: Şifreleme Yöntemlerinin Sınıflandırılması

13. ve 14. YÜZYILLARDA İSLAM MEDENİYETİNDE KULLANILAN ŞİFRELEME YÖNTEMLERİ



BÖLÜM III

ON ÜÇÜNCÜ VE ON DÖRDÜNCÜ YÜZYILLARDA İSLAM MEDENİYETİNDE KULLANILAN ŞİFRELEME YÖNTEMLERİ

3.1. YÖNTEMLERİN AÇIKLAMALARI

3.1.1. Anlamın Gizlenmesine Dayalı Şifreleme Yöntemleri

Bu başlık altında ele alınan yöntemlerdeki amaç, mesajın kendisini değil anlamını gizlemektir. Başka bir ifade ile anlaşılır halde yazılan bir metnin anlaşılamayacak hale dönüştürülmesidir.

3.1.1.1. Yerine Koyma Yöntemi

Yerine koyma şifrelemesi, alfabedeki her harfin yerine kendisinden farklı harf veya harflerin ya da herhangi bir sembolün konularak şifrlenmesiyle elde edilen yöntemdir (Borda, 2011:128). Kullanımı çok eskiye dayanan bu yöntem için 13. ve 14. yüzyıllarda İslam medeniyetinde çeşitli uygulama biçimleri geliştirilmiştir. Bu uygulama biçimleri, açık metinde bulunan harflerin yerine harf, sembol, sayı, kelime, dallı alfabe ile oluşturan harf ve sembolik resim konulması şeklinde altı alt başlıkta ele alınabilir.

3.1.1.1.1. Harf Konulması

Açık metindeki her harfin yerine başka bir harf ya da harflerin konulması ile uygulanmaktadır.

3.1.1.1.1.1. Her Harf Yerine Bir Harf Konulması

Bu yöntem düzenli bir kurala bağlı kalarak ya da kalmaksızın açık metnin dilini oluşturan tüm harflerin yerine kendisi dışında başka bir harfin konulmasıyla uygulanmaktadır.

3.1.1.1.1.1. Düzenli Bir Kurala Bağlı Olarak

İbnu'd-Dureyhim düzenli kuralı, harflerin ebced dizilişlerine göre teker teker ya da ikişerli ele alınmasıyla belirlenen bir sıraya göre birbirlerinin yerine geçmesi şeklinde açıklamıştır. Başka bir ifade ile açıklamak gerekirse yöntem, alfabenin bilinen harf dizilişinin değiştirilmesi ve harfin şeklinin yeni dizilişte kendi sırasına denk gelen harfe ödünç verilmesi ile uygulanmaktadır. Böylece alfabedeki her harfte bir değişiklik yapılması mümkün olmaktadır (Churchhouse, 2004: 15).

Bu noktada tıpkı bir kapı anahtarı gibi işlev gören ve mesajları açıp kilitlemeye yarayan (Cobb, 2004: 33) şifre anahtarı kavramından da bahsetmek gerekmektedir. Şifre anahtarı, açık metnin alfabesinin şifre alfabesine nasıl dönüştüğünü gösteren bilgiye denilmektedir. Bu bilginin şifreleme yapılmadan önce gönderici ve alıcı kişi arasında güvenli bir şekilde belirlenmesi ve saklanması gerekmektedir. Basit yerine koyma ve yer değiştirme yöntemleri gibi klasik şifreleme yöntemlerinde hem şifreleme hem de çözümleme algoritması aynı anahtara bağlıdır (Delfs ve Knebl, 2007: 1). Bu şifreleme türündeki anahtar ise alfabedeki harflerin kaç sıra ve hangi yöne doğru kaydırıldığı bilgisidir.

3.1.1.1.1.2. Düzenli Bir Kurala Bağlı Olmayarak

Düzensiz kural, alfabenin bilinen harf dizilişinin belirli bir kurala bağlı olmadan rastgele değiştirilmesi ile uygulanmaktadır. Bu durumda 28 harfli bir alfabe için $28!$ şifreli alfabe oluşturma olasılığı çıkmaktadır. İbnu'd-Dureyhim bu sayıyı neredeyse sayılamayacak kadar fazla olarak ifade etmiştir (Alam ve diğerleri, 2003b: 62). İbn 'Adlān ve İbnu'd-Dureyhim eserlerinde bu yöntem için şifre anahtarı görevini gören harf dizilişlerini örnek olması amacıyla aşağıdaki şekilde paylaşmıştır (Alam ve diğerleri, 2003a: 42, 2005: 98).

İbn 'Adlān'ın şifre alfabesinin dizilişi:

صَحَّ عِنْدِي وَقْتُ شُغْلٍ بِهِ أَخَذْتُ فَظٌّ كَتْ رَطِّ ضَرْجَسْ

İbnu'd-Dureyhim'in şifre alfabesinin dizilişi:

طرق ت شمس فضل ذا جزع خبالاً حديثك نصه غضّ

3.1.1.1.1.2. Her Harf Yerine Birden Fazla Harf Konularak

Açık metindeki her harfin yerine birden fazla harfin konmasıyla uygulanır. Yöntemin aşağıdaki gibi üç ayrı uygulanış biçimi bulunmaktadır.

3.1.1.1.1.2.1. Harflerin Ebced Sisteminde Denk Oldukları Sayısal Değerlerin Korunarak Tekrar Harfe Dönüştürülmesi

Arap alfabesindeki her harfin bir sayıya tekabül etmesi ve bundan istifade edilerek çeşitli işlemlerin yapılmasına “Ebced Hesabı²⁵” ya da “Hisâb-ı Cümel” denilmektedir (Yazıcıoğlu, 2004: 83). Ebced hesabına göre Arap alfabesindeki her harfin 1’den 1000’e kadar olan sabit bir sayısal değeri olduğu kabul edilmektedir. Harflere denk gelen sayısal karşılıklar aşağıdaki tabloda gösterilmiştir.

Tablo 2: Arap Harflerinin Ebced Sistemindeki Sayısal Karşılıkları									
ا	ب	ج	د	هـ	و	ز	ح	ط	ي
1	2	3	4	5	6	7	8	9	10
ك	ل	م	ن	س	ع	ف	ص	ق	ر
20	30	40	50	60	70	80	90	100	200
ش	ت	ث	خ	ذ	ض	ظ	غ		
300	400	500	600	700	800	900	1000		

²⁵ Ebced, Arapça eski Samî alfabesindeki harf sırasının sayı değerine göre tertiplenmesidir. Bu dizginin İbranî ve Süryanî Alfabesindeki harfleri içine aldığı ve dizgide yer alan kelimelerin aynı zamanda birer manaya da geldiği kabul edilir. Bu formülde yer alan kelimeler sırayla şunlardır: ebced, hevvez, huttî, kelemen, sa’fas, karaşet, sehaş, dazağ (zazığlen). Bu kelimelerin gerçekte Arapça köklere dayanmayışı ve bu suretle kelimelerin belli bir anlamının da olmayışı, Arapların bunları başka kavimlerden almış olduklarının açık bir delili olarak görülmektedir.

3.1.1.1.3.1. Bir Çeşit Harf Konulması

Açık metindeki boşluklar yerine tek çeşit bir harfin konulmasıyla uygulanmaktadır.

3.1.1.1.3.2. Çeşitli Harflerin Konulması

Açık metindeki boşluklar yerine birden fazla çeşit harfin konulmasıyla uygulanmaktadır.

3.1.1.1.2. Sembol Konulması

Harfler yerine sembol konularak yapılan şifreleme yöntemi, açık metindeki her harfin yerine tasarlanmış farklı sembollerin ya da farklı karakterlere sahip başka bir alfabenin harflerinin konmasıyla uygulanmaktadır. Bu çalışmada incelenen eserlerin hepsinde bu yöntem yer verilmiştir. Bununla birlikte yöntemin çözümlenmesini zorlaştırmak için kullanım sıklığı yüksek olan harflere birden fazla, sıklıkla beraber kullanılan harflere ise ortak bir sembol atama şeklinde yöntemler geliştirilmiştir.

3.1.1.1.2.1. Her Harf Yerine Bir Sembol Konulması

Açık metindeki her harfin yerine önceden belirlenmiş bir sembol konularak uygulanır. Bu yöntemde açık metindeki harf sayısı ile şifreli metinde kullanılan sembol sayısı birbirine eşittir. Bu uygulama şekli, bu çalışma içerisinde yer alan tüm müellifler tarafından kullanılmıştır.

3.1.1.1.2.2. Sıklıkla Beraber Kullanılan Harflere Ortak Bir Sembol Konulması

Şifreleme yapanlar oluşturdukları şifrelerinin çözümlenmesini daha güç hale getirmek, şifre çözümle yapanlar ise açık metni daha kolay bir şekilde elde etmek için o dilde genellikle beraber kullanılan iki ve üç harfli kelimelerin bulunma sıklıklarını hesaplamışlardır. Dolayısıyla bu başlık altındaki şifreleme yöntemlerinde harfler tek olarak değil birlikte olarak dikkate alınmaktadırlar. Türkçede “bu” işaret zamiri, “ve” bağlacı, “ama” bağlacı, “bir” belgisiz sıfatı Arapçada ise “ال” belirlilik takısı, “و” bağlacı

ile على ve من gibi harfi cerler bu tür sık kullanılan iki ve üç harfli kelimelere örnek verilebilir. Bu şifrelemedeki amaç, harflerin kullanım sıklığı oranlarının düşürerek frekans analiz yönteminin etkinliğini azaltmaktır.

Aşağıdaki tabloda Arap dilinde en yüksek bulunma sıklığına sahip ilk altı harfe bakıldığında sırasıyla %16,36 ile ا harfi, %11,91 ile ل harfi, %8,72 ile م harfi, %7,44 ile ه harfi, %7,14 ile و harfi, %6,87 ile ي harfi ve %6,02 ile ن harfi gelmektedir (Alam ve diğerleri, 2002: 58, 2005: 18, 2007: 20). Sıklıkla beraber kullanılan harflere ortak bir sembolün atanması bu oranları birbirine yaklaştıracaktır. Bu durum ise bu şekilde şifrelenmiş bir metni çözümlemeye çalışan kişinin, birçok harfi göz önünde bulundurması gerektirdiğinden süreci çok daha zor hale getirecektir.

Tablo 3: Arapçada Harflerin Bulunma Sıklığı Yüzdeleri

BULUNMA SIKLIĞI YÜKSEK OLAN HARFLER			BULUNMA SIKLIĞI ORTA OLAN HARFLER		
Sıralama	Harf	Bulunma Yüzdesi	Sıralama	Harf	Bulunma Yüzdesi
1	ا	%16,36	8	ر	%4,22
2	ل	%11,91	9	ع	%3,57
3	م	%8,72	10	ف	%3,32
4	ه	%7,44	11	ت	%3,27
5	و	%7,14	12	ب	%3,05
6	ي	%6,87	13	ك	%3,05
7	ن	%6,02	14	د	%2,50
			15	س	%2,48
			16	ق	%1,71
			17	ح	%1,55
			18	ج	%1,25
BULUNMA SIKLIĞI AZ OLAN HARFLER					
Sıralama	Harf		Bulunma Yüzdesi		
19	ذ		%0,95		
20	ص		%0,87		
21	ث		%0,63		
22	ض		%0,55		
23	خ		%0,55		
24	ط		%0,46		
25	ز		%0,44		
26	ظ		%0,41		
27	غ		%0,41		
28	ظ		%0,22		

3.1.1.1.2.2.1. Belirlilik Takısı Yerine Ortak Bir Sembol Konulması

Bu yöntem, Arapçada isimlerin başında belirlilik eki olarak sıklıkla kullanılan “ال” takısının yerine bu iki harfi birlikte temsil edecek ortak bir sembolün kullanılmasına dayanmaktadır. ال takısının ortak bir sembolle şifrelenmesi bulunma sıklığı en yüksek harfler olan ا ve ل harflerinin bulunma oranlarını düşürerek diğer harflerin bulunma oranlarına yaklaşmasını sağlayacaktır.

İbn ‘Adlān boşluk kullanılarak hazırlanmış bir şifreli metinde, kelimelerin sıklıkla başında kullanılan iki karakterin göze çarpacağını ve bu durumun ا ve ل harflerinin kolay bir şekilde ortaya çıkmasına neden olacağını ifade etmiştir. Bu duruma engel olmak için ال takısı yerine ortak bir sembolün kullanılmasını önermiştir.²⁶ Öte yandan kelimelerin başında sıklıkla tekrar eden bir sembolle yazılan şifre ile karşılaşmaları halinde bunun ortak bir sembol altında şifrelenmiş el takısı olarak düşünülmesi gerektiğine dair de okuyucularını uyarmıştır (Alam ve diğerleri, 2003a: 60-62). Bunun birlikte İbn ‘Adlān ال takısının çözümlenmesini kolaylaştırmak için bu takının bulunduğu kelimelerin sayısal tanımını üzerine de ayrı bir kuraldan bahsetmiştir.

Bu kuralda belirlilik takısı bulunan bir kelimenin sonunda eğer ي harfi bulunmuyorsa, kelimenin ال takısı dışında en az iki harften oluştuğunu belirtmiş ve الحبّ، الذرّ، المرّ، الشجّ gibi kelimeleri örnek vermiştir. Kuralın devamında, belirlilik takısı ile oluşturulan kelimelerin çoğunun yedi ve sekiz harfli kelimeler olduğunu belirtmiş ve مستخرجات، مصطلحين، مصطلحات، مستخرجين kelimelerini örnek vermiştir.

Bu iki ipucuna ek olarak belirlilik takısından önce gelen harflerle ilgili de bilgi veren İbn ‘Adlān ال takısından önce gelen harflerin azalan sırayla و ب ك ف harfleri olduğunu ve bu dört harften herhangi ikisinin de فوالله، فوالله، فوالله kelimelerinde olduğu gibi beraber olarak bulunabileceğini belirtmiştir (Alam ve diğerleri, 2003a: 66).

²⁶Bu yönteme benzer olarak A ve B’nin yazarı ise ا ve ل harflerinin ayrı ayrı iki veya daha fazla sembolle temsil edilmesinden bahsetmiştir. Eğer ا harfi iki ayrı sembolle temsil edilecek olursa bulunma sıklığı yüzdesi $16,36: 2 = \%8,18$ ’e düşecek ve yine bulunma sıklığı yüksek olan harfler aralığında kalacaktır. Eğer üç ayrı sembolle temsil edilecek olursa bulunma sıklığı oranı $16,36: 3 = \%5,453$ ’ya düşecektir. Böylece yüksek bulunma sıklığına sahip harflerin sonuncusu olan $\%6,02$ oranındaki ن harfinin bile altına düşerek yüksek bulunma sıklığına sahip harf grubu dışındaki diğer tüm harfler tarafından temsil edilebilir duruma gelecektir.

3.1.1.1.2.2. Belirlilik Takısı Dışında Sıklıkla Beraber Kullanılan Harfler Yerine Ortak Bir Sembol Konulması

İbn Duneynır, ال takısı dışında لا، ما، أو، لم، من، أن، عن، في، على، لها، بها gibi sık kullanılan iki ve üç harfli kelimeler için de ortak bir sembol kullanımından bahsetmiştir (Alam ve diğerleri, 2005: 78). Amaç ال takısında olduğu gibi harflerin bulunma oranlarını birbirine yaklaştırarak şifre çözümleyicinin yanılmasını sağlamaktır.

3.1.1.1.2.3. Kelime Aralarına Sembol Konulması

İbn ‘Adlān şifreli metinde boşluğun bir ya da birkaç sembolle temsil edilebileceğinden bunun tespiti için ise kelimelerin genellikle başında ve sonunda bulunan harflerin iyi bilinmesi gerektiğinden bahsetmiştir. İbnu’d-Dureyhim ise bu boşlukların yerine harfler için tasarlanan sembollere benzer sembollerin yanında tire, nokta, daire gibi işaretlerin de kullanılabileceğini belirtmiştir. Bu durumda bu yöntemin, boşlukların yerine bir çeşit ya da birden fazla çeşit sembol konulması olmak üzere iki şekilde uygulanabileceğinden bahsedilmiştir (Alam ve diğerleri, 2003a: 58, 2003b: 82).

3.1.1.1.2.3.1. Bir Çeşit Sembol Konulması

Açık metindeki boşluklar yerine tek bir sembolün konulmasıyla uygulanır. Bu yöntemle hazırlanmış bir şifrede kullanım sıklığı en yüksek olan sembol yüksek ihtimalle boşluk için kullanılan sembol olacaktır. Bu sebeple bu yöntemle oluşturulan bir şifrenin frekans analizi yöntemine karşı savunmasız kalması oldukça muhtemeldir.

3.1.1.1.2.3.2. Çeşitli Sembollerin Konulması

Açık metindeki boşluklar yerine birden fazla sembolün konulmasıyla uygulanır. Böylelikle bir önceki yöntemin dayanıklılığının artırılması amaçlanmaktadır. Boşluk için birden fazla sembolün kullanılması, harflerin kullanılma oranlarını birbirlerine yaklaştırarak frekans analizi yönteminin etkinliğini düşürecektir.

3.1.1.1.3. Sayı Konulması

Bu yöntemde açık metindeki harflerin yerine ebced sayı sistemindeki onluk sayısal değerler ya da şifreleyen kişinin belirlediği yeni sayısal değerler yerleştirilmektedir.

3.1.1.1.3.1. Harflerin Yerine Ebced Sistemindeki Sayı Karşılıklarının Konulması

Yöntem, açık metindeki her harfin yerine kendisine tekabül eden ebced sayı değerinin konması ile uygulanmaktadır. İbn Duneynîr ve İbnu'd-Dureyhim eserlerinde bu yöntemden bahsetmişlerdir. İbn Duneynîr 1 rakamından önce küçük bir yuvarlak gelirse 10 sayısı, iki küçük yuvarlak gelirse 100 sayısı, üç küçük yuvarlak gelirse 1000 sayısı olduğunu ve diğer sayıların da bu mantıkla elde edilebileceğini belirtmiştir. Bu şekilde oluşturulmuş bir şifrenin çözümlenmesinin oldukça kolay olduğunu ifade eden İbn Duneynîr, yöntemin açıklamasına *الله وليّ التوفيق* ifadesindeki harflerin onluk sayısal değerlerinin karşılıklarını göstererek son vermiştir (Alam ve diğerleri, 2005: 124).

İbnu'd-Dureyhim ise onluk sayı sistemi kullanılarak oluşturulan bir şifrelemenin aşağıdaki gibi dört farklı şekilde yapılabileceğinden bahsetmiştir (Alam ve diğerleri, 2003b: 68).

- a. Harflerin denk olduğu sayı değerleri ile yazılması
- b. Harflerin sayı değerlerinin okunuşları ile yazılması²⁷
- c. Harflerin belirlenen yeni sayısal değerler ile yazılması
- d. Harflerin sayı değerlerinin parmak işaretleri ile temsil edilmesi²⁸

3.1.1.1.3.2. Harflerin Yerine Yeni Belirlenen Sayısal Değerlerin Konulması

Yöntem her harf yerine şifrelemeyi yapan kişinin kendi belirlediği yeni sayısal değerini yazılması ile uygulanmaktadır.

²⁷ Bu yöntem 2.3.1.1.4.1. numaralı başlıkta ele alınmıştır.

²⁸ Bu yöntem 2.3.2.2.1 numaralı başlıkta ele alınmıştır.

3.1.1.1.4. Kelime Konulması

Açık metindeki harfler yerine kelimeler yerleştirilerek uygulanır. Bu yöntemin, harflerin yerine kendilerine karşılık gelen ebced değerlerinin okunuşlarının ya da ilişkilendirildikleri kategoriye ait isimlerin yazılması olarak iki farklı şekilde uygulandığı görülmektedir.

3.1.1.1.4.1. Harflerin Yerine Ebced Sistemindeki Sayısal Değerlerinin Okunuşlarının Konulması

Açık metindeki harfler yerine ebced sisteminde kendilerine karşılık gelen sayısal değerlerin okunuşları yazılır (Alam ve diğerleri, 2003b: 68, 2005: 124).

3.1.1.1.4.2. Harflerin Yerine Bir Kategoriye Ait İsimlerin Konulması

Yöntem, açık metindeki harflerin yerine daha önce ilişkilendirilmiş oldukları kategoriye ait isimlerin yazılmasına dayanmaktadır. İbnu'd-Dureyhim, bu ilişkilendirmeyi hem basit yerine koyma hem kurgulama şeklinde uygulamışken, İbn Duneynîr, sadece kurgulayarak İbn 'Adlân ise sadece basit yerine koyma yöntemi olarak uygulamıştır. Bunun yanı sıra, İbn 'Adlân'ın boşluk için de ayrıca bir isim kullanması dikkat çekmektedir (Alam ve diğerleri, 2003a: 104, 2003b:74).

3.1.1.1.5. Dalı Harf Konulması

Yöntem Arap harflerinin ebced dizilişini oluşturan ebced (أبجد), hevvez (هوز), huttî (حطي), kelemen (كلمن), sa'fes (سعفص), karaşet (قرشت), sehaş (ثخذ) ve dazağ (ضظغ) kelimelerinin bilgisine dayanmaktadır. Şifreleme yaparken öncelikle her harf için bir çubuk çizilmekte ve harfin içinde bulunduğu kelimeye bakılmaktadır. Çubuğun sağ tarafına kelimenin, ebced dizilişini oluşturan kelime grubu içerisinde bulunduğu sıra sayısı kadar, sol tarafına ise harfin o kelimenin içinde bulunduğu sıra sayısı kadar dal çizilmektedir (Alam ve diğerleri, 2003b: 74).

3.1.1.1.6. Sembolik Resim Konulması

Açık metindeki harfler yerine kuş, hayvan, bitki gibi hatırlatıcı sembol ya da resimler konularak yapılan şifreleme yöntemidir. Harflerin hangi sembol ya da resimlerle eşleştirildiği gönderici ve alıcı arasında önceden belirlenmelidir (Alam ve diğerleri, 2003b: 74).

3.1.1.2. Yer Değiştirme Yöntemi

Açık metindeki harflerin belirli bir kurala göre yerlerinin değiştirilerek şifreli metne dönüştürmesine yer değiştirme şifrelemesi denmektedir (Dooley, 2013: 8). Bu yöntemde harflerin kimlikleri aynı şekilde korunmaktadır. Başka bir ifade ile şifreli metin, açık metinde kullanılan harfler ile elde edilmektedir. Bu şifreleme yöntemleri harflerin çevresindekilere ve kendine göre pozisyonunu değiştirmesi şeklinde iki başlık altında ele alınmıştır.

3.1.1.2.1. Harflerin Çevresindeki Harflere Göre Yerlerinin Değiştirilmesi

Yöntem, açık metindeki her harfin etrafındaki harflerle olan bağlantısına göre yer değiştirilmesine dayanmaktadır. İbn Duneynîr bu şekilde hazırlanmış bir şifreleme ile karşılaştığı zaman harfler arasındaki uyumsuzluğun hemen fark edileceğini ve açık metne ulaşmak için anlamlı bir ifade elde edene kadar harflerin konumlarının sürekli olarak yeniden düzenlenmesi gerektiğini ifade etmiştir (Alam ve diğerleri, 2005: 100). İbnu'd-Dureyhim ise bu şifreleme türünü en fazla detaylandıran kişi olmuştur. İbnu'd-Dureyhim'in bu yöntem altında sunmuş olduğu alternatifler, uygulanış biçimleri açısından tek kelime içerisinde, iki kelime arasında ve birkaç kelime arasında içinde olmak üzere üç ayrı kategoride sınıflandırılabilir (Alam ve diğerleri, 2003b: 56-60).

3.1.1.2.1.1. Tek Kelime İçerisinde

1. Kelimenin baştaki harflerinin sırayla kendilerine karşılık gelen sondaki harfleriyle değiştirilmesi
2. Kelimenin son harfinin en başa yazılması
3. Kelimenin ilk harfi ile son harfinin yerlerinin değiştirilmesi
4. Kelimenin ilk harfi ile üçüncü veya dördüncü harfinin yer değiştirilmesi
5. Kelimedeki harflerin ikiyeşerli olarak ayrılması ve her ikili harfin bir önceki iki harfin önüne getirilmesi
6. Kelimedeki çift sıradaki harflerle tek sıradaki harflerin yerlerinin değiştirilmesi
7. Kelimenin baştaki harflerinden sonra sırayla sondaki harflerinin getirilmesi
8. Kelimenin sonundaki harflerin sırayla baştaki harflerinin önüne getirilmesi

3.1.1.2.1.2. İki Kelime Arasında

1. Birinci kelimenin ilk harfi ile ikinci kelimenin ilk harfinin değiştirilmesi
2. Birinci kelimenin son harfi ile ikinci kelimenin son harfinin değiştirilmesi
3. Birinci kelimenin ilk harfi ile ikinci kelimenin son harfinin değiştirilmesi
4. Birinci kelimenin son harfi ile ikinci kelimenin ilk harfinin değiştirilmesi
5. Birinci kelimenin ilk harfi ile ikinci kelimenin ilk harfi, birinci kelimenin son harfi ile de ikinci kelimenin son harfinin değiştirilmesi
6. Birinci kelimenin ilk harfi ile ikinci kelimenin son harfi, birinci kelimenin son harfi ile de ikinci kelimenin ilk harfinin değiştirilmesi

3.1.1.2.1.3. Bir Kelime Grubu İçerisinde

İbnu'd-Dureyhim metindeki kelimelerin belirlenen bir rakama göre gruplara ayrılarak çeşitli yöntemlerin uygulanabileceğini belirtmiştir. Örneğin kelimeler ikiyeşer, üçer ya da dörder gruplara ayrılır ve sırayla her kelimenin ilk harfinden başlanarak son harfine kadar art arda yazılır.

3.1.1.2.2. Harflerin Kendi Pozisyonuna Göre Değiştirilmesi

Bu yöntemde harfin pozisyonu çevresindeki harflere göre değil kendi bulunduğu pozisyona göre değiştirilmektedir. Harfin şekli ve kelime içerisinde bulunduğu konumu aynı kalmakla birlikte harfin standart görünüm açısından değişiklik yapılmaktadır. İbn Duneynîr bu yöntemi çözümlmek için her harfin farklı açılarda yazılışlarının göz önünde bulundurulması gerektiğini belirterek algısal iç görüye sahip bir insanın gözünden bu yöntemle hazırlanmış bir şifrenin asla kaçmayacağını ifade etmiştir (Alam ve diğerleri, 2005 :100).

3.1.1.3. Ekleme ve Çıkarma Yöntemi

Yöntem açık bir metnin ya da halihazırda şifrelenmiş bir metnin içerisine gereksiz değerler eklenmesi veya içerisinden bazı harflerin çıkarılması ile uygulanmaktadır.

3.1.1.3.1. Fazladan Harf ya da Sembollerin Eklenmesi

Eklenen yeni değerler metnin durumuna göre harf ya da sembollerden oluşabilir. Eğer metne daha önce bir şifreleme yapılmamış ise belirlenen bir kurala göre harfler doğrudan metin içerisine eklenerek metnin karmaşık hale gelmesi amaçlanır. İbn Duneynîr bu durumda harflerin sesli harf olmamasının şartını koştur. Bununla birlikte sembol kullanılarak şifrelenmiş bir metne ise karşılığı olmayan semboller eklenerek şifrenin çözümlenmesi daha güç hale getirilebilir (Alam ve diğerleri, 2003b: 82, 2005: 102).

3.1.1.3.1.1. Harf Eklenmesi

Açık metindeki kelimelerin içerisine belirli bir kurala göre harf ya da harflerin eklenmesi ile uygulanmaktadır.

3.1.1.3.1.2. Sembol Eklenmesi

Sembol kullanılarak yerine koyma yöntemi uygulanmış bir şifreli metne fazladan semboller eklenerek uygulanmaktadır. Halihazırda şifrelenmiş bir metne uygulanan bu

ikinci işlem şifrenin karmaşıklığını bir üst seviyeye taşımaktadır (Alam ve diğerleri, 2003b: 82).

3.1.1.3.2. Harflerin Tekrarlanması

Yöntem açık metindeki harflerin belirlenen bir kurala göre tekrarlanarak yazılmasına dayanmaktadır. Bu tekrarlama harflerin bazılarını ya da hepsine çeşitli şekillerde uygulanabilmektedir (Alam ve diğerleri, 2003b: 66, 2005: 80).

3.1.1.3.3. Harf Çıkarılması

Yöntem açık metindeki bazı harflerin metinden çıkartılması ile uygulanmaktadır. Şifreli metin belirli bir harfin ya da harflerin metin boyunca geçtiği her yerden çıkartılarak oluşturulabileceği gibi benzer yazılımlara sahip olan ya da olmayan harflerin ortak bir harf üzerinden temsil edilmesi ile de oluşturulabilmektedir (Alam ve diğerleri, 2003b: 66, 2005: 80).

3.1.1.3.3.1. Harflerin Tek Tek Çıkarılması

Yöntem açık metindeki bazı harflerin metinde geçtiği her yerden çıkarılması ile uygulanmaktadır.

3.1.1.3.3.2. Harflerin Birleştirilerek Çıkarılması

Yöntem yazılışları benzer olan ya da olmayan harflerin aynı harf üzerinden temsil edilmesi ile uygulanmaktadır. Bu uygulama yerine koyma şifreleme yöntemi ile karıştırılabilir. Ancak yerine koyma yönteminde kullanılan dilin alfabesindeki harflerde herhangi bir eksiltme yapılmadığı unutulmamalıdır. Harflerin birleştirilerek çıkarılması yönteminde ise çıkarılan harfler hiçbir şekilde şifreli metnin içerisinde yer almazlar.

3.1.1.3.3.2.1. Yazılışları Benzer Olan Harflerin Tek Bir Harf Üzerinden Temsil Edilmesi

Yöntem alfabedeki noktasız halde yazılışları aynı olan harflerin, seçilen herhangi bir harf tarafından temsil edilerek şifrlenmesine dayanmaktadır. Örneğin “c” ve “ç” harflerinin “m” harfi üzerinden temsil edilmesi gibi.²⁹

3.1.1.3.3.2.2. Yazılışları Benzer Olmayan Harflerin Tek Bir Harf Üzerinden Temsil Edilmesi

Yöntem şifreyi oluşturan kişi tarafından seçilen iki ya da daha fazla harfin tek bir harf üzerinden temsil edilerek şifrlenmesine dayanmaktadır. Örneğin “b” ve “c” harflerinin “m” harfi üzerinden temsil edilmesi.

3.1.1.4. Birleştirme ve Ayırma Yöntemi

Yöntem Arapçada birleşik olarak yazılan harflerin ayrı, ayrı olarak yazılan harflerin ise birleşik olarak yazılmasına dayanmaktadır.

3.1.1.4.1. Ayrı Yazılan Harflerin Birleştirilmesi

²⁹A ve B’nin yazarı, bu yöntemi bir adım daha ileri taşıyarak çıkarılan harflerin, bulunma sıklığı en yüksek olan ı ve ۛ harfini temsil etmesi için kullanılmasını önermiştir. Bu sayede şifreli metinde kullanılan toplam karakter sayısı açık metindeki harflerin sayısına eşitlenmiş olur. Amaç şifreyi çözümlmeye çalışan kişiyi şifrenin sadece basit ikame kullanılarak yapıldığı yanılgısına düşürmek ve böylece şifreli metindeki harflere karşılık olarak açık metindeki yanlış harfleri eşleştirmelerine sebep olmaktır. A ve B’nin yazarı bu tarz şifreleri okunması kolay olan fakat çözümlenmesi zor olan şifreler olarak tanımlamıştır. Ortak kullanılan harflerin sayısına göre değişmekle birlikte böyle bir şifrelemede belirlilik takısı için en az iki en fazla beş farklı kombinasyon ortaya çıkmaktadır. Bu durum, şifredeki karakterlerin bulunma sıklıkları ile açık metindeki harflerin bulunma sıklıklarının farklılığı frekans analizi yönteminin uygulanmasında ciddi bir zorluk oluşturmaktadır. İbnu Duneynir ise bu yöntemi tenkit ederek A ve B’nin yazarının şifreleme konusunda yeterli kadar bilgi sahibi olmadığını belirtmiş ve yazarın bu yöntem için herhangi bir çözümleme algoritması açıklamadığını da ifade etmiştir. İbnu Duneynir, bu şifreleme yöntemini kullanan kişinin örneğin ب, ت, ث harflerini temsil etmesi için belirlediği harfin aslında şifreyi hazırlayan kişi için de zor olduğunu ve bu yöntemle hazırlanmış bir şifreli metnin günlerce kalması durumunda unutulma ihtimalinin olduğu belirtmiştir. ث harfinin yüksek, ب harfinin orta ve ت harfinin de düşük bulunma sıklığından dolayı daha sonra şifreyi çözümlmek için frekans analizi yöntemine başvurulduğu zaman harflerin bulunma sıklıklarının istenilen değerleri vermeyeceğini de eklemiştir (Alam ve diğerleri, 2005: 176).

Yöntem doğal olarak birleşmeyen harflerin birleşik olarak yazılması ile uygulanmaktadır. Arap alfabesinde kendinden sonraki harfle birleşmeyen 6 tane harf bulunmaktadır. Bu harfler ا, ذ, د, ز, ر ve و harfleridir. İbn Duneynîr bu harflerin birleşik olarak yazılması ile şifreleme yapılabileceğinden bahsetmiştir (Alam ve diğerleri, 2005: 80).

3.1.1.4.2. Birleşik Yazılan Harflerin Ayrılması

Yöntem doğal olarak birleşen harflerin ayrı olarak yazılmasına dayanmaktadır. Arap alfabesinde ا, ذ, د, ز, ر ve و harfleri dışındaki tüm harfler kendisinden sonra gelen harfle birleşerek yazılmaktadır. İbn Duneynîr bu harflerin ayrı olarak yazılması ile şifreleme yapılabileceğinden bahsetmiştir ³⁰ (Alam ve diğerleri, 2005: 80).

3.1.2. Şifrenin Gizlenmesine Dayalı Şifreleme Yöntemleri

Bu başlık altında ele alınan yöntemler diğer yöntemlerden farklı olarak mesajın anlamını gizlemeye değil doğrudan şifrenin varlığını gizlemeye yöneliktir. Steganografi olarak da adlandırabileceğimiz bu başlık altındaki yöntemler, metin steganografisi olarak da isimlendirebileceğimiz kurgulama yoluyla yapılan şifrelemeler ve bir araç kullanılarak yapılan şifrelemeler olmak üzere iki ana alt başlığa ayrılmıştır.

3.1.2.1. Kurgulayarak Şifreleme

Kurgulayarak yapılan şifreleme yöntemlerindeki amaç, içerisinde şifreli bir mesajın olduğundan şüphe edilemeyecek kadar mantıklı ve uyumlu kelimelerle oluşturulmuş bir metin elde etmektir. Belirlenen kuralda açık metindeki harfleri temsil edecek olan her ne ise sıraları bozulmayacak şekilde yeni oluşturulacak metnin içerisine dikkat çekmeyecek şekilde yerleştirilmelidir (Gaines, 2014: 1).

3.1.2.1.1. Harflerin Bir Kategori ile İlişkilendirilmesine Dayalı Yöntemler

³⁰ A ve B'nin yazarı bu yöntemi daha zorlaştırmak amacıyla harflerin ayırdıktan sonra iki satıra bölünerek yazılmasını önermiştir. Böylece tek sıradaki harfler ilk satıra, çift sıradaki harfler ise ikinci satıra yazılacaktır.

Bu yöntemde alfabedeki her harf bir kategoriye ait isim ya da isimler ile ilişkilendirilmektedir. İbn Duneynîr ve İbnu'd-Dureyhim bu kategori isimlerini, cinslere ve türlere ait isimler olarak adlandırmışlardır. Ancak o dönemde kullanılan cins ve tür kavramlarının tanımları günümüzdeki kadar belirgin olmadığından müelliflerin bu kavramları, aynı ya da farklı kategorilere ait isimler olarak düşündükleri tahmin edilmektedir. Bu sebeple bu yöntem, “farklı kategorilere ait isimlerle ilişkilendirme” ve “aynı kategoriye ait isimlerle ilişkilendirme” olmak üzere iki çeşit altında ele alacaktır. Yöntemin uygulanabilmesi için gönderici ve alıcı arasında harflerle ilişkilendirilen kategori isimlerinin olduğu bir listenin bulunması gerekmektedir. Bu sayede şifreli metin alıcı kişiye ulaştığı zaman hangi ismin hangi harfe tekabül ettiğini görebilecek ve mesajı doğru bir şekilde okuyabilecektir. İki müellifin de Arap alfabesindeki harfler için önerdiği isimler, birleştirilerek 18 numaralı tabloda paylaşılmıştır. Harfler, farklı kategorilere ait isimlerde ilişkilendirildiği zaman birden fazla değer alabilirken aynı kategoriye ait isimlerle ilişkilendirildiğinde tek bir değer alabilmektedirler. Örneğin farklı kategorilere ait isimlerle ilişkilendirilmesinde herhangi bir kuş ismi ile temsil edilebilirken, aynı kategoriye ait isimlerle ilişkilendirilmesinde “güvercin” gibi sadece tek bir kuş ismi ile temsil edilebilmektedirler (Alam ve diğerleri, 2003b: 76-78, 2005: 76).

3.1.2.1.1.1. Harflerin Farklı Kategorilere Ait İsimlerle İlişkilendirilmesi

Alfabedeki her harf farklı kategorilerle ilişkilendirilmekte ve ilişkilendirildikleri kategoriye ait herhangi bir isimle temsil edilebilmektedir. Harflerin birden fazla değer almasına olanak sağlayan bu yöntem, İbn Duneynîr tarafından çözümlenmeye meydan okuyan şifreler olarak tanımlamıştır. Harflerle ilişkilendirdiği isimleri bir liste halinde paylaşan İbn Duneynîr, bu listenin öğrenilene kadar tekrar tekrar çalışılması gerektiğini belirtmiş ve yöntemin daha iyi anlaşılması için *الله ولي التوفيق* ifadesini bir hikâye içerisine yerleştirerek örneklendirmiştir (Alam ve diğerleri, 2005: 110-114). İbnu'd-Dureyhim ise bu yöntem kullanılarak hazırlanabilecek şifre alfabelerini 32 adet olarak belirleyerek yönteme özgün bir katkı sağlamıştır. Birinci alfabe herhangi bir kısıtlamaya tâbi tutulmazken, 29 tanesi sırayla alfabedeki her bir harf ile, son iki tanesi ise normal ve sayısal alfabe sırasına tâbi tutularak hazırlanmakta ve böylece toplam 32 tane şifre alfabesi elde edilmektedir. Bununla birlikte İbnu'd-Dureyhim bu kısıtlamaların zorlayıcı

olduğunu bu nedenle kısıtlama yaparak şifre hazırlayacak kişilerin dile iyi derecede hâkim olması gerektiğini belirtmiştir (Alam ve diğerleri, 2003b: 78-80).

3.1.2.1.1.1.1. Herhangi Bir Kısıtlamaya Tâbi Tutulmadan Yapılan İlişkilendirme

Harflerle ilişkilendirilen isimler herhangi bir harf ile başlayabilmektedir.

3.1.2.1.1.1.2. Bir Kısıtlamaya Tâbi Tutularak Yapılan İlişkilendirme

Aşağıdaki gibi alfabenin yalnızca bir harfine veya normal alfabe dizilişine veya sayısal alfabe dizilişine bağlı olmak üzere üç farklı şekilde uygulanmaktadır.

3.1.2.1.1.1.3. Alfabenin Bir Harfine Bağlı Kalarak

Harflerle ilişkilendirilen isimler ancak belirlenen bir harf ile başlayabilmektedir. Böylece 29 harfli bir alfabe için toplam 29 farklı şifre alfabesi oluşturmak mümkündür.

3.1.2.1.1.1.4. Normal Alfabe Dizilişine Bağlı Kalarak

Harflerle ilişkilendirilen isimler normal alfabe dizilişi sırasıyla başlayabilmektedir.

3.1.2.1.1.1.5. Sayısal Alfabe Dizilişine Bağlı Kalarak

Harflerle ilişkilendirilen isimler sayısal alfabe dizilişi sırasıyla başlayabilmektedir.

3.1.2.1.1.2. Harflerin Aynı Kategoriye Ait İsimlerle İlişkilendirilmesi

Alfabedeki her harf aynı kategoriye ait isimlerle ilişkilendirilmekte böylece yalnızca belirlenen bir isimle temsil edilmektedir. İbnu'd-Dureyhim bu yöntemde kitap, ağaç, meyve, insan, yıldız, ülke, ilaç, merhem isimleri, ayın evreleri, günün saatleri ve Kur'an-ı Kerim'deki sure isimleri gibi alternatifler ile şifreleme yapılabileceğinden bahsetmiştir. İbn Duneynîr ise alan ölçü birimleri, para birimleri, haftanın günleri ve saatleri ile şifreleme yapılabileceğini belirtmiş ve hepsini ayrı başlıklar altında incelemiştir. Metnin

bir şifre içerdiğine dair şüphe oluşturmamak için harflerle ilişkilendirilen bu isimler bir kurgu içerisine yerleştirilmektedir.³¹

3.1.2.1.1.2.1. Harflerin Arazi Ölçü Birimleri ile İlişkilendirilmesi

Bu yöntem arazi ölçü birimleri olan ar, dekar ve hektarın harflerin ebced sistemindeki sayı değerleri ile eşleştirilmesine dayanmaktadır. 1'den 9'a kadar olan sayılar için metrekare, 10'dan 100'e kadar olan sayılar için ar, 100'den 1000'e kadar olan sayılar için dekar ve Ğ harfini temsil eden 1000 sayısı için ise hektar ölçü birimi kullanılmaktadır. İbn Duneynîr bu şifreleme yönteminde oluşturulabilecek en yüksek dereceli gizlemenin şifreli metne, çiftçi ile köylü arasında geçen alım, satım gibi çeşitli pazarlıkların yapıldığı bir finansal kayıt görünümü vermek olduğunu ifade etmiştir. Böyle yapılmadığı takdirde şifrenin kolayca açığa çıkmasına sebep olacak bir görüntünün ortaya çıkabileceğine de dikkat çekmiştir (Alam ve diğerleri, 2005: 116).

3.1.2.1.1.2.2. Harflerin Para Birimi ile İlişkilendirilmesi

Bu yöntemde açık metindeki harfler tam, yarım ve çeyrek dinarlarla temsil edilmektedir. Ebced sistemindeki karşılıkları 1'den 9'a kadar olan harfler tam dinar ile, 10'dan 90'a kadar olan harfler çeyrek dinar ile, 100'den 900'e kadar olan harfler yarım dinar ile 1000 sayısına denk gelen Ğ harfi ise 1/8 dinar ile gösterilmektedir (Alam ve diğerleri, 2005: 138). Örneğin د harfi 4 tam dinar, ر harfi 4 çeyrek dinar, ت harfi ise 4 yarım dinar olarak yazılmalıdır.

3.1.2.1.1.2.3. Harflerin Haftanın Gün ve Saatleri ile İlişkilendirilmesi

³¹ İbn 'Adlân'ın eserini yazmasındaki asıl amacı şifre çözümü yöntemlerine pratik bir el kitabı hazırlamak olduğu için bu yöntemin hangi şekillerde ve nasıl uygulanacağına dair bir açıklama yapmamıştır. Ancak eserinin sonunda vermiş olduğu örnek, harflerin kuş isimleri ile ilişkilendirildiği bir metinden oluşmaktadır. Buradan anlaşıldığı kadarıyla ibn 'Adlân'ın harflerin kategorilere ait isimlerle ilişkilendirilerek şifrelenmesinden haberdar olduğu fakat şifreyi gizlemeye yönelik bir kurgulama yaparak değil, yerine koyma yöntemi ile kullanmayı tercih ettiği görülmektedir.

Bu yöntemde alfabedeki tüm harfler yedi gruba ayrılır. Bu yedi grup haftanın günlerine, harfler ise bulunduğu gruptaki sıra numarasına göre mensup olduğu günün saatıyla eşleştirilmektedir (Alam ve diğerleri, 2003b: 74, 2005: 128).

3.1.2.1.1.2.4. Harflerin Kitap İsimleri ile İlişkilendirilmesi

Alfabedeki her harf bir kitap ismi ile ilişkilendirilerek metnin içerisine yerleştirilmektedir (Alam ve diğerleri, 2003b: 74).

3.1.2.1.2. Harflerin Sayısal Değerlerinin Kullanılarak Bir Metnin İçerisine Yerleştirilmesi

Bu yöntem diğer kurgulama yöntemlerinden farklı olarak harflerin, isimlerle değil ebced sistemindeki sayı karşılıkları ile temsil edilip metin içerisine yerleştirilmesi ile uygulanmaktadır. İbn Duneynîr bu şifreleme yönteminin gök cisimlerinin durum, hareket, uzaklık, dönem, süre, devir sayısı ve birbirleri ile olan ilişkileri hakkında bilgi veren bir astronomi metni olarak sunulabileceğini açıklamıştır (Alam ve diğerleri, 2005: 140). Metindeki sayılar sırayla takip edilip, temsil ettikleri harfler yazıldığı zaman iletilmek istenilen mesaj açığa çıkmış olacaktır. Bunun yanında İbn Duneynîr'in bu tür bir şifrelemeyi yapacak kişinin aritmetik ve astronomi hakkında bilgi sahibi olması gerektiğini ifade etmiş olması, bu tarz şifrelerin bir kurgudan ziyade gerçeği yansıtan ve bir konu hakkında sahici bilgiler veren metinler olması gerektiği şeklinde yorumlanabilir.

3.1.2.1.3. Mesajların Başka Bir Bağlam İçerisine Yerleştirilmesine Dayalı Yöntemler

Yöntem, açık metindeki harflerin ya da kelimelerin ayrılması olarak iki farklı şekilde uygulanabilir.

3.1.2.1.3.1. Harflerin Ayrılması

Yöntem, açık metindeki harflerin sırayla alınarak yeni oluşturulacak metnin kelimelerinin birinci, ikinci, üçüncü veya sonuncu harflerine denk gelecek şekilde başka bir bağlam

içerisinde yerleştirilmesine dayanmaktadır. Böylece mesajdaki harf sayısı kadar kelime içeren bir şifreli metin elde edilmiş olur. İbn Duneynîr şifrenin çözümlenmesinin, mesajın kelimelerinin birinci, ikinci veya sonuncu harflerine odaklanıldığı zaman mesleğin dikkatli düşünenleri için oldukça kolay bir şekilde yapılabileceğini ifade etmiştir (Alam ve diğerleri, 2005: 136).

İbnu'd-Dureyhim ise diğer müelliflerin bahsettiği muhtemel seçeneklerden daha fazlasına değinmiş ve bu yöntemi en çok detaylandıran kişi olmuştur. Mesajın ilk harfinin şifrelenecek metnin kelimelerinin birinci, ikinci, üçüncü, orta, son, tek ya da çift numaralı harflerine denk getirilerek oluşturulabileceğinden bahsetmiş ve her birine örnek vermiştir. Yönteme dair daha fazla alternatif sunarak açıklamaya devam eden İbnu'd-Dureyhim, harflerin şifreli metnin ilk harfine denk getirerek iki harf ara verilmesi veya metnin ilk harfine denk getirilmeden iki harf ara verilerek başlanması veya her dördüncü ya da beşinci harfine denk getirilmesi şeklinde uygulanabileceğinin de örneklerini vermiştir. İbnu'd-Dureyhim tüm bu alternatiflerin yanında yöntemin sadece sabit bir sayıya göre değil kelimelerin üçerli alınarak birinci harfin birinci kelimenin ilk harfine, ikinci harfin ikinci kelimenin ikinci harfine, üçüncü harfin de üçüncü kelimenin üçüncü harfine denk getirebileceğini gösterip yönteme özgün bir taraf da eklemiştir (Alam ve diğerleri, 2003b: 70-72).

3.1.2.1.3.1.1. İlk Harfler ile

Şifreli metnin kelimelerinin ilk harfleri mesajı verir.

3.1.2.1.3.1.2. İkinci Harfler ile

Şifreli metnin kelimelerinin ikinci harfleri mesajı verir.

3.1.2.1.3.1.3. Sonuncu Harfler ile

Şifreli metnin kelimelerinin sonuncu harfleri mesajı verir.

3.1.2.1.3.1.4. Belirli Harfler ile

Şifreli metnin kelimelerinin önceden belirlenen sıradaki harfleri mesajı verir.

3.1.2.1.3.2. Kelimelerin Ayrılması

Yöntemde açık metni oluşturan harflere doğrudan bir müdahale yapılmazken kelimeler birbirinden ayrılarak başka bir bağlam içerisine yerleştirilir (Alam ve diğerleri, 2005: 136).

3.1.2.1.4. Harflerin Sayısal Değerlerine Denk Yeni Kelimeler Üretilmesi

Yöntem, açık metindeki her harfin sayısal değerine denk gelecek şekilde kelime ya da kelimeler üretilmesine dayanmaktadır. Harflerin sayısal değerlerine karşılık oluşturulan kelime ya da kelimeler bittiği zaman sonuna bir nokta konarak bir harfin değerine karşılık geldiği belirtilir. Bu sayede alıcı kişinin, noktalar arasındaki kelime ya da kelimelerin harf değerlerini toplayarak açık metindeki harflere ulaşması amaçlanmaktadır. Ancak belirtmek gerekir ki, bu yöntem sayısal değeri düşük olan harfler için meşakkatli bir hal almaktadır. Bu durum bu yöntemi bir kelime kadar kısa olan mesajlar için nispeten daha elverişli hale getirmektedir³² (Alam ve diğerleri, 2003b: 68).

3.1.2.2. Bir Araç Kullanarak Gizleme

Bu başlık altında ele alınan yöntemler için çeşitli araçlara ihtiyaç duyulmaktadır. Açık metnin harfleri boncuk, delikli tahta, satranç tahtası ve parmak işaretleri aracılığı ile temsil edilmektedir. Bu yöntemler, şifrelemenin sadece kâğıt ve kalem kullanımı ile sınırlı kalmadığını göstermesi açısından da ayrıca önemlidir.

3.1.2.2.1. Parmak İşaretleri ile Şifreleme

³² Bu yöntem, “harflerin yerine kelime konulması” yöntemi altında da ele alınabilirdi. Ancak oluşturulan kelimeler ile cümle kurulmasının da mümkün olmasından dolayı “şifrenin gizlenmesine dayalı şifreleme” yöntemleri altında ele alınması daha uygun görülmüştür.

Bu yöntemde iletilmek istenen mesajın harflerinin ebced sisteminde denk olduğu sayısal değerler, parmak işaretleriyle gösterilerek karşıda hazır bulunan kişiye aktarılmaktadır. İbn Duneynîr 1'den 100'e kadar olan sayılar için sağ elin, 100'den 1000'e kadar olan sayılar için ise sol elin kullanıldığını ifade etmiştir. Buna ilave olarak sayısal değeri ilk 10 sayıya denk gelen harflerin parmak işaretleri ile gösterimini aşağıdaki şekilde açıklamıştır (Alam ve diğerleri, 2003b: 68, 2005: 118).

Bir rakamı için (١ harfini temsil eder): Yüzük parmak bükülür ve serçe parmak yüzük parmağının üzerine geçirilir.

İki rakamı için (٢ harfini temsil eder): Serçe ve yüzük parmak içeriye doğru bükülür.

Üç rakamı için (٣ harfini temsil eder): 2 rakamını temsil eden parmaklar orta parmakla birleştirilir.

Dört rakamı için (٤ harfini temsil eder): Yüzük ve orta parmak bükülmüş halde tutulurken serçe parmak uzatılır.

Beş rakamı için (٥ harfini temsil eder): Orta parmak bükülmüş halde bırakılırken serçe ve yüzük parmakları uzatılır.

Altı rakamı için (٦ harfini temsil eder): Yüzük parmak bükülmüş halde tutularak orta parmak uzatılır.

Yedi rakamı için (٧ harfini temsil eder): Serçe parmak bükülmüş halde tutulur ve diğer tüm parmaklar uzatılır.

Sekiz rakamı için (٨ harfini temsil eder): Serçe ve yüzük parmak bükülür.

Dokuz rakamı için (٩ harfini temsil eder): Serçe, yüzük ve orta parmak bükülür.³³

On sayısını için (١٠ harfini temsil eder) Baş ve işaret parmağı bir halka haline getirilerek diğer tüm parmaklar açılır.

İbnu'd-Dureyhim ise harflerin yerine sayısal değerlerin konulabileceğinden bahsederken parmak işaretleri ile de gösterilebileceğini belirtmiş ancak yöntemin içeriğine dair herhangi bir açıklamada bulunmamıştır.

3.1.2.2.2. Katlanmış Kâğıt ile Şifreleme

³³ 2 ile 8 ve 3 ile 9 rakamları aynı parmak işareti ile tarif edilmiştir. Bunun nedeni tarafımızca anlaşılamamıştır.

Yöntem, kâğıt ve kalemin yaygın kullanımına farklı bir alternatif sunmaktadır. İbn Duneynîr ve İbnü'd-Dureyhim yöntemi iki farklı biçimde ele aldığı görülmektedir. İbn Duneynîr'in ele aldığı şekilde, kâğıt ilk olarak katlanarak pilili bir görünüm elde edilmekte ve iletilmek istenen mesaj bu kıvrımların üstüne yazılmaktadır. Bu sayede kâğıt açıldığı zaman mesajın harfleri, kıvrımlar üzerine yazıldığı için noktalar ve çizgiler olarak görünmektedir. Ancak tam bir güvenliğin sağlanması için bu nokta ve çizgilerin tam harflere dönüştürülmesi gerektiğini belirtmiştir. Bununla beraber İbn Duneynîr, bu yöntemin daha önce farklı bir konu hakkında yazılmış olan bir kâğıdın arka kısmına da uygulanabileceğini söylemiştir. Böylece pililerle bulunan nokta ve harf parçaları, sayfanın ıslakken katlandığı ve bu yüzden arka tarafında bu şekilde lekelerin oluştuğu izlenimi verecektir (Alam ve diğerleri ,2005: 130).

İbnü'd-Dureyhim ise bu yöntemi, kâğıdın üst ve alt ucunun ortada birleştirilerek mesajın tam olarak bu kısma yazılması şeklinde ele almıştır. Böylece kâğıt açıldığı zaman mesajın gizlenmesi amaçlanmaktadır. Ancak İbnü'd-Dureyhim, kâğıdın kalan kısımlarına gereksiz kelimeler yazılarak gizliliğin artırılması hakkında bir şey söylememiştir. Bununla beraber, bu yöntemin aslında gerçek bir şifreleme olmadığını bu sebeple çözümlenmesinin sağlam bir sağ duyu yapılabileceğinden bahsetmiştir (Alam ve diğerleri 2003b: 82).

3.1.2.2.3. Satranç Tahtası ile Şifreleme

Yöntem, alfabedeki harflerin sırayla satranç tahtasındaki karelere yazılı olduğunun varsayılması ve satranç taşının sırasıyla mesajdaki harflere denk gelen karelere getirilmesiyle uygulanmaktadır. İbn Duneynîr bu yöntemi, karşılıklı satranç oynayan iki kişiden mesajı iletmek isteyen satranç taşını sırayla mesajın harflerine denk gelen karelere hareket ettirdiği şeklinde tasvir ederek anlatmıştır (Alam ve diğerleri, 2003b: 66, 2005: 120-122).

3.1.2.2.4. Delikli Tahta ile Şifreleme

Bu yöntemde şifreli metin, mesajın harflerini temsil eden deliklerden geçirilen bir ip ile temsil edilmektedir. Yöntemi uygulamak için bir tahtaya mesajın alfabesinde bulunan

harf sayısı kadar delik açılır ve her deliğin alfabenin bir harfini temsil ettiği varsayılır. Daha sonra bir iplik alınır ve sırayla mesajda bulunan harflerin temsil ettiği deliklerden geçirilir. Bu şekilde alıcı kişiye mesajın iletilmesi amaçlanır. Mesajı çözmek için ipliğin son geçirildiği delikten ilk geçirildiği deliğe doğru sırayla harflerin tespit edilmesi gerekmektedir. İbn Duneynîr ve İbnu'd-Dureyhim eserlerinde bu yöntemle yer vermiş ve her ikisi de örnek olarak “Ahmet” ismini kullanmışlardır. İbn Duneynîr şifreleme yaparken normal alfabe sırasını tercih ederken İbnu'd-Dureyhim ise sayısal alfabe sırasını tercih etmiştir (Alam ve diğerleri, 2003b: 68, 2005: 132).

3.1.2.2.5. Renkli Boncuklar ile Şifreleme

Yöntemde mesajın harfleri renkli boncuklar aracılığı ile temsil edilmektedir. Şifreleme, mesajdaki harflerin sırasına uyumlu olacak şekilde boncukların tıpkı bir tespih gibi ipe teker teker dizilmesiyle gerçekleştirilmektedir. Yöntemin çözümleme algoritması en fazla kullanılan rengin 1, bir sonrakinin ise 2 harfini temsil ettiği varsayımına dayanmaktadır. Benzer şekilde diğer boncuklar da bulunma sıklıklarına göre takip edilerek kalan harflerle eşleştirilirler. İbn Duneynîr aynı renkteki boncuklara ayırt edici bir işaret konularak farklı harflerin temsil edebileceğini belirtirken İbnu'd-Dureyhim daha farklı bir yol izlemiştir. Boncuk kullanımını daha fazla detaylandıran İbnu'd-Dureyhim, alfabedeki bazı harflerle eşleştirdiği renkleri örnek olarak vermiştir. Görünüşe göre alfabedeki harf sayısı kadar farklı renkte boncuğun bulunmasının zorluğunu göz önünde bulunduran İbnu'd-Dureyhim aynı renkli boncukların ikişerli ve üçerli kullanılmasıyla farklı harflerin temsil edilebileceğini belirtmiştir. Beyaz renkli boncukların ise kelimeler arasında boşluk görevi görebileceğini ifade etmiştir. Bununla birlikte her harf için farklı renkte boncuğun kullanılmasının ve kullanılacak ipliğin de ipekten olmasının daha iyi olacağını da eklemiştir (Alam ve diğerleri, 2003b: 80, 2005: 134).

Sonuç itibariyle her iki müellifin de yazdıkları göz önüne alındığında, her harf için ayrı renkte boncuk kullanımı, aynı renkli boncukların ikişerli ve üçerli kullanımı ve farklı şekilde işaretlenmiş aynı renkteki boncukların kullanımı olmak üzere üç farklı şekilde yöntemin uygulanabileceği ortaya çıkmaktadır.

3.2. YÖNTEMLERİN ARAPÇA ÖRNEKLERİ

Bir araç kullanılarak yapılan şifreleme yöntemlerine kâğıt üzerinde uygulamanın zorluğundan ötürü örnek verilmemiştir.

3.2.1. Anlamın Gizlenmesine Dayalı Şifreleme Örnekleri

Anlamın gizlenmesi başlığı altında ele alınan yerine koyma, yer değiştirme, ekleme ve çıkarma, birleştirme ve ayırma alt başlıkları altında verilen örneklerde aşağıdaki metnin şifrelemesi yapılmıştır.

والواجب على الناظر في كتب العلوم إذا كان غرضه معرفة الحقائق أن يجعل نفسه خصما لكل ما ينظر فيه ويجعل فكره في متنه وفي جميع حواشيه ويخصمه من جميع جهاته ونواحيه ويتهم أيضا نفسه عند خصامه فلا يتحامل عليه ولا يتسمح فيه فإنه إذا سلك هذه الطريقة انكشفت له الحقائق وظهر ما عساه وقع في كلام من تقدمه من التّقصير والشّبه.

“Bizim yükümlülüğümüz, bilginin en yakınını almak, en meşhur ve yakın olanına erişmek, uzmanlarının bildirdiklerini toplamak, bunlar içinde doğrulayabildiklerimizi doğrulayıp, geri kalanlarını olduğu gibi terk etmek ve bütün bunları Allah’ın iradesi ve yardımıyla doğrunun taliplisi ve bilgelik sevdalısı kimselere faydalı olsun ve onları bize mümkün olmayan başarıya yönlendirsın diye yapmaktır.” (İbnu’l Heysem, Kitabul Menazir)

3.2.1.1. Harf ile Yerine Koyma Örnekleri

3.2.1.1.1. Düzenli Bir Kurala Bağlı Olarak

Açık metindeki her harf alfabe dizilişinde kendisinden sonra gelen 7. harfin yerine geçmiştir. Harflerin yeni değerleri aşağıdaki tabloda gösterilmiştir.

Tablo 4: Düzenli Bir Kurala Bağlı Olarak Arap Harflerini Eşleştirme

ا	ب	ت	ث	ج	ح	خ	د	ذ	ر
د	ذ	ر	ز	س	ش	ص	ض	ط	ظ
ز	س	ش	ص	ض	ط	ظ	ع	غ	ف
ع	غ	ف	ق	ك	ل	م	ن	ه	و
ق	ك	ل	م	ن	ه	و	ي		
ي	ا	ب	ت	ث	ج	ح	خ		

حذبحدسذ نبخ دبثدمظ وخ ارد دبببجت دطد ادث هطكج تنظور دبشيدخي دث خسنب ثوغج صقتد باب تد خثمظ
 وخج حخسخب واطج وخ ترثج حوخ ستخن شحدفخج حخصقتج تث ستخن سجدرج حثحدشخج حخرجت دخكد
 ثوغج نثض صقتج وبد خرشدتب نبخج حبد خرغتش وخج ودثج دطد غبا جطج دبلطخير دثافور بج دبشيدخي
 حمجظ تد نعدج حين وخ أبدت تث ريضتج تث دبريقظ حذبفج.

3.2.1.1.2. Düzenli Bir Kurala Bağlı Olmayarak

Açık metindeki her harf alfabadeki diğer harflerle rastgele eşleştirilmiştir. Harflerin yeni değerleri aşağıdaki tabloda gösterilmiştir.

Tablo 5: Düzenli Bir Kurala Bağlı Olmayarak Arap Harflerini Eşleştirme

ا	ب	ت	ث	ج	ح	خ	د	ذ	ر
ن	م	ا	و	ط	س	ع	ف	ض	ز
ز	س	ش	ص	ض	ط	ظ	ع	غ	ف
ب	ث	ق	د	ت	ح	غ	ي	ه	ر
ق	ك	ل	م	ن	ه	و	ي		
خ	ص	ك	ظ	ش	ج	ذ	ل		

ذئكذئطم يكل نكشنغز رل صام نكيكذظ نضن صنش هزتج ظيزرا نكسخلخ نش لطيك شرثج عدظن كصك ظن
 لشغز رلج ذلظلك رصزج رل ظاشج ذرل طظلي سذنقلج ذلعدطج ظش طظلي طجناج دشذئسلج ذلاجظ نلتن
 شرثج يشف عدنطج ركن لاسنظك يكلج ذكن لائظس رلج رنشج نضن تكص جضج نكحلخا نشصقرا كج
 نكسخلخ ذعجز ظن يثنج ذخي رل صكنظ ظش اخفظج ظش نكاخذلز ذئكمج

3.2.1.1.3. Harflerin Ebced Sisteminde Denk Oldukları Sayısal Değerlerin Tekrar Harfe Dönüştürülmesi

Açık metindeki her harf ebced sisteminde denk olduğu sayısal değeri korunacak şekilde başka harflerle temsil edilmiştir. Bu yöntemle hazırlanan harflerin yeni değerleri aşağıdaki tabloda gösterilmiştir. Şifreli metinde bu değerlerin bazıları kullanılmıştır.

Tablo 6: Arap Harflerinin Sayısal Değerlerinin Tekrar Harflere Dönüştürülmesi

ا	ب	ج	د	هـ	و	ز	ح	ط
1	2	3	4	5	6	7	8	9
	اا	اب	باا الب جا بب	دا بااا جاا جب	بد جج ببب ها	او به جد ببج	بو زا جه دد ابه	بز حا جو هد الز بجد هجا
ي	ك	ل	م	ن	س	ع	ف	ص
10	20	30	40	50	60	70	80	90
طا بح جز دو هه بجه ابجد بببب اجو ابز	اطي بجي يجز يود بجههيج حجهد زجدو ججدو يججد وزز يي	كي كطا كحب يحزه يههي طذري حزهي ححدي كزج يططب يبهه	لي كيجب كيزج كك كلهه كطحج لود بيك بيطزد	مي مطا ككي كيك لك ليهه لحزه كييود لههي كيجب مهه	ني نهه مك لكي ككك لكزج ممي نود	سي مل مكي لكيي نك للي سهه	عي سك نل مم ملي سيي لللك نكي ليم	في عك سل نم ممي ملك
ق	ر	ش	ت	ث	خ	ذ	ض	ظ
100	200	300	400	500	600	700	800	900
صي فك عل سم نن مني ملكي عكي	قق قصي قفك قل قسم قنن قنمي قسكك قعكي	رق رصي رفك رعل رسم رنن رعكي ققعل	شق رر شصي شفك شعل شنن شسم شفيي	تق شر ررق شقق تصي	ثق تر شش شرق تقنن ثنن ثصي ثفك	خق ثر تش خنن ششق ترق خسم	ذق خر تش تت تشق ذنن	ضق ذر خش ثت ششش
غ								
1000								
ظق ثث ضر نش خت تتر								

بداكي جج اباا. سي كطا طا. ا كطا مي ا ضق قق. عي بح. يجر شق اا. ا يحزه مكى يههي ببب كك. ا خق ا. يود
 ا ليهه. ثث قصي ذق باا. كطحج مكى قعل مم شفك. ا حزهى جه فك ا ججه عل. اككي. ابجد بالكيى حزهى. ليهه
 ملي مك جاا. تقنن نم لود ا. ححدي ججدو كزج. بيطزد ا. بببب كييود خش قسم. ملي اجو جب. ها بجه با جز كي.
 سك بجههيج قق دا. لللك طا. كلهه شسم ليهه جب. بد سبي بح. بالي اجو نك. دد بد ا رعل دودا. ببب بببب شش ممى
 كك جب. كيحب كييحب. بالود ابجد للى. با دا ارر باا. بد لههي جج ادد هه جب. ها بجه شفيى جاا بيطزد. ا ابجد
 ذنن ا. لحه سبي ككك جب. سهه مهه بب. ثفك عك اييك جاا. لللك ححيد ا. جز شصي ابه اكيهه ييهه. مكى كزج
 بح جب. جج ححيد ا. هه شق ميى ييك دد. نكي ابجد دا. ليم ا ليهه جب. ا ششق ا. نود كطا يجر. جاا خسم باا. ا
 ححدي هجا قنمي هه منى شعل. ا لك يي رعي عى شعل. كزج دا. ا يططب دد منى ا دو صى. ببب ششش جب
 قق. ييك ا. سهه نهه ا دا. جج نن للى. مم هه. وزز كزج اييك. بيطزد كييحب. ررنن بب كك جب. لي مي. اكي
 شفك سم سل جز قسم. ها ا كطا ققعل اا دا.

3.2.1.1.4. Harflerin Ebced Sisteminde Denk Olduğu Sayısal Değerlere Çarpma İşlemi Uygulanıp Tekrar Harfe Dönüştürülmesi

Açık metindeki her harfin yerine, ebced sisteminde denk olduğu sayısal değeri dört ile çarpılarak elde edilen yeni değerine denk başka harfler konulmuştur. Bu yöntemle hazırlanan harflerin yeni değerleri aşağıdaki tabloda gösterilmiştir. Şifreli metinde bu değerlerin bazıları kullanılmıştır.

Tablo 7: Arap Harflerinin Sayısal Değerlerinin Değiştirilerek Tekrar Harflere Dönüştürülmesi

ط	ح	ز	و	هـ	د	ج	ب	ا
9	8	7	6	5	4	3	2	1
36	32	28	24	20	16	12	8	4
لو لها لج كبو كيج لدب كحد	لب كب كد بيد كهدج كههب كهجد	كج كد بيج كهج كوب بيهج	كد كب بيد بيجا حج يجج يود حد	ك بي بهه يجز يجب يود حد	يو حج يجج حبو بيد	يب وو دد حد حيب	ح دد هج وب ججب	د بب جا بالا
ص	ف	ع	س	ن	م	ل	ك	ي
90	80	70	60	50	40	30	20	10
360	320	280	240	200	160	120	80	40
شس شمك رقمك رصل رفف رصع رقتي	شك شبي رقك رصل رقم رعن رسمك رعمي	رف رنل ققف قصص رمم رسك رعي	رم ققم ففف قصن صفع قعسي ركك رلي	ر قق قصي ققك قل قسق قن ققم صصك ععس	قس سس قمك صع فف قلل عنم فمم ننس صصي	سس قك صل قيي مم عن فم ننك صكي فكك	ف مم لك ملي ملهه ملحب مكك مكيهه للي	لي كك لود لججد كيود بيبي لهه كيهه
ظ	ض	ذ	خ	ث	ت	ش	ر	ق
900	800	700	600	500	400	300	200	100
3600	3200	2800	2400	2000	1600	1200	800	400
غغغغ غغظ غغضض غغغغغ	غغغر غغظش غغضت غغذث غغغخ غغغغن	غغض غغظظ غغذت غغذق غغغر غغغش غغظظق	غغذ غغغش غغغر غغظث غغغخ غغذ غغظق	غغ غغظق غغضر غغش غغذ غغث	غغ غغظق ظذ ضض غغر غغش غغضي غغن ظظق	غر ظش ضت ذث خخ غغصي ظرق ضشق	ض ذت ذق خر ثش ثشق ذنن خغصي ترر	ت رر شق شصي شقك شعل شسم شنن
								غ
								1000
								4000
								غغغغ غغغظق غغغضر غغغذش غغغذت غغغث

كد د سس كيب بب يب ح. رف قك كك. با صل ر د غغغ ض. شك لي. مم غخ ح. بب قبي رف مم بب قس. جا غغض با. للك د قق. غغغظق تت غغغر بهه. ففق قف تش شبي غثق. بب عن كحد ت د لججد رر. جا قعل. بببي ددد رمم ننك. قسم رفم صفع ححد. غغت شمك فمم سس. صكي ملي قبي. قس جا. لهه قنن غغضض خر. رسس كيهه ك. حح لججد حد لهه قك. رفم ملهه خر يحب. رعن كيهه. قلال ضض قعل يود. بب رقا كيهه. ددد ننس لي رسك. كههب ببجا د نث كك ححد. كيب لود غظث رفف صسي يجز. قس قسم. وو قلال لججد رنل. ددد بي بب ضض ححد. كد قفك يودد بب بببي ك. بب كيهه غتر يحب ننس. با كك غغذث جا. ر رعن رم بي. رنل قعل بب. غغض رصع د قلال ححد. شك عن جا. كيود غشش كهجد بب فمم فم. رسك مم لهه ك. يودد ننك د. لهه ظذ ركك سسم كيب. شبي لود بي. رصل د فمم ك. بب غغجرا. قعسي صكي مم. يود غظظ ححد. با سس لها ذق كك رر ظذ. د قنن ف خخ رفم غتر. صكي ك. د عن لب ت بب لي شف. ببجا غغغثق ححد ض. صع د. رعي رلي فم بهه. كيب شق رسك. شك لهه. للك قبي د عنم. فف قق. ظخق شسم يو قلال بي. صع صصك. د مم غخ شسم شس لورخر. كد د سس ضت دد يود.

3.2.1.1.5. Harflerin Yerine Okunuşlarının Konulması

Açık metindeki harflerin okunuşları sırayla bir düz ve bir ters olacak şekilde yazılarak şifrelenmiştir. Aşağıdaki tabloda harflerin okunuşlarının düz ve tersten yazılışları verilmiştir.

Tablo 8: Arap Harflerinin Düz ve Ters Okunuşları

HARFLER	DÜZ HALİ İLE OKUNUŞLARI	TERS HALİ İLE OKUNUŞLARI
ا	ليف	فيلأ
ب	باء	ءاب
ت	تاء	ءات
ث	ثاء	ءاث
ج	جيم	ميمج
ح	حاء	ءاح
خ	خاء	ءاخ
د	دال	لاد
ذ	ذاء	ءاذ
ر	راء	ءار
ز	زاي	ياز
س	سين	نيس
ش	شين	نیش
ص	صاد	دلص
ض	ضاد	داض
ط	طاء	ءاط
ظ	ظاء	ءاظ
ع	عين	نيع
غ	غين	نيغ
ف	فاء	ءاف
ق	قاف	فاق
ك	كاف	فاك
ل	لام	مال
م	ميم	ميم
ن	نون	نون
ه	هاء	ءاه
و	واو	واو
ي	ياء	ءاي

واو فيلا لامواو اليغميجباء نيعلامفيلاليفمالنوفيلاطاءار فاءاي كافءاتباء فيلالامنيعلامواوميم فيلاذافيلاكافيلانون
 نيغراءداضهءا ميمعينءار فاءءات اليفمالحاءفاقاليفءايقاف فيلانون ءايجمينيعلام نونفاءنيسهءا ءاخصادميماليف
 مالكامال ميمفيلال ياءنونظاءار فاءءايهءا واوباءميجباءمال فاءفاكرءاءا فاءاي ميمءاتنونءاه واوءافياء
 ميجميمءايعين ءاواوفيلاشينءايهءا واوباءءاخصادميمهءا ميمنون ميميمءايعين ميجهءافيلاتاءءاه
 واونونواوفيلاحءاءايهءا واوباءءاتهاءميم اليفءايضادفيلال نونءافسينءاه عينونءال ءاخصادفيلاميمهءا فاءمالاليف
 ءايتاءءاحاليفميام نيعلامءايهءا واوامفيلال ياءءاتسينميجءا ءافياءءاه فاءفيلانونءاه اليفءاذاليف نيسلامفاك
 هاءءاهءا فيلالامءاطراءءايقافءات اليفنونكافنيشفاءءات لامءاه اليفمالءاحفاقاليفءايقاف واوظاءءاهراء ميماليف
 نيعسينفيلاهءا واوقافنيغ فاءاي كافمالاليغميم ميمنون تاءفاقدالميمهءا ميمنون فيلالامءاتقافداصياءار
 واوفيلالامنيشباءءاه

3.2.1.1.6. Kelime Aralarına Bir Çeşit Harf Konulması

Açık metinde kelime aralarındaki boşluklara س harfi konulmuştur.

والواجبعليلالناظر سفيستبسالعلومساذاساكنسغرضهسمعر فةسالحقائقسانسيجعلسنفسهسخصماسلكسماسينظر
 فيهسو بجيلسفر هسفيستمتنهسو فيسجميعسحواشيهسو يخصمهسمنسنسجهاثهسو نو احيهسو يتهمسايساضانسفسه
 عندسخصمامهسفلاسيتحاملسعليهسو لاسيتسمحسفيهسفيانسهساذاساسلكسهذ هسالطريقهسانكشفتسلهسالحقائقسو ظهر
 ماسعسا هسو قعسفيستكلامسمنستقدهسمنسالنقصير سو الشبه.

3.2.1.1.7. Kelime Aralarına Birden Çeşitli Harflerin Konulması

Açık metinde kelime aralarındaki boşluklara س, ك ve ن harfleri konulmuştur.

والواجبعليلالناظر سفينكتبسالعلومكاذاساكنسغرضهكمعر فةسالحقائقناكييجعلسنفسهسخصماكلكلنماكينظر سفيه
 وبجيانفكر هكفيسمتنهسو فينجميعكحواشيهسو يخصمهمنكجميغناثهسو نو احيهنو يتهمكايساضانفسهسندسخصمامه
 فلانيتحاملسعليهكو لانيتسمحكفيهكفانسهساذاانسلكسهذ هنالطريقهسانكشفتكلهسالحقائقنو ظهر كماسعسا هنو قعكفينكلام
 منستقدهمكمنكالنقصير سو الشبه.

3.2.1.2. Sembol ile Yerine Koyma Örnekleri

3.2.1.2.1. Her Harf Yerine Bir Sembol Konulması

Açık metindeki harflerin yerine aşağıdaki tabloda kendileriyle eşleştirilen semboller konulmuştur.

Tablo 9: Arap Harflerinin Semboller ile Temsil Edilmesi

ر	ذ	د	خ	ح	ج	ث	ت	ب	ا
θ	Δ	Π	μ	υ	ℵ	η	δ	ψ	ξ
ف	غ	ع	ظ	ط	ض	ص	ش	س	ز
∇	⊗	Γ	τ	φ	ə	κ	ϖ	χ	Φ
		ي	و	ه	ن	م	ل	ك	ق
		α	&	β	ε	X	ω	Ξ	∪

∪αξ∪υωξ δ∇θΓX βəθ⊗ εξΞ ξΔξ X&ωΓωξ ψδΞ α∇ θτξεωξ ξαΓ ψℵξ&ωξ& εξ
ωΓℵα ΓαXℵ α∇& βεδX α∇ βθΞ∇ ωαℵα& βα∇ θτεα ξX ωΞω ξXκμ βχ∇ε
βαϖξ&υ βXκμα& βδξβℵ ΓαXℵ εX βXξκμ ΠεΓ βχ∇ε ξəαξ Xβδα& βαυξ&ε&
ξω& βαωΓ ωXξυδα ξω∇ δ∪αθφωξ βΔβ Ξωχ ξΔξ βεξ∇ βα∇ υXχδα δ∇ϖΞεξ
Γ∪& βξχΓ ξX θβτ& ∪αξ∪υωξ βω βXΠ∪δ εX XξωΞ α∇ θακ∪δωξ εX βψϖωξ&.

3.2.1.2.2. Belirlilik Takısı (ل) Yerine Ortak Bir Sembolün Konulması

Açık metinde belirlilik takısının (ل) geçtiği yerlerde ϕ sembolü konulmuştur.³⁴

∪αξ∪υ ϕ δ∇θΓX βəθ⊗ εξΞ ξΔξ X&ωΓ ϕ ψδΞ α∇ θτξε ϕ ξαΓ ψℵξ& ϕ &
ΓαXℵ α∇& βεδX α∇ βθΞ∇ ωαℵα& βα∇ θτεα ξX ωΞω ξXκμ βχ∇ε ωΓℵα εξ
βXξκμ ΠεΓ βχ∇ε ξəαξ Xβδα& βαυξ&ε& βδξβℵ ΓαXℵ εX βXκμα& βαϖξ&υ
βω δ∇ϖΞεξ δ∪αθφ ϕ βΔβ Ξωχ ξΔξ βεξ∇ βα∇ υXχδα ξω& βαωΓ ωXξυδα ξω∇
βψϖ ϕ & θακ∪δ ϕ εX βXΠ∪δ εX XξωΞ α∇ Γ∪& βξχΓ ξX θβτ& ∪αξ∪υ ϕ

³⁴ 2.1'deki şifreleme baz alınarak oluşturulmuştur. Tek farkı Belirlilik takısının olduğu yerlere ϕ sembolün yerleştirilmiş olmasıdır.

3.2.1.2.3. Belirlilik Takısı (ال) Dışında Sıklıkla Beraber Kullanılan Harfler Yerine Ortak Bir Sembol Konulması

Arap dilinde sıklıkla beraber kullanılan ve metinde geçen bu harflerin yerine aşağıdaki tabloda gösterilen semboller konulmuştur.³⁵

Tablo 10: Arap Dilinde Sıklıkla Birlikte Kullanılan Bazı Harfler ve Örnekte Temsil Edildikleri Semboller

أن	ما	في	مم	لا	ال
*	~	⊗	∞	π	∅
على	هذه	إذا	عند	علي	إن
φ	≅	≈	#	◇	*

ωΓΝα * ∪αξ∪ ∅ δ∇θΓX β∅θ⊗ *Ξ ξΔξ X&ωΓ ∅ ψδΞ ⊗ θτξε ∅ φ ψΝξ& ∅ &
βXκμα& βαϰξ&υ ΓαXΝ ⊗& βεδX ⊗ βθΞ∇ ωαΝα& β⊗ θτεα ~ ωΞω ξXκμ βχ∇ε
ωXξυδα π∇ βXξκμ βχ∇ε ξαξ Xβδα& βαυξ&ε& βδξβΝ ΓαXΝ ∞
βξχΓ ~ θβτ& ∪αξ∪ ∅ βω δ∇ϰΞ* δ∪αθφ ∅ ≅ Ξωχ ≈ β*∇ β⊗ υXχδα π& β◇
.βψϰ ∅ & θακ∪δ ∅ ∞ βXΠ∪δ ∞ XπΞ ⊗ Γ∪&

3.2.1.2.4. Kelime Aralarına Bir Çeşit Sembol Konulması

Açık metinde kelime aralarındaki boşluklara < sembolü konulmuştur.

εξ∪αξ∪ωξ<δ∇θΓX<β∅θ⊗<εξΞ<ξΔξ<X&ωΓωξ<ψδΞ<α∇<θτξεωξ<ξαΓ<ψΝξ&ωξ&
ΓαXΝ<α∇<βεδX<α∇<βθΞ∇<ωαΝα&<βα∇<θτεα<ξX<ωΞω<ξXκμ<βχ∇ε<ωΓΝα
ΠεΓ<βχ∇ε<ξαξ<Xβδα&<βαυξ&ε&<βδξβΝ<ΓαXΝ<εX<βX<κμα&<βαϰξ&υ
δ∪αθφωξ<βΔβ<Ξωχ<ξΔξ<βεδ∇<βα∇<υXχδα<ξω&<βαωΓ<ωXξυδα<ξω∇<βXξκμ
εX<βXΠ∪δ<εX<XξωΞ<α∇<Γ∪&<βξχΓ<ξX<θβτ&<∪αξ∪ωξ<βω<δ∇ϰΞεξ
.βψϰωξ&<θακ∪δωξ

³⁵ 2.1'deki şifreleme baz alınarak oluşturulmuştur. Farkı, genellikle beraber kullanılan harfler için de ayrıca sembollerin konulmasıdır.

3.2.1.2.5. Kelime Aralarına Çeşitli Sembollerin Konulması

Açık metinde kelime aralarındaki boşluklara ∞ , $\pm$, $\neq$ ve $\langle$ sembolleri konulmuştur.

$\neq \delta \nabla \theta \Gamma X \langle \beta \ni \theta \otimes \infty \xi \Xi \pm \xi \Delta \xi \neq X \& \omega \Gamma \omega \xi \langle \psi \delta \Xi \infty \alpha \nabla \pm \theta \tau \xi \varepsilon \omega \xi \neq \xi \alpha \Gamma \pm \psi \mathbb{N} \xi \& \omega \xi \&$
 $\alpha \nabla \infty \beta \theta \Xi \nabla \pm \omega \alpha \mathbb{N} \alpha \& \neq \beta \alpha \nabla \pm \theta \tau \varepsilon \alpha \infty \xi X \pm \omega \Xi \omega \neq \xi X \kappa \mu \langle \beta \chi \nabla \varepsilon \infty \omega \Gamma \mathbb{N} \alpha \pm \varepsilon \xi \cup \alpha \xi \cup \omega \xi$
 $\beta \alpha \cup \xi \& \varepsilon \& \langle \beta \delta \xi \beta \mathbb{N} \pm \Gamma \alpha X \mathbb{N} \langle \varepsilon X \neq \beta X \neq \kappa \mu \alpha \& \langle \beta \alpha \pi \xi \& \cup \neq \Gamma \alpha X \mathbb{N} \neq \alpha \nabla \& \infty \beta \varepsilon \delta X$
 $\beta \alpha \nabla \langle \cup X \chi \delta \alpha \pm \xi \omega \& \neq \beta \alpha \omega \Gamma \infty \omega X \xi \cup \delta \alpha \pm \xi \omega \nabla \infty \beta X \xi \kappa \mu \langle \Pi \varepsilon \Gamma \infty \beta \chi \nabla \varepsilon \neq \xi \ni \alpha \xi \pm X \beta \delta \alpha \&$
 $\beta \xi \chi \Gamma \infty \xi X \langle \theta \beta \tau \& \pm \cup \alpha \xi \cup \omega \xi \pm \beta \omega \pm \delta \nabla \pi \Xi \varepsilon \xi \langle \delta \cup \alpha \theta \phi \omega \xi \infty \beta \Delta \beta \infty \Xi \omega \chi \pm \xi \Delta \xi \neq \beta \varepsilon \xi \nabla$
 $\cdot \beta \psi \pi \omega \xi \& \infty \theta \alpha \kappa \cup \delta \omega \xi \pm \varepsilon X \neq \beta X \Pi \cup \delta \langle \varepsilon X \infty X \xi \omega \Xi \langle \alpha \nabla \neq \Gamma \cup \& \neq$

3.2.1.3. Sayı ile Yerine Koyma Örnekleri

3.2.1.3.1. Harflerin Yerine Ebcad Sistemindeki Sayı Karşılıklarının Konulması

Açık metindeki harflerin yerine ebcad sisteminde denk oldukları sayı değerleri konulmuştur.

Tablo 11: Arap Harflerinin Ebcad Sistemindeki Sayısal Değerleri									
ي	ط	ح	ز	و	هـ	د	ج	ب	ا
10	9	8	7	6	5	4	3	2	1
ر	ق	ص	ف	ع	س	ن	م	ل	ك
200	100	90	80	70	60	50	40	30	20
		غ	ظ	ض	ذ	خ	ث	ت	ش
		1000	900	800	700	600	500	400	300

50120 17001 4063070301 240020 1080 200900150301 13070 23163016
14090600 5608050 3070310 501 1001011008301 400802007040 58002001000
10806 55040040 1080 52002080 30103106 51080 2009005010 140 302030

405400106 510816506 5400153 7010403 5040 54090600106 510300168 7010403
1306 5103070 30401840010 13080 540190600 45070 5608050 1800101
400100102009301 57005 203060 17001 550180 51080 8406040010
5040 4013020 1080 701006 516070 140 20059006 1001011008301 530
523003016 2001090100400301 5040 5404100400

3.2.1.3.2. Harflerin Yerine Yeni Belirlenen Sayısal Değerlerin Konulması

Açık metindeki harflerin yerine yeni belirlenen sayı değerleri konulmuştur. Bu değerler aşağıdaki tabloda gösterilmiştir.

Tablo 12: Arap Harflerinin Rastgele Sayısal Değerler ile Temsil Edilmesi									
ا	ب	ج	د	هـ	و	ز	ح	ط	ي
400	50	600	9	4	300	800	7	60	900
ك	ل	م	ن	س	ع	ف	ص	ق	ر
5	70	100	700	20	10	1	30	90	1000
ش	ت	ث	خ	ذ	ض	ظ	غ		
200	8	2	80	500	6	40	3		

100300701070400 5085 9001 10004040070070400 4007010 5060040070400300
700400 9090040090770400 81100010100 4610003 7004005 400500400
49001 100040700900 400100 70570 4001003080 4201700 7010600900
49002004003007 10900100600 9001300 47008100 9001 4100051 70600900300
49007400300700300 484004600 10900100600 700100 41003080900300
7010040078900 400701 41004003080 970010 4201700 4006900400 10048900300
45004 57020 400500400 47004001 49001 7100208900 40070300 49007010
400100 1000440300 9090040090770400 470 812005700400 89090010006070400
700100 41009908 700100 100400705 9001 1090300 44002010
45020070400300 10009003090870400

3.2.1.4. Kelime ile Yerine Koyma Örnekleri

3.2.1.4.1. Harflerin Yerine Ebcad Sistemindeki Sayısal Değerlerinin Okunuşlarının Konulması

Açık metindeki harflerin yerine ebcad sisteminde denk oldukları sayısal değerlerin okunuşları konulmuştur. Her harf virgül ile birbirinden ayrılmıştır.

Tablo 13: Arap Harflerinin Ebcad Sistemindeki Sayısal Değerlerinin Okunuşları

ز	و	هـ	د	ج	ب	ا
7	6	5	4	3	2	1
سبعة	ستة	خمسة	أربعة	ثلاثة	اثنان	واحد
ن	م	ل	ك	ي	ط	ح
50	40	30	20	10	9	8
خمسون	أربعون	ثلاثون	عشرون	عشرة	تسعة	ثمانية
ش	ر	ق	ص	ف	ع	س
300	200	100	90	80	70	60
ثلاثمائة	مِئتان	مئة	تسعون	ثمانون	سبعون	ستون
غ	ظ	ض	ذ	خ	ث	ت
1000	900	800	700	600	500	400
ألف	تسعمئة	ثمانمائة	سبعمئة	ستمئة	خمسمة	أربعمئة

ستة، واحد، ثلاثون، ستة، واحد، ثلاثة، اثنان، سبعون، ثلاثون، عشرة، واحد، ثلاثون، خمسون، واحد، تسعمئة، مِئتان،

ثمانون، عشرة، عشرون، أربعمئة، اثنان، واحد، ثلاثون، سبعون، ثلاثون، ستة، أربعون، واحد، سبعمئة، واحد، عشرون، واحد، خمسون، ألف، مِئتان، ثمانمائة، خمسة، أربعون، سبعون، مِئتان، ثمانون، أربعمئة، واحد، ثلاثون، ثمانية، مئة، واحد، عشرة، مئة، واحد، خمسون، عشرة، ثلاثة، سبعون، ثلاثون، خمسون، ثمانون، ستون، خمسة، ستمئة، تسعون، أربعون، واحد، ثلاثون، عشرون، ثلاثون، أربعون، واحد، عشرة، خمسون، تسعمئة، مِئتان، ثمانون، عشرة، خمسة، أربعة، عشرة، ثلاثة، عشرة، ثلاثون، ثمانون، عشرون، مِئتان، خمسة، ثمانون، عشرة، أربعون،

أربعمئة، خمسون، خمسة، ستة، ثمانون، عشرة، ثلاثة، أربعون، عشرة، سبعون، ثمانية، ستة، واحد، ثلاثمئة، عشرة، خمسة، ستة، عشرة، ستمئة، تسعون، أربعون، خمسة، أربعون، خمسون، ثلاثة، أربعون، عشرة، سبعون، ثلاثة، خمسة، واحد، أربعمئة، خمسة، ستة، خمسون، ستة، واحد، ثمانية، عشرة، خمسة، ستة، عشرة، أربعمئة، خمسة، أربعون، واحد، عشرة، ثمانمئة، واحد، خمسون، ثمانون، ستون، خمسة، سبعون، خمسون، أربعة، ستمئة، تسعون، واحد، أربعون، خمسة، ثمانون، ثلاثون، واحد، عشرة، أربعمئة، ثمانية، واحد، أربعون، ثلاثون، سبعون، ثلاثون، عشرة، خمسة، ستة، ثلاثون، واحد، عشرة، أربعمئة، ستون، أربعون، ثمانية، ثمانون، عشرة، خمسة، ثمانون، واحد، خمسون، خمسة، واحد، سبعمئة، واحد، ستون، ثلاثون، عشرون، خمسة، سبعمئة، خمسة، واحد، ثلاثون، تسعة، مئتان، عشرة، مئة، أربعمئة، واحد، خمسون، عشرون، ثلاثمئة، ثمانون، أربعمئة، ثلاثون، خمسة، واحد، ثلاثون، ثمانية، مئة، واحد، عشرة، مئة، ستة، تسعمئة، خمسة، مئتان، أربعون، واحد، سبعون، ستون، واحد، خمسة، ستة، مئة، سبعون، ثمانون، عشرة، عشرون، ثلاثون، واحد، أربعون، خمسون، أربعمئة، مئة، أربعة، أربعون، خمسة، أربعون، خمسون، واحد، ثلاثون، أربعمئة، مئة، تسعون، عشرة، مئتان، ستة، واحد، ثلاثون، ثلاثمئة، اثنان، خمسة.

3.2.1.4.2. Harflerin Yerine Bir Kategoriye Ait İsimlerin Konulması

Açık metindeki her harfin yerine ilişkilendirilmiş oldukları kuş isimleri konulmuştur. Bu isimler aşağıdaki tabloda gösterilmiştir. Kelimeler arasındaki boşluklar ise وقواق (guguk kuşu) ismi ile temsil edilmiştir.

Tablo 14: Arap Harflerinin Kuş İsimleri ile Temsil Edilmesi

ا	ب	ج	د	هـ
Güvercin	Kumru	Saksağan	Kırlangıç	Şahin
حمامة	قُمري	عقّعق	سنونو	شاهين
و	ز	ح	ط	ي
Ebabil	Çavuş Kuşu	Sığircık	Kartal	Çayır Kuşu
ابابيل	هدهد	زرزور	عقاب	قُنبرة
ك	ل	م	ن	س
Karga	Doğan	Serçe	Tahtalı	Gökkuzgun
غراب	باز	عصفور	حمام مطوق	شقراق
ع	ف	ص	ق	ر
Bülbül	Karatavuk	Telli turna	Baykuş	Martı
بلبل	شحرور	كركي	بومة	نورس
ش	ت	ث	خ	ذ
Muhabbet Kuşu	Kızıl gerdan	Saka kuşu	Kanarya	Ağaçkakan
بادجي	أبو الحنّاء	حسن	كناري	نقار الخشب
ض	ظ	غ		
Yeşilbaş	Ulu doğan	İbibik		
البط البري	صقر الغزال	هدهد		

ابابيل حمامة باز ابابيل حمامة عقّعقُ مري وقواق بلبل باز حمامة وقواق حمامة باز حمام مطوق حمامة صقر الغزال نورس وقواق شحرورُ نبرة وقواق غراب أبو الحنّاء قُمري وقواق حمامة باز بلبل باز ابابيل عصفور وقواق حمامة نقار الخشب حمامة وقواق غراب حمامة حمام مطوق وقواق هدهد نورس البط البري شاهين وقواق عصفور بلبل نورس شحرور أبو الحنّاء وقواق حمامة باز زرزور بومة حمامة قُنبرة بومة وقواق حمامة حمام مطوق وقواق قُنبرة عقّعق بلبل باز حمام مطوق شحرور شقراق شاهين وقواق كناري كركي عصفور حمامة وقواق باز غراب باز وقواق عصفور حمامة وقواق نبرة حمام مطوق صقر الغزال نورس وقواق شحرور قُنبرة شاهين وقواق ابابيل قُنبرة عقّعق

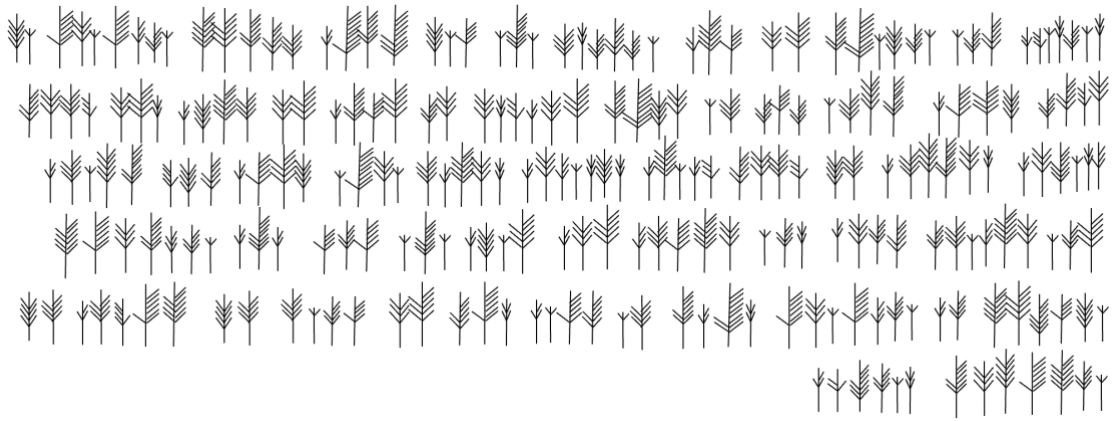
قُنْبَرَة باز وقواق شحرور غراب نورس شاهين وقواق شحرور قُنْبَرَة وقواق عصفور أبو الحنّاء حمام مطوق شاهين وقواق ابابيل شحرور قُنْبَرَة وقواق عقق عصفور قُنْبَرَة بلبل وقواق زررور ابابيل حمامة بادجي قُنْبَرَة شاهين وقواق ابابيل قُنْبَرَة كناري كركي عصفور شاهين وقواق عصفور حمام مطوق وقواق عقق عصفور قُنْبَرَة بلبل وقواق عقق شاهين حمامة أبو الحنّاء شاهين وقواق ابابيل حمام مطوق ابابيل حمامة زررور قُنْبَرَة شاهين وقواق ابابيل قُنْبَرَة أبو الحنّاء شاهين عصفور وقواق حمامة قُنْبَرَة البط البري حمامة وقواق حمام مطوق شحرور شقراق شاهين وقواق بلبل حمام مطوق سنونو وقواق كناري كركي حمامة عصفور شاهين وقواق شحرور باز حمامة وقواق قُنْبَرَة شقراق عصفور زررور وقواق شحرور قُنْبَرَة شاهين وقواق شحرور حمامة مطوق شاهين وقواق حمامة نقار الخشب حمامة وقواق شقراق باز غراب وقواق شاهين نقار الخشب شاهين وقواق حمامة باز عقاب نورس قُنْبَرَة بومة أبو الحنّاء وقواق حمامة مطوق غراب بادجي شحرور أبو الحنّاء وقواق باز شاهين وقواق حمامة باز زررور بومة حمامة قُنْبَرَة بومة وقواق ابابيل صقر الغزال شاهين نورس وقواق عصفور حمامة وقواق بلبل شقراق حمامة شاهين وقواق ابابيل بومة بلبل وقواق شحرور قُنْبَرَة وقواق غراب باز حمامة عصفور وقواق عصفور حمام مطوق وقواق أبو الحنّاء بومة سنونو عصفور شاهين وقواق عصفور حمام مطوق وقواق حمامة باز أبو الحنّاء بومة كركي قُنْبَرَة نورس وقواق ابابيل حمامة باز بادجي قُمري شاهين.

3.2.1.5. Dallı Alfabe ile Yerine Koyma Örneği

Açık metindeki her harfin yerine dallı alfabenin harfleri konulmuştur. Aşağıdaki tabloda Arap harflerine karşılık gelen dallı harfler gösterilmiştir.

Tablo 15: Arap Harflerinin Dalli Alfabenin Harfleri ile Temsil Edilmesi

و	ه	د	ج	ب	ا
ل	ك	ي	ط	ح	ز
م	ن	س	ع	ف	ص
ق	ر	ش	ت	ث	خ
ذ	ض	ظ	غ		



3.2.1.6. Sembolik Resimler ile Yerine Koyma Örneđi

Açık metindeki her harf bir meyve veya sebze ismi ile eşleştirilmiştir. Her harfin yerine aşağıdaki tabloda gösterildiđi şekilde kendisi ile eşleştirilen meyve veya sebze emoji³⁶ konulmuştur.

³⁶ Duygu, fikir ve nesneleri sembolik olarak ifade etmek için kullanılan küçük resim ya da simgelere verilen isimdir.

Tablo 16: Arap Harflerinin Meyve ve Sebze Emojileri ile Temsil Edilmesi

Harf	Şekil	Arapça	Türkçe
ا		أُجَاص	Armut
ب		بَطِيخَة	Karpuz
ج		جُوز الهند	Hindistan Cevizi
د		جزر	Havuç
ه		بادنجان	Patlıcan
و		اس برّي	Yaban Mersini
ز		مانجو	Mango
ح		الفلل المَحْشِي	Dolmalık Biber
ط		طماطم	Domates
ي		يوسفي	Mandalina
ك		كرز	Kiraz
ل		لَيْمُون	Limon
م		موز	Muz
ن		كيوي	Kivi
س		خَسْ	Marul
ع		عنب	Üzüm
ف		فراولة	Çilek
ص		بصل	Soğan
ق		بروكولي	Brokoli
ر		فُلُّل أَحْمَر	Kırmızı Biber
ش		شَمَام	Kavun
ت		تَفَاح	Elma
ث		ثوم	Sarımsak
خ		خَوْخَة	Şeftali
ذ		بطاطا	Patates
ض		اناناس	Ananas
ظ		افوكادو	Avokado
غ		خيار	Salatalık



3.2.1.7. Harflerin Çevresindeki Harflere Göre Yer Değiştirme Örnekleri

Açık metindeki kelimeler tekli, ikili ve dörtlü olacak şekilde ayrılarak aşağıdaki şekillerde şifrelenmiştir.

3.2.1.7.1. Tek Kelime İçerisinde

- Kelimenin baştaki harflerinin sırayla kendilerine karşılık gelen sondaki harfleriyle değiştirilmesi:

بجالواو يلع رطانلا يف بتك مولعلا اذا ناك هضرغ تفرعم قياقحلا نا لعجي هسفن امصخ للك ام رظني هيف
ليجيو هرکف يف هنتم يفو عيمج هيشاوح همصخيو نم عيمج هتاهج هياونو مهتيو اضيا هسفن دنع هماصخ
الف لماحتي هيلع وال حمستي هيف هناف اذا کلس هذه تقيرطلا تفشکنا هل قياقحلا رهظو ام هاسع عقو يف
مالک نم همدقت نم ريصقتلا هبشلاو.

- Kelimenin son harfinin en başa yazılması:

بوالواج يعل رالناظ يف بکت مالعلو اذ نکا هغرض تمعرف قالحقاي نا لیجع هنفس اخصم للک ام رینظ هفي
لويجي هفکر يف همتن يوف عجمي هحواشي هويخصم نم عجمي هجهات هونواحي مويته الايص هنفس دعن
هخصام افل ليتحام هعلي اول حيثسم هفي هفان اذ کسل ههذ تالطريق تانکشف هل قالحقاي روظه ام هعسا عوق
يف مکلا نم هتقدم نم رالتقصي هوالشب.

- Kelimenin ilk harfi ile son harfinin yerlerinin değiştirilmesi:

بالواجو يلع رلناظا يف بتك ملعلوا اذا ناك هرضع تعرفم قلحقايا نال جعي هفسن اصمخ لكل ام رنظي هيف ليجيو
هكر ف هتتم يفو عميج هواشيح هيخصمو نن عميج ههاتج هنواحيو ميتهو أيضا هفسن دنع هصامخ الف
لتحامي هليع الو حتسمي هيف هانف اذا كلس هذه تلطريقا تنكشفا هل قلحقايا رظهو ام هساع عقو يف ملاك نم
هقدمت نم رلتقصيا هالشبو.

d. Kelimenin ilk harfi ile üçüncü harfinin yer değiştirilmesi:

لاوواجب يلع نلاظر في بتك عللوم اذا ناك ضرغه رعمفة حلاقايق ان عجيل سفنه مصخا لكل ما ظنير هيف جيويل
ركفه في نتمه يفو يجمع اوحييه خيوصمه من يجمع اهجتة ونواحيه تيوهم ضياا سفنه دنع اصخمه اقل حتيامل يلعه
اول ستيح هيف نافه اذا كلس هذه طلاريقة كناشفت له حلاقايق هظور ما اسعه عقو في الكم من دقتمه من تلاقصير
لاوشبه.

e. Kelimedeki harflerin ikişerli olarak ayrılması ve her ikili harfin bir önceki iki harfin önüne getirilmesi:

لوواجب علي نالظر في كتب عللوم اذا كان ضهغر رفمعة حقالايق ان عليج سهنف ماخص لكل ما ظرين فيه
جيويل رهفك في نهتم وفي يعجم اشحويه خصوصيه من يعجم اتجهه اونوحيه تهويم ضالي سهنف عند امخصه
فلا حايتمل يهعل ولا سميتح فيه نهفا اذا سلك هذه طراليقة كناشفت له حقالايق هروظ ما هاعس وقع في امكل من
دمتقه من تقالصير لشوابه.

f. Kelimedeki çift sıradaki harflerle tek sıradaki harflerin yerlerinin değiştirilmesi:

اوولجاب لعي لانرظ يف تكب لالعمو اذا اكن رغهض عمفرة لاقحيق نا جيلع فنهس صخام كلل ام نيرظ يفه
يوبجل كفهر يف تمهن فوي مجعي وحشاهي يوصخهم نم مجعي هجتاه نواويحه يوهتم يااض فنهس نعد صخماه
لفا تياحلم لعيي لوا تيمسح يفه افهن اذا لسك ذهه لارطقية ناشكتف هل لاقحيق ظوره ام سعاها قوع يف لكما نم
قتمه نم لاقتيصر اوشلهب.

g. Kelimenin baştaki harflerinden sonra sırayla sondaki harflerinin getirilmesi:

وباجلاو عيل ارلظنا في كبت املوعل اذا كنا غهرض متعفر اقلحاق ان يلجع نهفس خاصم للك ما يرنظ فهي
ولييج فهكر في مهتن ويف جمعي جهوياش وهيمخص من جمعي جههتا وهنيوفا وميهت الايض نهفس عدن

خهصما فال يلتما عهلي وال يحتمس فهي فهان اذ سكل ههذ اتلقطير انتفكش له اقليحاق ورظه ما عهسا وعق في كملا من تهقمذ من ارليتصق وهابلش.

h. Kelimenin sonundaki harflerin sırayla baştaki harflerinin önüne getirilmesi:

بوجالو يعل راطلان يف بكت ماوللع اذ نكا هغضر تمفر قايلاحق نا ليعج هنسف اخمص للك ام ريطن هفي لوييج هفرك يفه منت يوف عجم هجوشا هوميصخ نم عجم هجتها هوينحوا موهيت اضي هنسف دعن هخمصا افل ليמתاح هعيل اول حيمتس هفي هفنا اذ كسل ههذ تاقلطر تافنشك هل قايلاحق روهظ ام هعاس عوق يف مكال نم هتمقد نم رايلتصق هوباشل.

3.2.1.7.2. İki Kelime Arasında

a. Birinci kelimenin ilk harfi ile ikinci kelimenin ilk harfinin değiştirilmesi:

عالوجب ولي فلناظر اي اتب كلعلوم كذا ان مرضه غعرفة الحقايق ان نجعل يفسه لصما خكل يا منظر ويه فيجبل فكره في وتنه مفي جميع جواشيه ميخصمه ون جميع جهاته ونواحيه ويتهم نيضا افسه خند عصامه يلا فتامل وليه علا فتسمح بيه انه فذا هلك سذه الطريقة انكشفت اه للحقايق مظهر وا وساه عقع كي فلام تن مقدمه ان ملتقصير والشبه.

b. Birinci kelimenin son harfi ile ikinci kelimenin son harfinin değiştirilmesi:

والواجي علب الناظي فر كتم العلوب اذن كاا غرضة معرفه الحقايق اق يجعه نفسل خصمل لكا مر ينظا فيل ويجيه فكري فه متني وفه جميعه حواشيع ويخصمن مه جميعه جهاتع ونواحيه ويتهو هبضا نفسا عنه خصامد فلل يتحاما عليا وله يتسمه فيح فانا اذه سله هذك اطريقت انكشفت لق الحقايق وظها مر عساع وقه فم كلاي مه تقدمن مر التقصين والشبه.

c. Birinci kelimenin ilk harfi ile ikinci kelimenin son harfinin değiştirilmesi:

يالوجب علو يلناظر فا متب العلوك نذا كاا ترضه معرفغ نلحقايق اا هجعل نفسي لصما لكخ را ينظم ليه ويجيف يكره فف يتنه وفم جميع حواشيع نيخصمه مو جميع جهاتع منواحيه ويتهو هبضا نفسا هند خصامع للا يتحامف اعليه ولع هتسمح فيني انه اذف هلك هذس تلطريقة انكشفا فه الحقايا اظهر مو عساه وقع مي كلاف هن تقدمن رن التقصيم والشبه

d. Birinci kelimenin son harfi ile ikinci kelimenin ilk harfinin deęiştirilmesi:

والواقع بلي الناظف ري كذا بلعلوم اذك ان غرضم معرفة الحقايا فن يجعن لفسه خصمل اكل مي انظر فيو
هيجيل فكرف هي متنو هفي جميع عواشيه ويخصم هن جميع عهاته ونواحيو هيتهم ايضن افسه عنخ دصامه
فلي اتحامل عليو هلا يتسمف حيه فانا هذا سله كذا الطريقا تنكشفت لا هلقايق وظهم را عساو هقع فك يلام مت
نقدمه ما نلتقصير والشبه.

e. Birinci kelimenin ilk harfi ile ikinci kelimenin ilk harfi, birinci kelimenin son harfi ile de ikinci kelimenin son harfinin deęiştirilmesi:

عالواحي ولب فلناظي ار اتم كلعلوب كذن اا مرضة غعرفه الحقاين اق نجعه يفسل لصمل خكا ير منظا ويل
فيجيه فكري فه وتني مفه حميه جواشيع ميخصمن وه جميعه جهاتع ونواحيم ويتيه نيضه افسا خنه عصامد يلل
فتحاما وليا عله فتسمه ييح انا فذه هله سذك الطريقت انكشفة اق للحقايه مظهر ور وساع عقه كم فلاي ته مقدمن
ار ملتقصين والشبه.

f. Birinci kelimenin ilk harfi ile ikinci kelimenin son harfi, birinci kelimenin son harfi ile de ikinci kelimenin ilk harfinin deęiştirilmesi:

ويااللوناظير عفلي كمتابذا الكعالنو غارلضحهقما عيرققاتن يخجصعملانلفكسله مياهيونيظجريفل فتكنر ههوففييم
جهمويييعخخصوماهشمين جومايحيجههوايتتههومن اعينضداخنصفاسمهه فللعالبيتحوالما يفتاسنمهافذايه
سيلقكتهاذنهكاشلفطتر لقهاوظلهرقماي عفسياكهلو اقم مناتلقتدقمصهيمر والشبه.

3.2.1.7.3. Bir Kelime Grubu İçerisinde

Açık metindeki kelimeler öncelikle dörüü gruplara ayrılmıştır. ³⁷ Her grubun ilk harfi yazıldıktan sonra üç harf atlanarak sıradaki harf yazılmıştır. Gruptaki tüm harfler bitene kadar bu işlem tekrar başa dönerek devam ettirilmiştir.

³⁷ Toplam 61 kelimeden oluşan metin 4'e eşit olarak bölünemediğı için son kelimeye herhangi bir işlem yapılmamıştır.

Açık metindeki her β ve ∇ sembolünden sonra γ sembolü, her Γ ve $\&$ sembolünden sonra ise $\bullet$ sembolü eklenmiştir. ³⁸

$\delta\gamma\nabla\theta\bullet\Gamma X\ \gamma\beta\exists\theta\otimes\ \varepsilon\xi\Xi\ \xi\Delta\xi\ X\bullet\&\omega\bullet\Gamma\omega\xi\ \psi\delta\Xi\ \alpha\gamma\nabla\ \theta\tau\xi\omega\xi\ \xi\alpha\bullet\Gamma\ \psi\aleph\xi\bullet\&\omega\xi\bullet\&$
 $\alpha\gamma\nabla\ \gamma\beta\theta\Xi\gamma\nabla\ \omega\alpha\aleph\alpha\bullet\&\ \gamma\beta\alpha\gamma\nabla\ \theta\tau\epsilon\alpha\ \xi X\ \omega\Xi\omega\ \xi X\kappa\mu\ \gamma\beta\chi\gamma\nabla\epsilon\ \omega\bullet\Gamma\aleph\alpha\ \varepsilon\xi\ \cup\alpha\xi\cup\omega\xi$
 $\gamma\beta\delta\xi\gamma\beta\aleph\ \bullet\Gamma\alpha X\aleph\ \epsilon X\ \gamma\beta X\kappa\mu\alpha\bullet\&\ \gamma\beta\alpha\omega\xi\bullet\&\cup\ \bullet\Gamma\alpha X\aleph\ \alpha\gamma\nabla\bullet\&\ \gamma\beta\epsilon\delta X$
 $\gamma\beta\alpha\omega\bullet\Gamma\ \omega X\xi\cup\delta\alpha\ \xi\omega\gamma\nabla\ \gamma\beta X\xi\kappa\mu\ \Pi\epsilon\bullet\Gamma\ \gamma\beta\chi\gamma\nabla\epsilon\ \xi\exists\alpha\xi\ X\gamma\beta\delta\alpha\bullet\&\ \gamma\beta\alpha\cup\xi\bullet\&\epsilon\bullet\&$
 $\cup\alpha\xi\cup\omega\xi\ \gamma\beta\omega\ \delta\gamma\nabla\omega\Xi\varepsilon\xi\ \delta\cup\alpha\theta\phi\omega\xi\ \gamma\beta\Delta\gamma\beta\Xi\omega\chi\ \xi\Delta\xi\ \gamma\beta\varepsilon\xi\gamma\nabla\ \gamma\beta\alpha\gamma\nabla\ \cup X\chi\delta\alpha\ \xi\omega\bullet\&$
 $\gamma\beta\psi\omega\xi\bullet\&\ \theta\alpha\kappa\cup\delta\omega\xi\ \epsilon X\ \ \gamma\beta X\Pi\cup\delta\ \epsilon X\ X\xi\omega\Xi\ \alpha\gamma\nabla\ \bullet\Gamma\cup\&\ \gamma\beta\xi\chi\bullet\Gamma\ \xi X\ \theta\gamma\beta\tau\bullet\&$

3.2.1.10. Harf Tekrarlama Örneği

Açık metindeki kelimelerin harfleri sırayla üç ve iki kere tekrarlanarak yazılmıştır.

و وواللواااجبببععلليي الالانناظظرر فففي كككتتببب اللالععللوومم اذاااا ككاانن غغغررضضضهه
مممععررففةة الالححققاايقق انن ييبجبععل ننففسسهه خخصصمما للالكلمم ماما بيبينظظر
فففيهه ووويجبجلل ففككررهه فففي مممتتننهه وووفيي ججمبييع ححووااششبيهه
ووويخخصصمهه ممنن ججمبييع ججههااتهه ووونووالاحديهه ووويتتههمم اايضضا
ننففسسهه ععنندد خخصصاممهه ففللاا يبيتتححاممل ععلليهه ووللاا بيتتسسصح فففيهه
ففااننه اذااا سسللك ههذهه اللططررييقةة الانككشففت لله الالححققاايقق وووظظههر
مما ععسااهه وووقعهه فففي ككللامم ممنن تتقدهمهه ممنن التتقصصييرر ووواللششبيهه.

3.2.1.11. Harflerin Çıkarılması Örnekleri

3.2.1.11.1. Harflerin Tek Tek Çıkarılması ile

Açık metindeki tüm ل, م, ط ve ف harfleri çıkartılmıştır.

واوجب على الناظر في كتب احوالهم ان كان غرضه معرفة الحقائق أن يجمع نفسه خصا كذا ينظر فيه ويجري كرهه في تنهيه ويجمع حواسه ويخصصه من جميع جهاته ونواحيه ويته ايضا نفسه عند خصاصها يتحاشى به ويتسحر به إنه إذا سلك هذه الطريقة انكشفت له الحقائق وظهر له عسا وقعه كما ن تقدمه ان التصدير واشبه.

³⁸ 2.1'deki şifreleme baz alınarak oluşturulmuştur.

3.2.1.11.2. Yazılışları Benzer Olan Harflerin Tek Bir Harf Üzerinden Temsil Edilmesi ile

Açık metindeki noktasız halde yazılışları aynı olan harfler, belirlenen ortak bir harf tarafından temsil edilmiştir. Aşağıdaki tabloda gösterildiği üzere bu şifrede ، ذ، خ، ح، ز، harfleri kullanılmamıştır.

Tablo 17: Yazılışları Benzer olan Arap harflerinin ortak bir harf ile temsil edilmesi

ا	ب	ت	ث	ج	ح	خ	د	ذ	ر
ج	ي	ي	ي	ل	ل	ل	م	م	ط
ز	س	ش	ص	ض	ظ	ظ	ع	غ	ف
ط	و	و	ر	ر	ا	ا	ن	ن	ه
ق	ك	ل	م	ن	ه	و	ي		
د	ع	ب	ف	ق	س	ص	ك		

صحبصجلي نيك جبجباط هك عيي جبنبصف جمج عجق نطرس فنطهي جبادجكد جق كلنب قهوس لرفج
بعب فج كقاط هكس صكالكب هعطس هك فيقس صهك لفكن لصجوكس صكلرفس فق لفكن لسجيس
صقصجلكس صكيسف جكرج قهوس نقم لرجفس هيج كيلجفب نبكس صبح كيوفل هكس هجقس جمج وب
سمس جباطكدي جقعوهي بس جبادجكد صاسط فج نوجس صدن هك عبجف فق يدمفس فق جببدركت
صحبويس.

3.2.1.11.3. Yazılışları Benzer Olmayan Harflerin Tek Bir Harf Üzerinden Temsil Edilmesi ile

Açık metinde yazılışları benzer olmayan bazı harfler belirlenen ortak bir harf tarafından temsil edilmiştir. Aşağıdaki tabloda gösterildiği üzere bu şifrede ب ve ط harfleri و harfi ile، ذ ve م harfleri ح harfi ile، ظ ve ف harfleri ج harfi ile، ل ve و harfleri ise س harfi ile temsil edilmiştir. Dolayısıyla şifreli metinde د، ف، ط ve ل harfleri kullanılmamıştır.

Tablo 18: Bazı Arap Harflerinin Ortak Bir Harf Tarafından Temsil Edilmesi

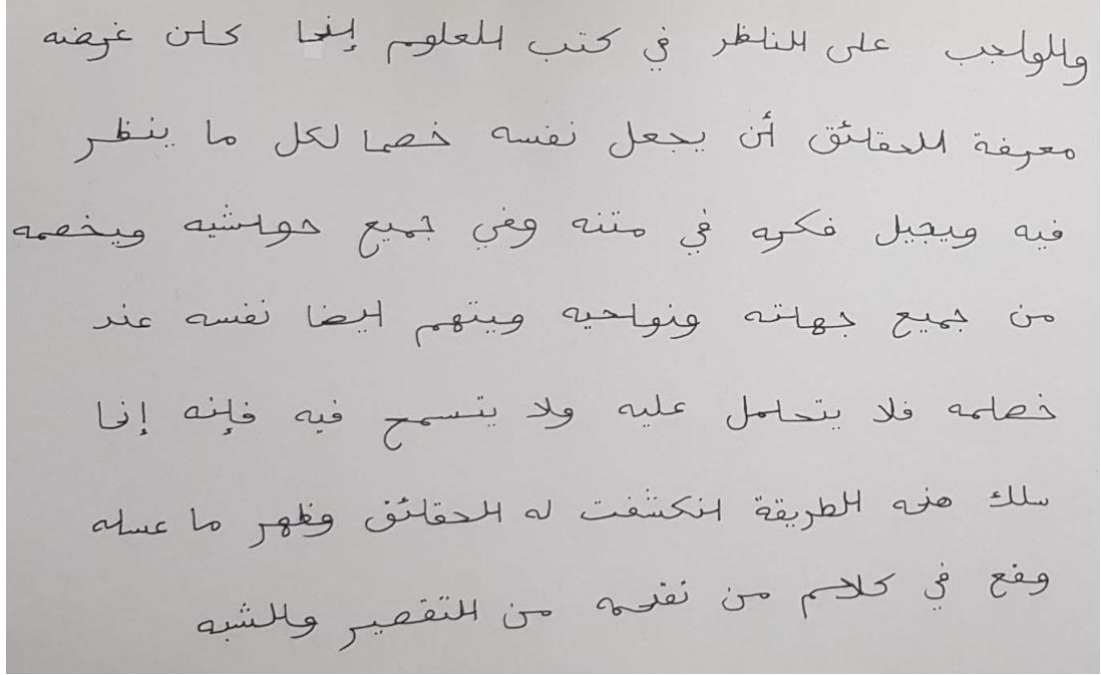
ا	ب	ت	ث	ج	ح	خ	د	ذ	ر
ذ	و	ش	ا	ي	ق	ظ	ح	ه	ص
ز	س	ش	ص	ض	ط	ظ	ع	غ	ف
ع	ن	ث	خ	ك	و	ج	م	ر	ج
ق	ك	ل	م	ن	ه	و	ي		
ت	ز	س	ح	ض	ب	س	غ		

سذسذيو مسع ذسضذجص جع زشو ذسر سسح ذهذ زذض رصكب حمصجش ذسقتذغت ذض غيمس ضجذب ظخذ
 سزس حذ غضجص جغب سغيغس جزصب جغ حشضب سجغ يحغم قسذثغب سغظخب حض يحغم ييذشب
 سضسذقغب سغشبح ذغكد ضجذب مضح ظخذجب جسذ غشقرحس مسغب سسذ غشحق جغب جذضب ذهذ نسز
 بهب ذسوصغتش ذضزثجش سب ذسقتذغت سجبص حذ منذب ستم جغ زسذح حض شتحب حض ذسشتخغص
 سذسثوب.

3.2.1.12. Ayrı Yazılan Harfleri Birleştirme Örneği

Şifre, Arap alfabesinde sondan birleşmeyen ا، و، د، ذ، ر، ز harflerinin kendisinden sonra gelen harflere birleşik olarak yazılması ile oluşturulmuştur

Resim 4: Ayrı Yazılan Harflerin Birleşik Yazılması



3.2.1.13. Birleşik Yazılan Harfleri Ayırma Örneği

Şifre Arap alfabesinde sondan birleşerek yazılan harflerin ayrı yazılması ile oluşturulmuştur.

والواجب على الناظر في كتب العلوم إنما كان غرضه معرفة الحقائق أن يجعل نفسه خصاصا لكل ما ينظر فيه ويحيل فكره في مكنه وفي جميع خواشيه ويخصه من جميع جهاته ونواحيه ويتهم أيضا نفسه عند خطمه فلا يتحامل عليه ولا يتسمح فيه فإنه إذا سلك هذه الطريقة انكشفت له الحقائق وظهر ما عساه وقع في كلام من نغمه من التقصير والشبه

3.2.2. Şifrenin Gizlenmesine Dayalı Şifreleme Örnekleri

Kurgulayarak yapılan şifreleme yöntemleri başlığı altında ele alınan yöntemlerde, ebced değerinden kelime üretme yöntemi dışındaki tüm yöntemlerin örneklendirilmesinde نصر من الله وفتح قريب (Allah'ın yardımı ve yakında gerçekleşecek bir zafer) cümlesinin şifrelemesi yapılmıştır.

3.2.2.1. Bir Kategori ile İlişkilendirme Örnekleri

3.2.2.1.1. Harflerin Farklı Kategorilere Ait İsimlerle İlişkilendirilmesi

Aşağıdaki tabloda Arap alfabesindeki harflerin eşleştirildikleri kategori isimleri verilmiştir. Her kategori ismi eşleştirilmiş olduğu harf ile başlamaktadır. Bu yöntem ile oluşturulan şifreli metinlerde, harfler eşleştirilmiş oldukları kategorilere ait bir isim ile temsil edilmekte ve sadece mesajın harfleri kadar isim bulunmaktadır.

Tablo 19: Arap Harflerine Karşılık Gelen Kategori İsimleri

Harf	Kategorisi	Anlamı
ا	أنام	Kişi isimleri
ب	بقول	Bitki isimleri/ Kuru baklagiller
ت	تمور/ تراب / توابل	Hurma/ Toprak/ Baharat isimleri
ث	ثياب	Kıyafet isimleri
ج	جلود	Deriden yapılmış bir şey
ح	حبوب / حديد	Tahıl çeşitleri veya demirden yapılmış bir şey
خ	خشب	Ahşaptan yapılmış bir şey
د	دواب / دهان	Hayvan/ merhem isimleri
ذ	ذهب	Altından yapılmış bir şey
ر	رياحين	Aromatik bitki isimleri
ز	زجاج	Camdan yapılmış bir şey
س	سلاح / سمك	Silah/ balık isimleri
ش	شهور / شطرنج/ شعور	Ay isimleri/ satranç oyunu/ saç ya da duygu ile ilgili bir şey
ص	صبوغ / صُفر / صوف/ صموغ	Boya/ pirinç/ yünden yapılmış bir şey veya yapışkan bir şey
ض	ضوء / ضياع	Işık ile ilgili bir şey veya bir bölge ismi
ط	طيور	Kuş isimleri
ظ	ظلام / ظباء	Karanlık ile ilgili bir şey/ antilop türleri
ع	عطر / عيون / عدد	Koku/ göz/ alet edevat ile ilgili bir şey
غ	غنم	Küçükbaş hayvanlar
ف	فواكه	Meyve isimleri
ق	قرى / قصب	Köy isimleri veya kamış ile ilgili bir şey
ك	كتب / كواكب	Kitap veya gezegen isimleri
ل	لبن	Süt veya süt ürünleri isimleri
م	مدن	Şehir isimleri
ن	نجوم / نحاس	Yıldız isimleri veya bakırdan yapılmış bir şey
و	وحوش / ورق	Vahşi hayvan/ kâğıt/ Para birimi isimleri
ه	هوام	Zararlı böcek isimleri
ي	يوافيت	Ziynet eşyaları

3.2.2.1.1.1. Bir Kısıtlamaya Bağlı Kalmadan Yapılan Şifreleme

Şifre, sırasıyla نصر من الله وفتح قريب cümlesindeki 17 harfin mensup olduğu kategoriye ait isimlerle kurgulanan bir metinden oluşmaktadır. Yöntem herhangi bir kısıtlamaya bağlı kalınmadan oluşturulduğu için 17 harfin her biri kendi kategorisinde herhangi bir harf ile başlayan bir isim ile temsil edilmiştir. Bu 17 harf için kullanılan isimler aşağıdaki tabloda gösterilmiş ve şifreli metinde kalın olarak yazılmıştır.

Tablo 20: Bir Kısıtlamaya Bağlı Kalmadan Yapılan Şifrelemede Kullanılan Kelimeler

Harf	Kategori	Kullanılan Kelime	Anlamı
ن	Bir yıldız ismi	أبرق	Sirius yıldızı
ص	Yünden yapılmış bir eşya	كنزة صوف	Yün kazak
ر	Bir aromatik bitki ismi	ورقة يانسون	Anason yaprağı
م	Bir şehir ismi	القاهرة	Kahire
ن	Bir yıldız ismi	أبرق	Sirius yıldızı
ا	Bir kişi ismi	أحمد	Ahmet
ل	Bir süt ürünü ismi	الحليب	Süt
ل	Bir süt ürünü ismi	الحليب	Süt
ه	Bir böcek ismi	جرادة	Çekirge
و	Bir vahşi hayvan ismi	أسداً	Aslan
ف	Bir meyve ismi	تُفاحاً	Elma
ت	Bir Hurma çeşidi	تَمَر المدينة	Medine hurması
ح	Bir tahıl ürünü	الخُبز	Ekmek
ق	Bir köy ismi	قرية النَّاصِرِيَّة	En-Nâsiye köyü
ر	Bir aromatik bitki ismi	الأقحوان	Papatya
ي	Bir ziynet eşyası	الأساور	Bilezik
ب	Bir sebze ismi	الفول	Bakla

بَيْنَمَا كَانَ يَسِيرُ تَحْتَ نَجْمٍ أَهْبَقَ لَاحِظًا أَنَّ عَلَى كَنْزَةِ صُوفٍ وَرَقَةً يَنْسُونُ. ظَنَّ أَنَّهُ مِنْ ذَلِكَ الَّذِي نَشَأُ فِي الْقَاهِرَةِ. وَلَكِي يَسْتَطِيعُ أَنْ يَرَاهُ بِشَكْلِ أَفْضَلٍ أَرَادَ أَنْ يَمُدَّ بَصَرَهُ نَاطِرًا إِلَى نَجْمٍ أَهْبَقَ مَرَّةً أُخْرَى. كَانَ شَدِيدَ التَّرْكِيزِ فِي ذَلِكَ الْوَقْتِ لِدَرَجَةٍ أَنَّهُ لَمْ يُدْرِكْ أَنَّ أَحْمَدَ كَانَ يَقْتَرِبُ مِنْهُ حَامِلًا الْحَلِيبَ الَّذِي حَلَبَهُ إِلَى أَنْ وَصَلَ إِلَى جَانِبِهِ وَرَأَى عَلَى الْحَلِيبِ جَرَادَةً، وَبِمَجَرَّدِ رُؤْيِيهِ صَرَخَ كَمَا لَوْ أَنَّهُ قَابِلٌ أَسَدًا وَجْهًا لَوَجْهِهِ. وَالَّذِينَ سَمِعُوا صَوْتَهُ أَتَوْا إِلَى جَانِبِهِ وَمِنْ أَجْلِ تَهْدِئَتِهِ أَعْطَوْهُ ثَفَاحًا وَتَمَرَ الْمَدِينَةِ وَقَلِيلًا مِنَ الْخُبْزِ. وَعِنْدَمَا هَذَا انْطَلَقَ مَرَّةً أُخْرَى إِلَى قَرْيَةِ النَّاصِرِيَّةِ وَمَعَهُ الْأَقْحَوَانُ لِبَيْعِ الْأَسَاوِرِ الَّتِي صَنَعَهَا مِنْهُ وَشِرَاءِ بَعْضِ الْفُولِ مُقَابِلَ ذَلِكَ.

Sirius Yıldızının altında yürürken, yün kazağının üzerinde bir anason yaprağının olduğunu fark etti. Kahire’de yetişenlerden olmalı herhalde diye düşündü. Onu daha iyi görebilmek için Sirius yıldızına doğru uzatarak bir daha bakmak istedi. O kadar dikkatliydi ki o sırada Ahmet’in sağdığı sütleri taşıyarak kendisine doğru geldiğini fark edememişti bile. Ta ki yanına gelip, sütün üzerindeki çekirgeyi görene kadar. Görür görmez, sanki bir aslanla karşı karşıya gelmiş gibi bağırdı. Sesini duyanlar hemen yanına gelip rahatlaması için elma, Medine hurması ve biraz ekmek uzattılar. Sakinleşince Nasıriye Köyüne doğru, papatyalardan yaptığı bilezikleri satıp karşılığında bir miktar bakla almak üzere tekrar yola koyuldu.

3.2.2.1.1.2. Alfabenin Bir Harfine Bağlı Kalarak Yapılan Şifreleme

Şifre, sırasıyla نصر من الله وفتح قريب cümlesindeki 17 harfin mensup olduğu kategoriye ait isimlerle kurgulanan bir metinden oluşmaktadır. Kısıtlama için alfabedeki “ب” harfi seçilmiştir. Dolayısıyla 17 harfi temsil eden tüm isimler kendi kategorisine ait olmak üzere “ب” harfi ile başlamıştır. Bu harfler için kullanılan isimler aşağıdaki tabloda gösterilmiş ve şifreli metinde kalın olarak yazılmıştır.

Tablo 21: Bir Kısıtlamaya Bağlı Kalarak Yapılan Şifrelemede Kullanılan Kelimeler

Harf	Kategori	Kullanılan Kelime	Anlamı
ن	Bir yıldız ismi	بقار	Nekkar yıldızı
ص	Boya ile ilgili bir şey	بویا	Boya
ر	Bir aromatik bitki ismi	بابونج	Papatya
م	Bir şehir ismi	بغداد	Bağdat
ن	Bir yıldız ismi	بيض	Beid Yıldızı
ا	Bir kişi ismi	بلال	Bilal
ل	Bir süt ürünü ismi	بوزا	Boza
ل	Bir süt ürünü ismi	بوطة	Dondurma
ه	Bir böcek ismi	بعوض سام	Zehirli sivrisinek
و	Bir vahşi hayvan ismi	بغل بري	Vahşi katır
ف	Bir meyve ismi	برتقال	Portakal
ت	Bir Hurma çeşidi	بلح	Olgunlaşmamış Hurma
ح	Bir tahıl ürünü	بُر	Buğday
ق	Bir köy ismi	بستان	Bostan
ر	Bir aromatik bitki ismi	بلسم	Melisa
ي	Bir ziynet eşyası	بروش	Broş
ب	Bir sebze ismi	بازلاء	Bezelye

قد أنار نجم البقار الشيء الذي تبدو حية كأنها مصبوغة ببويا وهي أزهار البابونج. وفي الطريق إلى بغداد بدأ نجم بيض بالظهور أيضا. في تلك اللحظة رأيت بلالا قادما إلى من الاتجاه المعاكس. شكرا له لقد جاء بي البوزة والبوطة. لكن حينما كنت على وشك الأكل تسلط البعوض سام علي. كما لو أن هذا لم يكن كافيا كان البغل البري قادما على وعاد بغنة. لقد أخافني هذا كثيرا. وأكرمت البرتقال والبلح والبر القليل لأستريح مباشرة. كلها تجيء من قرية بستان التي بلسمها مشهور. كنت أشعر جيدا بعد عندما قمت مرة أخرى لاحظت أنني أسقطت البروش. لكن لحسن الحظ كان البازلاء لا يزال هناك.

Nekkar yıldızı, sanki bir **boya** ile boyanmış kadar canlı görünen **papatyaları** aydınlatmıştı. **Bağdat şehrine** doğru giderken **Beid yıldızı** da artık görünmeye başlamıştı. O sırada karşıdan bana doğru gelen **Bilal**'i gördüm, sağ olsun benim için **boza** ve **dondurma** getirmişti. Ancak tam yemek üzereydim ki, **zararlı bir sivrisinek** bana musallat oldu. Bu da yetmezmiş gibi **vahşi bir katır** tam üzerime doğru gelirken son anda geri döndü. Bu beni çok korkutmuştu, hemen rahatlamam için bana **portakal, hurma** ve biraz **buğday** ikram edildi. Tüm bunlar **Bostan köyünden** geliyormuş hani **melisası** meşhur olan... Artık iyi hissediyordum, tekrar ayağa kalktığımda **broşumu** düşürdüğümü fark ettim ama neyse ki **bezelyeler** hala orada yerinde duruyordu.

3.2.2.1.1.3. Normal Alfabe Dizilişine Bağlı Kalarak Yapılan Şifreleme

Şifre, sırasıyla نصر من الله وفتح قريب cümlesindeki 17 harfin mensup olduğu kategoriye ait isimlerle kurgulanan bir metinden oluşmaktadır. 17 harf kendi kategorisine ait olmak şartıyla Arap alfabesinin diziliş sırasıyla başlamıştır. Bu harfler için kullanılan isimler aşağıdaki tabloda gösterilmiş ve şifreli metinde kalın olarak yazılmıştır.

Tablo 22: Normal Alfabe Dizilişine Göre Kullanılan Kelimeler

Harf	Kategori	Kullanılan Kelime	Anlamı
ن	Bir yıldız ismi	أَبْرَق	Sirius Yıldızı
ص	Pirinçten yapılmış bir eşya	البوصلة صفر	Pirinç pusula
ر	Bir aromatik bitki ismi	ثَابِل	Kışniş
م	Bir şehir ismi	ثُول	Suval
ن	Bir yıldız ismi	الجوزا	Orion takım yıldızı
ا	Bir kişi ismi	حَوَى	Havva
ل	Bir süt ürünü ismi	خَمِير الرَّائِبِ	Yoğurt mayası
ل	Bir süt ürünü ismi	دُنْدُرْمَة	Dondurma
ه	Bir böcek ismi	دُنَابَة	Sinek
و	Bir vahşi hayvan ismi	رَاكُون	Rakun
ف	Bir meyve ismi	زَبِيب	Kuru üzüm
ت	Bir Baharat ismi	سَعْتَر	Kekik
ح	Bir tahıl ürünü	شَعِير	Arpa tanesi
ق	Bir köy ismi	صَيِّدَا	Sayda Köyü
ر	Bir aromatik bitki ismi	صَرْغُ الْكَلْبَةِ	İğde
ي	Bir ziynet eşyası	طُوق	Kolye
ب	Bir bitki ismi	ظِيَّان	Kır yasemini

كَانَ يَذْهَبُ تَقْرِيْبًا إِلَى مَا يَقْرُبُ مِنْ بُعْدِ نَجْمِ أَبْرَقٍ لِلْحَصُولِ عَلَى الْبَوْصَلَةِ صَفَرِ الَّتِي يُرِيدُهَا. هُنَاكَ مَدِينَةٌ مَشْهُورَةٌ بِالتَّابِلِ وَهِيَ ثُولُ، لَقَدْ قَطَعَ طَرِيقًا طَوِيلَةً جِدًّا. نَظَرَ إِلَى نَجْمِ الْجُوزَاءِ وَقَالَ: أَعْتَقِدُ أَنَّي اقْتَرَبْتُ، خَطَرَ عَلَى عَقْلِهِ شَيْءٌ عَائِدٌ لِحَوَى هُوَ اسْتِخْدَامُ خَمِيرِ الرَّائِبِ لِصِنَاعَةِ الدُّنْدُرْمَةِ فَتَبَسَّمَ. وَلَمْ يُعِدْهُ إِلَى صَوَابِهِ إِلَّا رُؤْيَا ذُبَابٍ قَدْ حَطَّ عَلَى رَاكُونٍ مَرَّةً بِشَكْلِ مُفَاجِئٍ مِنْ أَمَامِهِ. وَادْرَكَ أَنَّهُ شَعَرَ بِالْجُوعِ فَمَرَّ لِيَتَنَاوَلَ زَبِيبًا وَسَعْتَرًا وَمَطْبُوحًا بِقَرِيَةِ صَيِّدَا. وَجَذَبَ انْتِبَاهَهُ عُشْبَةُ صَرْغِ الْكَلْبَةِ الْمَوْجُودَةُ بِكَثْرَةٍ هُنَاكَ. وَعِنْدَمَا كَانَ يَتَجَهَّزُ لِإِكْمَالِ طَرِيقِهِ مَرَّةً أُخْرَى لَاحَظَ أَنَّهُ قَدْ أَسْقَطَ طَوْقَهُ الَّذِي يَحْمِلُهُ مَعَهُ دَائِمًا بَيْنَ أَزْهَارِ الظِّيَّانِ، لَكِنْ لَمْ يَكُنْ بِمَقْدُورِهِ أَنْ يَفْعَلَ شَيْئًا إِذْ لَمْ يَعُدْ بِإِمْكَانِهِ الْعُودَةَ.

Neredeyse bir **Sirius yıldızı** kadar uzağa, o çok istediği **pirinç pusulayı** alabilmek için gidiyordu. Burası **kişnişleriyle** meşhur olan **Suval şehri** idi. Epey yol kat etmişti. **Orion'un yıldızlarına** baktı ve galiba yaklaşıyorum artık dedi. Aklına **Havva'nın yoğurt mayası** kullanarak **dondurma** yapmaya çalışması geldi, gülümsedi. Üzerinde konmuş **sineklerle** bir **rakunun** aniden önünden geçmesi onu kendine getirdi. Acıktığını fark etti. **Kuru üzüm** ve **kekikle** pişirilen **arpa tanelerini** yemek için **Sayda köyüne** uğradı. Burada fazlasıyla bulunan **iğdeler** dikkatini çekmişti. Yola çıkmak için tekrar hazırlandığında her zaman yanında taşıdığı **kolyesini**, **kır yaseminlerinin** arasında düşürdüğünü fark etti. Ama yapacak bir şeyi yoktu. Artık geri dönemezdi.

3.2.2.1.1.4. Sayısal Alfabe Dizilişine Bağlı Kalarak Yapılan Şifreleme

Şifre, sırasıyla نصر من الله وفتح قريب cümlesindeki 17 harfin mensup olduğu kategoriye ait isimlerle kurgulanan bir metinden oluşmaktadır. 17 harf kendi kategorisine ait olmak şartıyla ebced diziliş sırasıyla başlamıştır. Bu harfler için kullanılan isimler aşağıdaki tabloda gösterilmiş ve şifreli metinde kalın olarak yazılmıştır.

Tablo 23: Sayısal Alfabe Dizilişine Göre Kullanılan Kelimeler

Harf	Kategori	Kullanılan Kelime	Anlamı
ن	Bir yıldız ismi	أبرق	Sirius yıldızı
ص	Pirinçten yapılmış bir eşya	بلوزة صوف	Yün bluz
ر	Bir aromatik bitki ismi	جوري	Gül
م	Bir şehir ismi	دمشق	Şam
ن	Bir yıldız ismi	هقعة	Meissa yıldızı
ا	Bir kişi ismi	واسيب	Vasip
ل	Bir süt ürünü ismi	زبدة	Tereyağı
ل	Bir süt ürünü ismi	حليباً	Süt
ه	Bir böcek ismi	طلح	Bir kene türü
و	Bir vahşi hayvan ismi	يغور	Jaguar
ف	Bir meyve ismi	كرزاً	Kiraz
ت	Bir Baharat ismi	لمسيّة	Ham hurma
ح	Bir tahıl ürünü	ملت	Arpa
ق	Bir köy ismi	ناعور	Naur Köyü
ر	Bir aromatik bitki ismi	سعتراً	Kekik
ي	Bir ziynet eşyası	عصمتي	Kolye
ب	Bir bitki ismi	فاصوليا	Fasulye

بينما كنت أفكر في نجم أبرق الذي تعرفت إليه مؤخراً كنت أحاول إيصال بلوزة صوف إلى حيث كنت سأخذها. وبينما رائحة جوري في كل مكان كنت في طريقي إلى دمشق. كان الأمر كما لو أن نجمة هقعة اقتربت كثيراً وأضاءت المكان كله. ورأيت واسيب قادماً نحوي حاملاً زبدة وحليباً. في تلك الأثناء مرّ أمامي بشكل سريع حيوان بريّ عليه طلح كثير، إنه يغور. تفاجأت كثيراً بما حدث فبدأت أركض وأصرخ. أولئك الذين سمعوني جاءوا إلي على الفور وقدموا لي كرزاً وتمر لمسي وقليلاً من ملت ومن قرية ناعور سعتراً لتهدئتي. وأدركت أنني أسقطت عصمتي بين شجيرات فاصوليا أثناء الركض ولكن فات أوان العودة.

Yeni öğrendiğim **Sirius yıldızını** düşünürken, **yün bluzu** götüreceğim yere yetişmeye çalışıyordum. Her tarafı saran **güllerin** kokusuyla birlikte **Şam**'a doğru ilerliyordum. Sanki **Meissa yıldızı** çok yakına gelmişse her yeri aydınlatmış gibiydi. Karşıdan **Vasip**'in **tereyağı** ve **süt** taşıyarak bana doğru geldiğini gördüm. Tam o sırada üzerinde bir sürü **kene** olan bir **Jaguar** önümden hızlıca geçti. Neye uğradığımı şaşırmıştım, bu yüzden bağırarak koşmaya başladım. Beni duyanlar hemen yanıma geldiler ve beni sakinleştirmek için **kiraz**, **hurma**, biraz **filizlendirilmiş arpa** ve **Naur**'dan gelen **kekik** ikram ettiler. Koşarken **kolyemi**, **fasulyelerin** arasında düşürdüğümü fark ettim ancak geri dönmek için artık çok geçti.

3.2.2.1.2. Harflerin Aynı Kategoriye Ait İsimlerle İlişkilendirilmesi

3.2.2.1.2.1. Harflerin Arazi Ölçü Birimleri ile İlişkilendirilmesi

Açık metindeki harfler arazi ölçü birimleri ile temsil edilmiştir. Ebced sistemindeki sayısal değerleri 1-9 arasında olan harfler m² ile, 10-90 arasında olan harfler aşır ölçü birimi³⁹ ile, 100-1000 arasında olan harfler ise kafiz⁴⁰ ölçü birimi ile, 1000 sayısına denk gelen ğ harfi ise cerib⁴¹ ölçü birimi ile temsil edilmektedir. Aşağıda verilen tabloya göre şifreli metindeki ölçü birimlerinin sırası takip edildiği zaman نصر من الله وفتح قريب cümlesini verecektir.

³⁹ 1 aşır = 100 m²'dir.

⁴⁰ 1 kafiz = 1000 m²'dir.

⁴¹ 1 Cerib = 10.000 m²'dir.

Tablo 24: Arap Harflerinin Arazi Ölçü Birimleri ile Temsil Edilmesi

ا	ب	ج	د	هـ
واحد متر مربع	اثنان متر مربع	ثلاثة متر مربع	أربعة متر مربع	خمسة متر مربع
1 m ²	2 m ²	3 m ²	4 m ²	5 m ²
و	ز	ح	ط	ي
ستة متر مربع	سبعة متر مربع	ثمانية متر مربع	تسعة متر مربع	واحد عشرين
6 m ²	7 m ²	8 m ²	9 m ²	1 aşîr
ك	ل	م	ن	س
اثنان عشرين	ثلاثة عشرين	أربعة عشرين	خمسة عشرين	ستة عشرين
2 aşîr	3 aşîr	4 aşîr	5 aşîr	6 aşîr
ع	ف	ص	ق	ر
سبعة عشرين	ثمانية عشرين	تسعة عشرين	واحد قفزان	اثنان قفزان
7 aşîr	8 aşîr	9 aşîr	1 kafîz	2 kafîz
ش	ت	ث	خ	ذ
ثلاثة قفزان	أربعة قفزان	خمسة قفزان	ستة قفزان	سبعة قفزان
3 kafîz	4 kafîz	5 kafîz	6 kafîz	7 kafîz
ض	ظ	غ		
ثمانية قفزان	تسعة قفزان	واحد جربان		
8 kafîz	9 kafîz	1 cerîb		

قول لك كتابيا معلومات زرع حقلي الذي استأجرت على احتمال النسيان أو الالتباس. أولا سيتم زرع الليمون على **خمسة عشرين** الذي على يمين المدخل من الأرض وبجواره سيزرع التفاح **تسعة عشرين** من الأرض. إذا سألت ماذا سيحدث للمنطقة المحاطة بالحجارة المقابلة اعلم لن يتم أي شيء عملا الآن هناك. لأن فيها **اثنان قفزان** من الكرز. سيزرع السفرجل **أربعة عشرين** من الأرض الذي بجانب هذه المنطقة. وسيزرع الموز **خمسة عشرين** من الأرض الذي بجانبه. فقط في هذه المنطقة يوجد **متر مربع واحد** الذي ليس مناسباً للزراعة. لذلك سوف يبقى هناك فارغا. هناك **منطقتان منفصلتان** تفصل بينهما **ثلاثة عشرين** و**ثلاثة عشرين** مقابل المنطقة التي سيزرع الموز. سيتم زراعة لتجربة في هذه المنطقة البرقوق والكيوي الذين هما نادران في هذا الاقليم. إذا لم يتم الحصول على المحصول المطلوب من هاتين الثمار، فسيتم دمجهما وسيتم زراعة الموز في هذه المنطقة. بمساحة **خمسة أمتار مربعة وستة أمتار مربعة** مساحات صغيرة بجوار النافورة ستستخدم كمستودعات لوضع المواد اللازمة. فسيتم زرع السفرجل **ثمانية عشرين** من الارض مقابل النافورة مباشرة. وفي هذه المساحات يوجد **خص ثمانية متر مربع** لاستريح فيه.

سيتم الزرع التمر الذي هو النتاج يكسبني أكثر مساحات واسعة في الاقصى أربعة قفران من الارض. سيتم دمج المساحتين التين قياسهما قفران واحد واثنان قفرانان وفي يمين باب الخروج وسيتم زرع العنب فيها. المكان الذي مقابل هذه المنطقة وميقاسه عشرين واحد واثنان متران مربع لأخي ولن يلمسه. حاولت أن أكتب كل خطة الحقل بشكل واضح. أتمنى أن يأتي بما فيه الخير لك.

Kiralamış olduğun tarlaman ekim bilgisini unutma ya da karıştırma olasılığına karşı sana yazılı olarak anlatıyorum. İlk olarak girişin hemen sağındaki **5 aşirlik** yere limon ve yanındaki **9 aşirlik** yere elma ekilecek. Eğer hemen karşıdaki taşlarla çevrili alana ne olacak diye soracak olursan, o halde bil ki şimdilik oraya bir şey yapılmayacak çünkü orada geçen seneden kalan **2 kafizlik** kiraz bulunmaktadır. Bu alanın hemen yanındaki **4 aşirlik** yere ayva onun yanındaki **5 aşirlik** yere ise muz ekilecek yalnız bu alanın içerisinde **1 metrekarelik** ekime uygun olmayan bir alan bulunmakta orası mecburen boş kalacak. Muz ekilecek alanın hemen karşısında **3 aşir**, **3 aşir** olmak üzere eşit şekilde ayrılmış iki ayrı alan bulunmakta, bu alanlara deneme amaçlı bu bölgede az bulunan erik ve kivi ekilecek. Eğer bu iki meyveden istenilen verim alınamazsa birleştirilip bu alana da muz ekilecek. Çeşmenin yanındaki **5 metrekare** ve **6 metrekarelik** küçük alanlar gerekli malzemelerin konulması için depo olarak kullanılacak. Çeşmenin tam karşısında kalan **8 aşirlik** yere ise ayva ekimi yapılacaktır. En uçtaki **4 kafizlik** geniş alana da bana en çok kazandıracak ürün olan hurma ekilecek, bu alanın içerisinde **8 metrekarelik** dinlenmen için bir kulübe de bulunuyor. Çıkış kapısının hemen sağında kalan **1 kafiz** ve **2 kafiz** olarak ayrılmış yerler birleştirilecek ve üzüm ekilecek. Bu alanın tam karşısında yer alan ve toplam **1 aşir** ve **2 metrekare** olan yer ise kardeşimindir oraya dokunulmayacaktır. Tüm tarlanın planını olabildiğince açıklayıcı şekilde yazmaya çalıştım. Senin için tekrar hayırlı olmasını dilerim.

3.2.2.1.2.2. Harflerin Para Birimi ile İlişkilendirilmesi

Açık metindeki harfler dinar miktarı ile temsil edilmiştir. Ebced sistemindeki sayısal değerleri 1-9 arasında olan harfler tam dinar ile, 10-90 arasında olan harfler çeyrek dinar ile, 100-1000 arasında olan harfler ise yarım dinar ile temsil edilmiştir. Aşağıda verilen tabloya göre şifreli metindeki dinar miktarlarının sırası takip edildiği zaman نصر من الله وفتح قريب cümlesini verecektir.

Tablo 25: Arap Harflerinin Dinar Para Birimi ile Temsil Edilmesi

ا	ب	ج	د	هـ
واحد دينار	اثنان دينار	ثلاثة دينار	أربعة دينار	خمسة دينار
1 Dinar	2 Dinar	3 Dinar	4 Dinar	5 Dinar
و	ز	ح	ط	ي
سنة دينار	سبعة دينار	ثمانية دينار	تسعة دينار	واحد ربع دينار
6 Dinar	7 Dinar	8 Dinar	9 Dinar	1 Çeyrek Dinar
ك	ل	م	ن	س
اثنان ربع دينار	ثلاثة ربع دينار	أربعة ربع دينار	خمسة ربع دينار	سنة ربع دينار
2 Çeyrek Dinar	3 Çeyrek Dinar	4 Çeyrek Dinar	5 Çeyrek Dinar	6 Çeyrek Dinar
ع	ف	ص	ق	ر
سبعة ربع دينار	ثمانية ربع دينار	تسعة ربع دينار	واحد نصف دينار	اثنان نصف دينار
7 Çeyrek Dinar	8 Çeyrek Dinar	9 Çeyrek Dinar	1 Yarım Dinar	2 Yarım Dinar
ش	ت	ث	خ	ذ
ثلاثة نصف دينار	أربعة نصف دينار	خمسة نصف دينار	سنة نصف دينار	سبعة نصف دينار
3 Yarım Dinar	4 Yarım Dinar	5 Yarım Dinar	6 Yarım Dinar	7 Yarım Dinar
ض	ظ	غ		
ثمانية نصف دينار	تسعة نصف دينار	ثمان دينار		
8 Yarım Dinar	9 Yarım Dinar	1/8 Dinar		

أخي العزيز

سعدت أنني حصلت على رسالتك وأنت بخير. بارك الله فيك دائماً. سأخبرك في رسالتي بكيفية اعداد عشاء الدعوة الشهير الذي طلبت مني. هذا الطبق ليس طبقاً دائماً يمكن اعداده بسبب وفرة المكونات المستخدمة فيه. لهذا السبب سوف أخبرك بكميات المواد من حيث السعر حتى تعرف المبلغ الذي يجب أن تنفقه حتى تتمكن من معرفة والتحضير وفقاً لذلك .

أولاً اشتر خمسة أرباع دينار من بصل وتسعة أرباع دينار من كراث وقشر القشر الخارجي واغسله وتطبخ في الماء حتى تصبح طرية. اتركه يبرد بعد أن يلين بدرجة كافية واقطع بشكل جيد حتى تصبح صغيراً. الآن، اقطع اثنان نصفي دينار من الجرز الى قطع صغيرة واطبخها في القليل من الماء في نفس الوعاء واضف أربعة أرباع دينار من الجرجير وخمسة أرباع دينار من الثوم بالحجم الصغير. ثم اخلط كل هذه المكونات معاً جيداً واطبخها جانباً. قشر الباذنجان التي سيكلف سعرها ديناراً واحداً في وعاء آخر وقسمها الى أربعة أجزاء واطبخها في الماء المالح وبعد أن تلين بدرجة كافية فاسحقها جيداً. سحق ثلاثة أرباع دينار من قرفة وثلاثة أرباع دينار من كزبرة في الهاون وأضف قليل من الملح واخلطها كلها. الآن قد يكون غالياً قليلاً ما سأقول لكن هذا هو الجزء الذي سيعطي الطعم الحقيقي للطبق فذلك أوصي أن تضع المكونات التي سوف أقول. تليين خمسة دنائير من التين المجفف وستة دنائير من اللوز عن طريق النقع في الماء الساخن. انتبه أن اللوز مقشراً وتقسيمها الى قسمين. ثم أضف ثمانية أرباع دنائير من العناب وأربعة أنصاف دنائير من الزبيب التي يسهل التليين واخلطها مرة أخرى كلها. ثم أخرج كلها من الماء واهرق على الباذنجان الذي هرسته.

ثم خذ ثمانية دنائير من لحم الغنم وقطعه الى قطع متوسطة الحجم وابدأ الطبخ بوضع القليل من الزيت عليه لكن إذا كانت هناك أجزاء ذات رائحة كريهة من اللحم يجب أن تقشطها أولاً. اخلط جيداً واحد نصف دينار من الخل واثنان نصفي دينار من العسل في وعاء منفصل ثم اخلط كلها مرة أخرى برش واحد ربع دينار من الزعتر عليها واهرقها على قطع اللحم المطبوخة. ثم اترك اللحم للنقع لفترة. بعد أن ينقع اللحم بشكل كافٍ، اخلطه مع مزيج البصل الذي ذكرته في الجزء الأول. أخيراً، أهرق الخليط اللحمي على خليط الباذنجان الذي أعدته من قبل فيكون طبقك مجهزاً. إذا أردت يمكنك تقديمها برش دينارين من أوراق الأترج عليها في النهاية. كما ترى يا أخي على الرغم من صعوبة صنع هذا الطبق لذته جيد حتى أولئك الذين يذوقوه مرة واحدة لن ينسوه أبداً. يمكنك تقديمه لضيوفك براحة البال. رحمة الله وبركاته عليك.

Sevgili kardeşim,

Mektubunu aldığıma ve iyi olmana çok sevindim. Allah afiyetini daim eylesin.

Mektubunda benden istediğin meşhur davet yemeğinin yapılışını sana anlatacağım. Bu yemek, içinde kullanılan malzemelerin çokluğundan dolayı her zaman yapılabilecek bir

yemek değildir bu nedenle ne kadar harcaman gerektiğini bilmen için malzemelerin miktarlarını sana fiyat türünden söyleyeceğim ki bilip ona göre hazırlığını yapabilesin.

İlk olarak **5 çeyrek dinarlık** soğanı ve **9 çeyrek dinarlık** pırasayı al, dış kabuklarını soy, yıka ve yumuşayana kadar suda pişir. Yeterince yumuşadıktan sonra soğumaya bırak ve küçük hale getirene kadar güzelce doğra. Şimdi aynı kapta **2 yarım dinarlık** havucu küçük parçalara ayırarak çok az bir su içerisinde haşla ve üzerine **4 çeyrek dinarlık** roka ve **5 çeyrek dinarlık** sarımsakları küçülterek ekle. Daha sonra tüm bu malzemeleri birbiri ile iyice karıştırarak bir kenarda beklet.

Başka bir kapta fiyatı **1 dinar** kadar tutacak patlıcanları soy, dört parçaya ayır ve tuzlu suyun içerisinde pişir, yeterince yumuşadıktan sonra iyice ez. Bir havanda **3 çeyrek dinarlık** tarçın ile **3 çeyrek dinarlık** kişnişi ez ve bir tutam tuz ekleyerek hepsini karıştır. Şimdi söyleyeceklerim biraz pahalı olabilir ama yemeğin asıl tadını verecek olan bu kısımdır bu yüzden şimdi sayacağım malzemeleri koymayı kesinlikle tavsiye ederim. Yaklaşık **5 dinar** kadar kuru incir ve **6 dinar** kadar bademi sıcak suyun içerisinde bekleterek yumuşat. Bademlerin soyulmuş ve ikiye ayrılmış olmasına dikkat et. Sonra içerisine yumuşaması daha kolay olan **8 çeyrek dinar** kadar hünnap ile **4 yarım dinar** kadar kuru üzümü de ekleyerek hepsini tekrar karıştır. Daha sonra hepsini sudan çıkar ve ezmiş olduğun patlıcanların üzerine dök.

Ardından **8 dinar** kadar kuzu etini alarak orta büyüklükte parçalara ayır ve üzerine az bir miktar yağ koyarak pişirmeye başla fakat eğer etin kötü kokulu kısımları var ise onları önceden sıyırmalısın. Ayrı bir kapta **1 yarım dinarlık** sirke ile **2 yarım dinarlık** balı iyice karıştır sonra üzerine **1 çeyrek dinarlık** kekik de serpererek hepsini tekrar karıştır ve pişmiş et parçalarının üzerine dök. Bu haliyle eti bir süre demlemeye bırak. Et yeterince demlendikten sonra üzerine ilk kısımda söylediğim soğanlı karışım ile karıştır. Son olarak bu etli karışımı daha önceden hazırladığın patlıcanlı karışımın üzerine dök böylece yemeğin hazır olacak. Eğer istersen en son üzerine **2 dinar** kadar turunç yaprağı da serpiştirerek servis edebilirsin.

Gördüğün gibi kardeşim bu yemeği yapmak oldukça zahmetli olsa da tadı bir kez tadanların bir daha unutamayacağı kadar güzeldir. Misafirlerine gönül rahatlığı ile ikram edebilirsin. Allah'ın rahmeti ve bereketi üzerine olsun.

3.2.2.1.2.3. Harflerin Haftanın Gün ve Saatleri ile İlişkilendirilmesi

Açık metindeki harfler haftanın gün ve saatleri ile temsil edilmektedir. Tüm harfler 7 gruba ayrılmış ve her grup haftanın bir günü ile ilişkilendirilmiştir. Harfler ise bulunduğu gruptaki sıra numarasına göre mensup olduğu günün saati ile temsil edilmektedir. Aşağıdaki tabloda harflerin gün ve saatleri belirtilmiştir. Metindeki gün ve saatlerin sırası takip edildiği zaman نصر من الله وفتح قريب cümlesini verecektir.

Tablo 26: Arap Harflerinin Haftanın Gün ve Saatleri ile Temsil Edilmesi

Harf	Gün		Saat	
ت	الاثنين	Pazartesi	١٣:٠٠	13:00
ث	الاثنين	Pazartesi	١٤:٠٠	14:00
ذ	الاثنين	Pazartesi	١٥:٠٠	15:00
ق	الاثنين	Pazartesi	١٦:٠٠	16:00
د	الثلاثاء	Salı	١٣:٠٠	13:00
و	الثلاثاء	Salı	١٤:٠٠	14:00
ر	الثلاثاء	Salı	١٥:٠٠	15:00
ج	الأربعاء	Çarşamba	١٣:٠٠	13:00
ح	الأربعاء	Çarşamba	١٤:٠٠	14:00
ظ	الأربعاء	Çarşamba	١٥:٠٠	15:00
هـ	الأربعاء	Çarşamba	١٦:٠٠	16:00
ش	الخميس	Perşembe	١٣:٠٠	13:00
م	الخميس	Perşembe	١٤:٠٠	14:00
س	الخميس	Perşembe	١٥:٠٠	15:00
ط	الجمعة	Cuma	١٣:٠٠	13:00
ا	الجمعة	Cuma	١٤:٠٠	14:00
غ	الجمعة	Cuma	١٥:٠٠	15:00
ي	الجمعة	Cuma	١٦:٠٠	16:00
ك	الجمعة	Cuma	١٧:٠٠	17:00
ن	السبت	Cumartesi	١٣:٠٠	13:00
ص	السبت	Cumartesi	١٤:٠٠	14:00
ف	السبت	Cumartesi	١٥:٠٠	15:00
ض	السبت	Cumartesi	١٦:٠٠	16:00
خ	الأحد	Pazar	١٣:٠٠	13:00
ز	الأحد	Pazar	١٤:٠٠	14:00
ع	الأحد	Pazar	١٥:٠٠	15:00
ب	الأحد	Pazar	١٦:٠٠	16:00
ل	الأحد	Pazar	١٧:٠٠	17:00

خرجت سفري الذي خططت أن أخرجه يوم السبت في الساعة الواحدة يوم السبت في الساعة الثانية متأخرا من أجل الخلط البسيط الذي خرج في اللحظة الأخيرة. استطعت أن أصل في الوقت الذي عاهدت به صديقي يعني يوم الثلاثاء في الساعة الثالثة الى بيته. بعد أن أكلنا طعاما لذيذا معا وقضينا وقتا قليلا خرجنا لنسبح المدينة. كنت أشعر بعجيب لأنه كأنه ما تغير لا شيء منذ مجيئي الأخير على الرغم من مرور وقت طويل وبقي كل شيء كما تركته. قد كان حان وقت الوداع يوم الخميس في الساعة الثانية لبعضنا البعض منذ الان. قلت انه الى اللقاء صديقي العزيز سأشتاقك. يوم السبت في الساعة الواحدة. وبقي أن أصل الى هي المدينة القديمة قليلا. أنا متحمس لأنني ستكون لدي الفرصة لرؤية هذه المدينة التي يقص الزاهيون إليها باعجابها مرة أولى. أنوي السوح مباشرة بعد العثور على مكان آمن للإقامة. سيوجد وقتي هنا يوم الجمعة حتى الساعة الثانية لذلك يجب أن أقيمه بشكل جيد.

كانت هذه المدينة حقاً مثل ما قاله المسافرون. أريد أن أقول ما رأيته لأولئك الذين ليس لديهم الفرصة فأولئك يعلمون أيضاً. حان وقت الوداع من هذه المدينة الان. حان الوقت الآن لنصل إلى الطريق تكرارا.

يوم الأحد والساعة الخامسة. هل هذا القدر من الوقت ذهب حقاً؟ دون أن ألاحظ أصبح يوم الأحد الساعة الخامسة. يبدو لي أنه كان الوقت القليل مضى. أنا في الطرق. هناك الكثير لأقوله منذ الان لكن سأستطيع أن أكتب كله واحدا واحدا. يوم الأربعاء والساعة الرابعة. جئت قرية صغيرة. هذا المكان لم يكن في خطتي في الواقع لكن قررت البقاء هنا قليلا لما شعرت بي جيدا ولأحتاج الى الاستراح.

يوم الثلاثاء والساعة الثانية. أشعر بأحسن الان. لقد كان جو هذه القرية الصغيرة جيداً جداً بالنسبة لي. التقيت بشخص لطيف هنا. قد كان ابن بلد. شكرا له، اعتنى بي وساعدني في قضاء بعض احتياجاتي. قلت إنني أريد التعرف عليه بشكل أفضل وأشكره وقد قبل. اتفقنا على الاجتماع أمام المسجد الذي في المركز يوم السبت في الساعة الثالثة. دعاني إلى منزله لأنني أجنبي هنا وقدم لي شراب العسل. تجاذبنا أطراف الحديث قليلا. سألته ماذا يعمل. قال إنه كان يعمل في التجارة وأنه غالباً ما كان يغادر القرية من أجلها. سألته عن رحلته القادمة. قال إنه على الفور سيخرج هذا يوم الاثنين في الساعة الواحدة. قل، قلت إننا لن نواجه مرة أخرى. وداعا وغادرننا منزله.

يوم الأربعاء والساعة الثانية. سأرتحل عن هذه القرية الجميلة. إذا لم يحدث لي شيء وإذا كان بإمكانني الوصول بالسلامة سأكتب ان شاء الله. يوم الاثنين في الساعة الرابعة وصلت الى مدينة سياحتي الأخيرة بالسلامة. لكن ما وجدت مكان الإقامة حتى الان. لكن قال لي آخر مكان زرتة انني أن أجياً غدا يعني يوم الثلاثاء في الساعة الثالثة. سأرتب شيئاً لنفسي هذه الليلة. الآن سأبلغ في اليوم التالي. كانت الليلة أبرد مما توقعت. أنا شعرت بالبرد قليلاً، لكنني بخير الآن. أتمنى أن أقضي وقتاً ممتعاً في هذه المدينة التي هي محطتي الأخيرة.

عدت من رحلتي التي كنت قد بدأتها يوم الجمعة في الساعة الرابعة إلى منزلي يوم الأحد في الساعة الرابعة بعد لأي. سأكتب بالتفصيل كل ما رأيته وكل ما حدث لي في هذه الرحلة بعد أن أستريح بشكل جيد دون النسي.

Cumartesi günü saat 1’de yola çıkmayı planladığım yolculuğuma son anda çıkan ufak bir aksaklıktan dolayı gecikerek cumartesi günü saat 2’de çıkmış bulundum.

Yine de arkadaşşıma söz vermiş olduğum vakitte yani **salı günü saat 3’te** evlerine varabildim. Birlikte güzel bir yemek yiyip biraz hasret giderdikten sonra şehri dolaşmaya

çıktık. Garip hissediyordum çünkü son gelişimden beri onca zaman geçmesine rağmen sanki hiçbir şey değişmemiş, her şey bıraktığı gibi kalmıştı. **Perşembe günü saat 2**'de artık birbirimize veda vaktimiz gelmişti. Hoşça kal canım dostum seni özleyeceğim dedim. **Cumartesi günü saat 1** ve benim o kadim şehre varmama çok az kaldı. Heyecanlıyım çünkü gidenlerin hayranlıkla anlattığı bu şehri ilk defa görme imkanına sahip olacağım. Kalacak güvenilir bir yer bulduktan hemen sonra gezmeye koyulma niyetindeyim. Burada **cuma günü saat 2**'ye kadar vaktim olacak bu yüzden iyi bir şekilde değerlendirmem gerekiyor. Bu şehir gerçekten gezenlerin anlattıkları kadar varmış, ben de gördüklerimi imkânı olmayanlara anlatmak istiyorum ki onlar da öğrensinler. Artık bu şehirden ayrılma vakti geldi. Şimdi tekrar yola çıkma zamanı. **Pazar günü saat 5**! O kadar vakit geçti mi gerçekten, fark etmeden **pazar günü saat 5** olmuş bile. Bana yola çıkmalı sanki çok az bir zaman geçmiş gibi geliyor. Yollardayım, şimdiden anlatacak çok şey var ancak dönünce hepsini tek tek yazabileceğim. **Çarşamba günü saat 4**, küçük bir kasabaya geldim. Burası aslında planımda yoktu ama kendimi pek iyi hissetmediğim ve dinlenmeye ihtiyacım olduğu için biraz burada kalmaya karar verdim. **Salı günü saat 2**, şimdi daha iyi hissediyorum, bu küçük kasabanın havası bana çok iyi geldi, burada güzel bir insana da rastladım. Kendisi buranın yerlisiymiş, sağ olsun benimle ilgilendi ve bazı ihtiyaçlarımı karşılamam için yardımcı oldu. Onu daha yakından tanımak ve teşekkür etmek istediğimi söyledim kabul etti, **cumartesi günü saat 3**'te merkezdeki caminin önünde buluşmak için sözleştik. Buraların yabancısı olduğum için beni evine davet etti ve bir bal şerbeti ikram etti. Biraz sohbet ettik ona ne iş yaptığını sordum, ticaretle uğraştığını bunun için sık sık kasabadan ayrıldığını söyledi. Ona bir dahaki yolculuğunu sordum, hemen bu **pazartesi günü saat 1** gibi çıkacağını söyledi. Desene bir daha görüşemeyeceğiz dedim, helalleştik ve evinden ayrıldım. **Çarşamba günü saat 2** şimdi bu güzel kasabadan ayrılıyorum, yolda başıma bir şey gelmez ve sağ salim varabilirsem inşallah tekrar yazarım. **Pazartesi günü saat 4**'seyahatimin son şehrine sağ salim ulaştım ama henüz kalacak yer bulamadım ama en son uğradığım yer bana yarın yani **salı günü saat 3**'te gelmemi söyledi. Bu gece artık bir şekilde başımın çaresine bakacağım. Şimdi ertesi günden bildiriyorum gece tahminimden daha serin geçti biraz üşüdüm ama şu an gayet iyiyim. Son durağım olan bu şehirde güzelce vakit geçirmeyi umuyorum. **Cuma günü saat 4**'te çıkmış olduğum yolculuğumdan nihayet **pazar günü saat 4** evime

dönmüş bulunuyorum. Güzelce dinlendikten sonra unutmadan bu seyahatimde tüm gördüklerimi ve başımdan geçen her şeyi ayrıntılı bir şekilde yazacağım.

3.2.2.1.2.4. Harflerin Kitap İsimleri ile İlişkilendirilmesi

Açık metindeki harfler kitap isimleri ile temsil edilmiştir. Her harf bir kitap ismi ile eşleştirilmiş ve kurgulanarak bir metin içerisine yerleştirilmiştir. Metindeki kitap isimlerinin sırası takip edildiği zaman نصر من الله وفتح قريب cümlesini verecektir.

Tablo 27: Arap Harflerinin Kitap İsimleri ile Temsil Edilmesi

Harf	Kitap İsmi		Müellif
ا	حياة الحيوان الكبرى	Hayat'ül Hayvan el-Kübra	Demîrî
ب	الجامع بين العلم والعمل النافع في صناعة الحيل	El Câmi-u'l Beyn'el İlmî ve El-Ameli'en Nâfi fi Sınâ'ati'l Hiyel	Cezerî
ج	كتاب المناظر	Kitâbü'l-Menâzır	İbnü'l-Heysem
د	الهاوي في الطب	El-Hâvî fî't-tıb	Ebû Bekr er-Râzî
هـ	مُرُوجُ الذَّهَبِ وَمَعَادِينُ الْجَوْهَرِ	Mürûcü'z-zeheb ve me'âdinü'l-cevher	Mes'ûdî
و	زيج ايلخانى	Zîc-i İlhanî	Tûsî
ز	كتاب فيما يحتاج إليه الكتاب والعمال من علم الحساب	Kitâb fimâ yahtâcü ileyhi'l-küttâb ve'l-'ummâl min 'ilmi'l-hisâb	Bûzcânî
ح	كتاب المختصر في حساب الجبر والمقابلة	Kitâbü'l-Muhtaşar fî hisâbi'l-cebr ve'l-muqâbele	Hârezmî
ط	كتابه ميزان الحكمة	Kitâbü Mîzânî'l-hikme	el-Hâzinî

ي	رسالة في البراهين على مسائل الجبر والمقابلة	Risâle fî'l-berâhîn 'alâ mesâ'ili'l-cebr ve'l muḳābele.	Ömer hayyâm
ك	كتاب الزيج	Kitâbü'z-Zîc.	Bettânî
ل	الجماهر في معرفة الجواهر	el-Cemâhir fî ma'rifeti'l-cevâhir	Bîrûnî
م	تذكرة الكحالين في العين وأمراضها	Tezkiretü'l-keḥḥâlîn fî'l-'ayn ve emrâziḥâ	Ali bin İsa-el-Kehhar
ن	الموجز في الطب	el-Mûcez fî't-ṭib	İbnü'n-Nefîs
س	الرسالة المسماة جدول الدقائق	Risâle fî cedveli'd-daḳ'a'ik.	İbn Irâk
ع	كتاب صناعة الأسطرلاب	Kitâbü San'ati'l-uṣṭurlâb	Kûhî
ف	أبواب لا يستغنى من يروم عمل الإسطرلاب	Ebvâb lâ yestacnî men yerûmü 'amele'l-uṣṭurlâb	Mecrîṭî
ص	الجامع لمفردات الأدوية والأغذية	el-Câmi' li-müfredâti'l-edviye ve'l-acziye	İbnü'l-Baytâr
ق	الفخري في الجبر والمقابلة	el-Faḥrî fî'l-cebr ve'l-muḳābele.	Kerecî
ر	كتاب التصريف لمن عجز عن التأليف	Kitâbü't-Taṣrîf li-men 'aceze 'ani't-te'lîf	Zehrâvî
ش	مصالح الأبدان والأنفس	Mesâlihu'l-ebdân ve'l-enfûs	Ebû Zeyd el-Belhî
ت	كتاب الهيئة	Kitâbü'l-Hey'e	Bitrûcî
ث	القانون في الطب	el-Kânûn fî't-ṭib	İbn Sînâ
خ	كتاب المسائل العددية	Kitâbü'l-Mesâ'ili'l-'adediyye	Ebû Ca'fer el-Hâzin
ذ	عيون الأنباء في طبقات الأطباء	Uyûnü'l-enbâ' fî ṭabaḳati'l-etıbbâ	İbn Ebu Usaybia
ض	صورة الأرض	Sûretü'l-arz	İbn Havkal
ظ	كتاب الفلاحة	Kitâbü'l-Filâḥa	İbnü'l-Avvâm
غ	عجائب المخلوقات وغرائب الموجودات	Acâ'ibü'l-mahlûkât ve garâ'ibü'l-mevcûdât.	Kazvînî

يا أخي طلبت مني بعض النصائح للعلوم المفيدة. سأشارك بكل سرور ما يتبادر إلى ذهني أولاً. عندما وجدت هذه الكتب اعلم أنك وجدت شيئاً أغلى من الذهب وابتهج وفقاً لذلك لكن لا يكفي أن تبتهج فقط يجب عليك تطبيق ما تفهمه وإنتاج منه ومشاركته. إذا علمت هذه المسؤولية فترى بركاتها.

إذا أردت العمل في مجال الرعاية الصحية ابدأ من كتاب **الموجز في الطب**. في هذا الكتاب، يمكنك العثور على الكثير من المعلومات النظرية والعملية حول علم الطب ويمكنك الحصول على معلومات مفيدة مثل وصفات الأدوية المختلفة والعلاقة بين الأعضاء والأمراض. ثانياً أنصحك بقراءة **الجامع لمفردات الأدوية والأغذية**. في هذا الكتاب يمكنك الحصول على المعلومات حول الأدوية التي يمكن صنعها من النباتات المزروعة في العديد من مناطق البحر الأبيض المتوسط والشرق الأوسط والأناضول ومدى فعالية هذه الأدوية في الوقاية من الأمراض. كما تعلم، الأمراض هي حقيقة من حقائق الحياة وأفضل طريقة للتعامل معها هو استخدام الأدوية التي تؤثر عليها.

إذا كنت لا تزال عازماً على العمل في هذا المجال، فحاول بالتأكيد الحصول على كتاب **التصريف لمن عجز عن التأليف** لأنني لا أستطيع أن أنهى بإخبار المحتويات. انظر بنفسك، سوف تعجب كثيراً. بصرف النظر عن ذلك يحتوي كتاب **تذكرة الكحالين في العين وأمراضها** على معلومات شاملة عن العين والتي تعتبر عضواً مهماً جداً بالإضافة إلى المعلومات الصحية العامة. إذا كانت لديك الفرصة، فإنني أوصي بالتأكيد بمراجعتها. إذا كنت تهتم بموضوع العين يمكنك مراجعة كتاب مؤلف كتاب **الموجز في الطب** الذي يفحص فيه عضو العين بشكل منفصل.

لا أتذكر اسمه الآن. إذا كنت تريد الخروج من الإنسان يمكنك مراجعة كتاب **حياة الحيوان الكبرى** الذي ستستطيع أن تفكر مثل نوع من موسوعة الحيوانات، ينقل المؤلف في هذا الكتاب ملاحظاته على العديد من الحيوانات التي درسها. بغض النظر عن العلم الذي تتعامل معه، يجب أن تحاول الحفاظ على ثقافتك العامة في مستوى جيد ويجب أن تقوم بقراءات مختلفة لهذا الغرض. يمكنك قراءة مواضيع الثقافة العامة مثل الأخلاق والسياسة وعلم النفس والتاريخ من الكتاب المسمى **الجماهر في معرفة الجواهر**. بالطبع كما يمكنك معرفة اسم **الجماهر في معرفة الجواهر**، يحتوي هذا الكتاب أيضاً على معلومات شاملة عن الأحجار الكريمة والمعادن. إذا كنت مهتماً، يمكنك أيضاً قراءة هذه الأجزاء. ومع ذلك، فإن الكتاب المسمى **مروج الذهب ومعادن الجوهر** غني جداً من حيث التاريخ والثقافة والجغرافيا والعديد من الموضوعات. أوصي بقراءته لتوسيع آفاقك. إذا كنت تريد أن توجه إلى مجالات تقنية أكثر يمكنك معرفة الكثير من الأمور المتعلقة بعلم الفلك، مثل معلومات التقويمات، ومواقع الكواكب وإحداثيات المستوطنات، وأوقات الصلاة من الكتاب المسمى **زيج ايلخاني**. ستساعدك هذه المعلومات على فهم الكون الذي تعيش فيه بشكل أفضل وتعيش حياة أكثر تنظيماً. إذا كنت ترغب في التعرف على البنية التقنية لأداة الإسطرلاب المستخدمة في العديد من الأغراض وكيفية استخدامها، يمكنك الحصول على المساعدة من الكتاب المسمى **أبواب لا يستغني من يروم عمل الإسطرلاب**. بعد أن تصل إلى مستوى معين، يمكنك قراءة كتاب **الهيئة** الذي يحتوي على بعض الابتكارات في مجال علم الفلك وسيمنحك وجهات نظر مختلفة.

إذا كنت تريد أن تكون مهتماً بالرياضيات، فإن الكتاب المسمى **كتاب المختصر في حساب الجبر والمقابلة** هو الأفضل في مجاله. سوف يساعدك كثيراً في الحسابات التي ستحتاجها في حياتك اليومية. لإلقاء نظرة على المسائل الجبرية ونظريات التفاضل والتكامل والبراهين والمعادلات يمكنك الحصول على كتاب **الفخري في الجبر والمقابلة**. هذا الكتاب هو كتاب أصلي مثل الكتاب الذي ذكرته سابقاً اسمه **كتاب التصريف لمن عجز عن التأليف**. لتصنيف المعادلات

وطرق الحل أوصي أن تراجع الى الكتاب المسمى رسالة في البراهين على مسائل الجبر والمقابلة. أخيراً، في هذا الكتاب المسمى الجامع بين العلم والعمل النافع في صناعة الحيل يمكنك تعلم المعلومات التقنية حول كيفية صنع العديد من الأدوات المستخدمة لأغراض مختلفة في الحياة اليومية والغرض من استخدام هذه الأدوات. إن سرد هذا الكتاب، الذي يحتوي على معلومات عملية بدلاً من معلومات نظرية، هو أيضاً توضيحي وجميل للغاية. هذه هي كل النصائح التي يمكنني تقديمها الآن. بعد أن تدخل هذا الطريق ستخبر الحداث وتقرر ما ينفعك أكثر. زاد اللع تعالى علمك.

Kardeşim benden faydalı ilim için bazı tavsiyeler istedin. Ben de aklıma öncelikli olarak gelenleri memnuniyetle paylaşacağım. Bu eserleri bulduğun zaman altından daha kıymetli bir şey bulduğunun farkında ol ve ona göre sevin, ama sadece sevinmek yetmez anladıklarını uygulaman, üzerine üretmen ve bunları da paylaşman gerekir. Bu sorumluluğu bilersen bereketini de görürsün.

Eğer sağlık alanında çalışmak istersen *el-Mûcez fi't-tıb* adlı kitaptan başlayabilirsin. Bu kitapta tıp ilmine dair hem teorik hem pratik pek çok bilgi bulabilir, çeşitli ilaç tarifleri ve organlarla hastalıkların ilişkileri gibi faydalı bilgiler edinebilirsin. İkinci olarak *el-Câmi' li-müfredâtı'l-edviye ve'l-acziye* adlı eseri okumanı tavsiye ederim. Bu kitapta Akdeniz, Ortadoğu ve Anadolu'nun birçok bölgesinde yetişen bitkilerden hangi ilaçların yapılabildiğini ve bu ilaçların hastalıkları önlemede ne derece etkili olduklarını hakkında bilgi sahibi olabilirsin. Senin de bildiğin gibi hastalıklar bu hayatın bir gerçeğidir ve onlarla baş edebilmenin en güzel yolu onlara etki eden ilaçları kullanmaktır.

Eğer hala bu alanda çalışmaya kararlı isen *Kitâbü't-Taşrif li-men 'aceze 'ani't-te'lif* kitabını mutlaka temin etmeye çalış, içindekileri ben anlatmakla bitiremem. Sen kendin gör, fazlasıyla şaşıracaksın. Bunun dışında *Tezkiretü'l Kehhalin fi'l Ayn ve Emraziha* adlı eser genel sağlık bilgilerinin yanında çok önemli bir organ olan göze dair kapsamlı bilgiler sunmaktadır. İmkânın olursa mutlaka bakmanı tavsiye ederim. Eğer göz konusu ilgini çekerse en başta söylediğim *el-Mûcez fi't-tıb* isimli eserin yazarının göz organını ayrı olarak incelediği eserine de bakabilirsin. İsmi şu an hatırlayamıyorum. Eğer insanın dışına çıkmak istersen bir tür hayvanlar ansiklopedisi gibi düşünebileceğin *Hayat'ül Hayvan el-Kübra* isimli esere bakabilirsin, bu eserde müellif incelediği birçok hayvana dair gözlemlerini aktarmaktadır.

Hangi tür ilimle uğraşırsan uğraş genel kültürünü iyi bir seviyede tutmaya çalışmalı ve bunun için çeşitli okumalar yapmalısın. *El-Cemâhir fi ma 'rifeti'l-cevâhir* adlı eserden ahlak, siyaset, psikoloji ve tarih gibi genel kültür konularını okuyabilirsin. Tabii isminin

el-Cemâhir fî ma‘rifeti’l-cevâhir olmasından anlayacağın gibi bu kitap aynı zamanda değerli taşlar ve madenlerle ilgili kapsamlı bilgiler de içermektedir, ilgili çekerse bu kısımları da okuyabilirsin. Bununla birlikte *Mürûcû’z-zehab ve me‘âdinü’l-cevher* isimli eser de tarih, kültür, coğrafya ve birçok konu açısından oldukça zengindir, ufkunu genişletmen için okumanı tavsiye ederim. Eğer daha teknik alanlara yönelmek istersen *Zîc-i İlhânî* adlı eserden takvimlerin bilgileri, gezegenlerin yerleri, yerleşim merkezlerinin koordinatları ve namaz vakitleri gibi astronomiye dair birçok meseleyi öğrenebilirsin. Bu bilgiler yaşadığın evreni daha iyi anlamana ve daha düzenli bir hayat sürmene yardımcı olacaktır. Birçok amaçta kullanılan usturlap aletinin teknik yapımı ve nasıl kullanıldığına dair bilgi edinmek istersen de *Ebvâb lâ yestacnî men yerûmü ‘amele’l-usturlâb* isimli eserden yardım alabilirsin. Belirli bir düzeye geldikten sonra ise astronomi alanında bazı yenilikler içeren ve sana farklı bakış açıları kazandıracak olan *Kitâbü’l-Hey’e*’yi okuyabilirsin.

Matematikle ilgilenmek istersen *Kitâbü’l-Muhtaşar fî hisâbi’l-cebr ve’l-muqâbele* adlı eser tam bir baş ucu kitabıdır, günlük hayatta ihtiyaç duyacağın hesaplamalar için sana oldukça yardımcı olacaktır. Cebirsel problemler, hesap teorileri, ispatlar ve denklemlere bakmak için *el-Fahrî fî’l-cebr ve’l-muqâbele* adlı eseri temin edebilirsin. Bu eser de tıpkı daha önceden söylediğim *Kitâbü’t-Taşrîf li-men ‘aceze ‘ani’t-te’lîf* isimli eser gibi oldukça özgün bir eserdir. Denklerin sınıflandırılması ve çözüm yöntemleri için ise *Risâle fî’l-berâhîn ‘alâ mesâ’ili’l-cebr ve’l-muqâbele* isimli esere bakmanı öneririm. Son olarak *El Câmi-u’l Beyn’el İlmî ve El-Amelî’en Nâfi fî Sınâ’ati’l Hiyel* isimli bu kitapta günlük hayatta farklı amaçla kullanılan birçok aletin nasıl yapılacağına dair teknik bilgileri ve bu aletlerin kullanım amaçlarını öğrenebilirsin. Teorik bilgilerden ziyade pratik bilgileri içeren bu eserin anlatımı da gayet açıklayıcı ve güzeldir.

Benim verebileceğim tavsiyeler şimdilik bu kadar, sen bu yola girdikten sonra zamanla yenilerinden haberdar olacak ve neyin senin için daha faydalı olacağına kendin karar vereceksin inşallah. Allah ilmini artırsın.

3.2.2.2. Harflerin Sayısal Değerlerinin Bir Metnin İçerisine Yerleştirilmesi Örneği

“نصر من الله وفتح قريب” cümlesindeki harflerin ebced sistemindeki sayısal değerleri sırasıyla aşağıdaki metin içerisine yerleştirilmiştir.

في دورة واحدة، يدور عطارد حول الشمس ٥٠ مرة، والزهرة يدور حوله ٩٠ مرة، والأرض تدور حوله ٢٠٠ مرة، والمريخ يدور حوله ٤٠ مرة، والمشتري يدور ٥٠ مرة، وزحل يدور ١ مرة. إذا استخدمنا دورة أخرى، فإن عطارد يدور حول الشمس ٣٠ مرة، والزهرة يدور حوله ٣٠ مرة، والأرض تدور حوله ٥ مرة، والمريخ يدور حوله ٦ مرة، والمشتري يدور ٨٠ مرة، وزحل يدور ٤٠٠ مرة. في الدورة الثالثة، يدور عطارد حول الشمس ٨ مرة، والزهرة يدور حوله ١٠٠ مرة، والأرض تدور حوله ٢٠٠ مرة، والمريخ يدور حوله ١٠ مرة، والمشتري يدور ٢ مرة.

Tek bir periyotta, Merkür Güneş'in etrafında 50 kere döner, Venüs 90 kere döner, Dünya 200 kere döner, Mars 40 kere döner, Jüpiter 50 kere döner, Satürn 1 kere döner. Diğer periyotta, Merkür Güneş'in etrafında 30 kere döner, Venüs 30 kere döner, Dünya 5 kere döner, Mars 6 kere döner, Jüpiter 80 kere döner, Satürn 400 kere döner. Üçüncü periyotta, Merkür Güneş'in etrafında 8 kere döner, Venüs 100 kere döner, Dünya 200 kere döner, Mars 10 kere döner, Jüpiter 2 kere döner.

3.2.2.3. Mesajın Başka Bir Bağlam İçerisine Yerleştirilmesi Örnekleri

3.2.2.3.1. İlk Harfler ile

Aşağıdaki metinde her kelimenin ilk harfî sırayla وفتح قريب Aşağıdaki metinde her kelimenin ilk harfî sırayla وفتح قريب harflerle başlamaktadır.

نريد صبرا رضا مغفرة، نحب الله، لذلك لازم أن هلكننا وسائل فتنة. ترك حلم قبيح رافعا يمشي بروح

Sabır, rıza ve mağfîret istiyoruz. Allah Teala'yı seviyoruz. Bu yüzden fitnenin vesilelerini yok etmemiz lazım. Kötü hayali terk etmek bizi yükseltir ve ruh ile yürütür.

3.2.2.3.2. İkinci Harfler ile

Aşağıdaki metinde her kelimenin ikinci harfî sırayla وفتح قريب Aşağıdaki metinde her kelimenin ikinci harfî sırayla وفتح قريب harflerden oluşmaktadır.

من نصر مريم سمع منافعها. كاسب الخير الجميل كاسب أهمية أو مفحارة. اتباع رحمة مقوي ارتفاعها بين عباد

Kim Meryem'e yardım ederse onun faydalarını duyar. Güzel hayrın sahibi, önem ya da iftihar kazanır. Merhamete ittiba etmek, kullar arasında onun artması için güçlendirici kuvvettir.

3.2.2.3.3. Sonuncu Harfler ile

Aşağıdaki metinde her kelimenin son harfı sırayla نصر من الله وفتح قريب cümlesindeki harflerle bitmektedir.

رمضان قص الأزهار. كتم السكين وملاً الرجل الحقل بزهرتنا نفسه. أخو يوسف مات بفتح الخندق. أزهار تيلي وتغوب.

Ramazan çiçekleri kesti. Bıçağı sakladı ve adam kendisinin iki çiçeğini çukura doldurdu. Yusuf'un kardeşi çukurun açılmasıyla öldü. Çiçekler çürümüş ve kaybolmuştu.

3.2.2.3.4. Belirli Harfler ile

Aşağıdaki metinde her üç kelimedede bir, birinci kelimenin birinci harfi, ikinci kelimenin ikinci harfi, üçüncü kelimenin üçüncü harfi نصر من الله وفتح قريب sırayla cümlesindeki harflere denk gelecek şekilde oluşturulmuştur.

ناجي أصبح أسرع من منافسيه، رياضته لعب الكرة، ساهم وزنه بفوزه، ابتهج حاملاً بقلبه أفراحاً يريد أبنياً.

Naci rakiplerinden daha hızlı oldu. Onun sporu top oynamaktır. Az kilolu olması kazandı. Çok sevindi. Kalbinin içinde mutluluklar taşıdı. O mutluluğun ebedi olmasını ister.

3.2.2.3.5. Kelimeleri Ayrılması ile

Aşağıdaki metinde sırayla her cümlenin ilk kelimesi نصر من الله وفتح قريب cümlesini vermektedir.

نصر الله شيء يريد. من جميع الناس. الله تعالى صاحب التوفيق. ويعطي الله تعالى عبده ما يريد من فضله. فتح الشيء يحقق بالدعاء بإذن الله تعالى. قريب الألفة يكون بالدعاء.

Allah'ın yardımını istenilen şeydir. Tüm insanlar tarafından. Allah-u Teâlâ başarının sahibidir. Allah Teâlâ kuluna istediğini fazlından verir. Bir şeyin fethi Allah'ın izni ve dua ile gerçekleşir. Ülfetin yakınlığı dua ile olur.

3.2.2.4. Harflerin Sayısal Değerlerine Denk Yeni Kelimelerin Üretilmesi Örneği

Aşağıdaki şifreli metinde nokta ile ayrılan kelimelerin harflerinin sayısal değerlerinin toplamı açık metindeki her harfin sayısal değerine denk olacak şekilde hazırlanmıştır.

İbn Dureyhim bu yöntem için aşağıdaki örneği vermiştir.⁴²

Tablo 28: "علي" Mesajındaki Harflerin Sayısal Değerlerine Karşılık Kelime Üretme			
Mesaj	Sayısal Değer	Şifre	Sayısal Değer
ع	70	سبح	60+2+8
ل	30	وهاباً جواداً	6+5+1+2+1+3+6+1+4+1
ي	10	هدأ	5+4+1
علي	110	سبح. وهاباً جواداً. هدأ	60+2+8+6+5+1+2+1+3+6+1+4+1+5+4+1

3.3. ARAPÇA ÖRNEKLERİN TÜRKÇEYE UYARLANMASI

Türkçede isimler, önüne Arapçada olduğu gibi belirlilik takısı (ال) gibi bir ek almadığından ve harfler her zaman ayrı olarak yazıldığından dolayı konu ile ilgili şifreleme yöntemlerine örnek verilmemiştir. Bununla birlikte Türkçedeki harflerin

⁴² İbnu'd Dureyhim'in vermiş olduğu bu örnekteki kelimeler bir cümle oluşturmamaktadır. Buna rağmen bu yöntem kullanılarak anlamlı bir cümle oluşturulması mümkün olduğundan "şifrenin gizlenmesine dayalı yöntemler" başlığı altında yer almıştır. Nitekim yöntemin Türkçeye uyarlanması bir cümle olarak hazırlanmıştır.

Arapçada olduğu gibi sayısal karşılıkları da bulunmamaktadır. Bu sebeple örneklerde kullanılmak üzere Türk alfabesindeki harfler için aşağıdaki tabloda belirtilen sayısal değerler farazi olarak eşleştirilmiştir.

Tablo 29: Türk Alfabesindeki Harflere Farazi Olarak Atanan Sayısal Değerler									
F	Ş	M	H	E	P	N	U	B	İ
1	2	3	4	5	6	7	8	9	10
O	I	Y	L	Ü	K	T	A	V	R
20	30	40	50	60	70	80	90	100	200
Ö	Z	S	D	G	C	Ç	Ğ	J	
300	400	500	600	700	800	900	1000	-	

3.3.1. Anlamın Gizlenmesi Dayalı Şifreleme Örnekleri

Anlamın gizlenmesi başlığı altında ele alınan yerine koyma, yer değiştirme, ekleme ve çıkarma, birleştirme ve ayırma alt başlıkları altında verilen örneklerde aşağıdaki metnin şifrelemesi yapılmıştır.

“Bizim yükümlülüğümüz, bilginin en yakınına almak, en meşhur ve yakın olanına erişmek, uzmanlarının bildirdiklerini toplamak, bunlar içinde doğrulayabildiklerimizi doğrulayıp, geri kalanlarını olduğu gibi terk etmek ve bütün bunları Allah’ın iradesi ve yardımıyla doğrunun taliplisi ve bilgelik sevdalıları kimselere faydalı olsun ve onları bize mümkün olmayan başarıya yönlendirsın diye yapmaktır.” (Bîrûnî, Âsârü’l- Bâkiye)

3.3.1.1. Harf ile Yerine Koyma Örnekleri

3.3.1.1.1. Düzenli Kurala Bağlı Olarak

Açık metindeki her harf alfabe dizilişinde kendisinden sonra gelen 7. Harfin yerine geçmiştir. Harflerin yeni değerleri aşağıdaki tabloda gösterilmiştir.

Tablo 30: Düzenli Bir Kurala Bağlı Olarak Türk Alfabesindeki Harflerini Eşleştirme

A	B	C	Ç	D	E	F	G	Ğ	H
G	Ğ	H	I	İ	J	K	L	M	N
I	İ	J	K	L	M	N	O	Ö	P
O	Ö	P	R	S	Ş	T	U	Ü	V
R	S	Ş	T	U	Ü	V	Y	Z	
Y	Z	A	B	C	Ç	D	E	F	

Ğöföş eçrçşşçşçmçşçf göslötöt jt egrototo gşşgr jt şjancy dj egrot usgtotg jyöaşjr
 cfşgtsgyotot gösiöyiorsjyötö buvsgşgr ğctsgy öiötij iumycsgeggösiörsjyöşöfö
 iumycsgeov llyö rgsgtsgyoto usicmc löğö bjyr jbsjr dj ğçbçt ğctsgyo gssgnot öygijzö dj
 egyioşoesg iumyctct bgsövsözö dj gösljsör zjdigsozo röşzjsjy kgeigso uszct dj utsgyo
 ğöfj şçşrçt usşgegt ğgagyoeg eütsjtiöyzöt iöej egvşgrboy.

3.3.1.1.2. Düzenli Bir Kurala Bağlı Olmayarak

Açık metindeki her harf alfabedeki diğer harflerle rastgele eşleştirilmiştir. Harflerin yeni değerleri aşağıdaki tabloda gösterilmiştir.

Tablo 31: Düzenli Bir Kurala Bağlı Olmayarak Türk Alfabesindeki Harflerini Eşleştirme

A	B	C	Ç	D	E	F	G	Ğ	H
N	İ	Z	O	K	B	Ş	J	U	V
I	İ	J	K	L	M	N	O	Ö	P
M	D	C	T	Ö	H	G	Ç	A	Ğ
R	S	Ş	T	U	Ü	V	Y	Z	
L	Ü	P	E	R	Y	I	F	S	

İdsdh fytyhöyöyuyhys idöjdgdg bg fntmgmgm nöht bg hbpvrl ıb fntmg çöngmgn
 bldphbt rshngönlmg idökdldtöbldgd eçğönhnt irgönl dodgkb kçulröfnidökdtdöbldhd
 kçulrönmğ jblt tnöngönlmgm çökrur jdld ebld behbt ıb iyeyg irgönlm nöönmvg dlnkbüd

ıb fnlkmhmfön kçulrgrg eaödğödüd ıb idöjbödt übıknömüı tdhüböblb şnfknöm çöürg ıb
çgönlm idsb hyhtyg çöhnfng inpnlmfn fagöbgkdlüdğ kdfb fnğhnteml.

3.3.1.1.3. Harflerin Denk Oldukları Sayısal Değerlerin Tekrar Harfe Dönüştürülmesi

Açık metindeki her harf sayısal sistemde denk olduğu değer korunacak şekilde başka harflerle temsil edilmiştir. Bu yöntemle hazırlanan harflerin yeni değerleri aşağıdaki tabloda gösterilmiştir. Şifreli metinde bu değerlerin bazıları kullanılmıştır.

Tablo 32: Türk Alfabesindeki Harflerin Sayısal Değerlerinin Tekrar Harflere Dönüştürülmesi

F	Ş	M	H	E	P	N	U	B
1	2	3	4	5	6	7	8	9
f	ff	fş fff	fm ffş şş	fh ffm şm fşş	fe şh fşm mm şşş	fp şe fmm fşh ffe mh	fn şp me hh şşh fmh	fu şn md he şmh ffn
İ	O	I	Y	L	Ü	K	T	A
10	20	30	40	50	60	70	80	90
fb şu mn hp ee fhe fmp	ii fbi şui hdi eei mni şhhi	io iii eeo hdo fbo mni şuo	ii oo eei hpı fbio iio	iy oi eey iui ioo fby hpy	il ooo ii oy ioi iiy fbl	iü ol iui ooi iy iil ioy	ik oü ıl yy iiü oiı ooy	it ok iü iyy ool ııı oiy
V	R	Ö	Z	S	D	G	C	Ç
100	200	300	400	500	600	700	800	900
ia ot ık yü ll	iav otv ıkv yüv llv	vvv vr iar llr otr ıkr yür	vö rr iaö otö ıkö yüö llö	vz vrr rö vvö iaz otz llz	vs rz öö ias ots vrö lls	dv sr ööv öz rrrv llrö dyü	vg rd ös zz rrz röö vvd	vc rg öd vzz rrs vrd ööö
Ğ	J							
1000	-							
vç rc ög zd ss ööz rzz	-							

Fu fb vö şu fş. ii ol iü ooo fş iy ii oi oy vç ioi fş iyy vö. şn mn fby vd hp fp ee fmm. fh fşh. oo it ol hdo şe hp fşh eeo. ok eey fş iü iui. şm şe. fff fmm ff şş fn iav. ia fşş. hpı iyy ill mni ffe. eei ioo ool mh mni şuo fp iui. şm oyv ee ff fff fmm iy. hh rr fş ool ffe iui iıı ıkv iii fmm eeo fşh. md mn hpy vs hp yüv öö ee ooi ioo fh llv fhe mh fmp. iiü hdi mm fby ool

fff ııı iıl. he hh ffe fby iyy iav. ee vzz hp fp ias fşş. vs ii ööz ıkv şşh ioo oıy eei it şmh ee
ioo lls mn ıy fby şm yüv fhe fş fb rr şu. vrö mni rc ıkv şşh hpy iyy iio eeo şşş. vöö şm iav
fmp. ıy it iıı iyy fmm ioo ool yüv eeo ffe mni. şui hpy vrö hh ss hh. rrö mn ffn fhe. ooy
ffm llv iıı. fşş yy fş fh ol. ot şm. şn ooo öü ıı fmm. şmh fmh fmm iy it iav io. ool oı iıı ııı
şş io ffe. fhe iav ok vs şm verr şu. yü fşş. iio it iav rz iıı fff eeo hpı fby ııı. öö şui ög ıkv me
şe hh fşh. ooy ool eey ee şşş iıı fb verr fmp. ll fmm. md mn fby vöö fh hpy hp ıy. verr fşş yü
öö oıy iy eeo llz şuo. iü fhe fff iaz fmm fby şm yüv fmm. f iü oo ots ool oı eeo. şhhi oı vvö
hh fşh. ia şm. eei ffe fby iü ıkv hdo. ffn şu yüö fh. fş oy fff ııı oy şe. hdi ioo fş ok iio oıy
ffe. he iyy ff oıy otv iıı fbio ool. oo llr fmm ioo fh şe vrö ee iav verr fhe ffe. öö ee oo fh.
iio iü mm fff ok ool öü io llv.

3.3.1.1.4. Harflerin Denk Oldukları Sayısal Değerlere Çarpma İşlemi Uygulanıp Tekrar Harfe Dönüştürülmesi

Açık metindeki her harfin yerine, sayısal sistemde denk olduğu değer dört ile çarpılarak elde edilen yeni değerine denk başka harfler konulmuştur. Bu yöntemle hazırlanan harflerin yeni değerleri aşağıdaki tabloda gösterilmiştir. Şifreli metinde bu değerlerin bazıları kullanılmıştır.

Tablo 33: Türk Alfabesindeki Harflerin Sayısal Değerlerinin Değiştirilerek Tekrar Harflere Dönüştürülmesi

F	Ş	M	H	E	P	N	U	B
1	2	3	4	5	6	7	8	9
4	8	12	16	20	24	28	32	36
şş fm	hh şmm şşmf	hhh hhşş iş bm uh pp en	ip bn uu fei nnş	ii eei bbş uuh fbi nnp	oh iih uuu bbu nub bbhş	ou bbi şpi mei fni uuuu	ış ppo şiii şio eno ffi	ıp pio uuo
İ	O	I	Y	L	Ü	K	T	A
10	20	30	40	50	60	70	80	90
40	80	120	160	200	240	280	320	360
y oo iiii ii eeı fbı mnı	t yy iny ooy oü ıl ik	ov ty kl üü yyy aı	tt vü vki vıı ak	r vv vll via aao tty kkü	ry roo ttt vkk aat	rt ryy rüo rki rlı vaa	öo öii rüü rty rkl raı	öü öıı öoy öıl rtt rvü
V	R	Ö	Z	S	D	G	C	Ç
100	200	300	400	500	600	700	800	900
400	800	1200	1600	2000	2400	2800	3200	3600
rr öv öll öai ök öüy	zz ös dr gv zrr öör	ğr vvv çö cz gs dd	ğd cc ğöo ğzr ğsv	j ğğ ğçv ğcr ğgö	jz ccc ggg jöv jrr	jc jzz jgv jdr jsö	jğr jğvv jdd jcz jgs	cccc jğd jğöo jcc
Ğ	J							
1000	-							
4000	-							
jj jğğ jğss jğcr	-							

jjjj y ğd iii hhh. Tt ry rt roo hhşş r roo vv ttt jj vkk iş aat ğd. jjjğğ oo vll jzz ii spi eeı mei. Uuh bbi. Tt öü ryy ov mei kl uuuu üü. Öl tty bm rtt vaa. Fbb fni. Pp nnp hh nnş şiii zz. Öll ii. Vü öoy rki yyy bbi. İk vv rvü ou ov fni öü. İi ös eeı şmm bm uuh rlı. Ffi cc hhşş rtt mei r öl zz ty fni kl uuuu. jjjj iiii kkü ccc oo zrr ğgg mnı rüo vv bbş gv eeı ou fbı. Rty ooy nub aao rtt bm rvü ryy. jjjğçv ppo ou tty öoy dr. Y jcc oo fni jrr eeı. jz t jj öör şiii r öü vü rvü jjjj ii vll jöv fbı rki aao bbş ös oo iş ii ğöö eeı. jz t jğss gv eno tty öl vki yyy uuu. jgy nnp zrr oo. Rlı ön vll öoy mei aao rtt gv üü fni yyy. İk tty jöv ffi jj ppo. jdr ii jjjğğ y. Rkl uuh gv vaa. Eei öii bm eeı vaa. Rr ii. jjjj roo rüü ttt ou. jjjğçv şio ou aao rvü öör kl. Rtt vv vll öoy nnş yyy ou. Oo öör ön ğgg uuh ğcr mnı. Öık bbş. Vü öü zrr jrr kl bm ty vı vll ön. Ccc yy jj zz iş ou ppo şpi. Rkl rtt aao iiii iih via eeı ğğö fbı. Öık fbi. jjjj oo vv jsö ii kkü eeı rki. Ğcr uuh öll jöv rtt vv üü ğğ aı. Ryy oo iş ğğ fbi tty nnp dr ii. Şş öu vu jz öov via ty. Yy aao j eno uuuu. Rr uuh. T ou vv öü ös ov. jjjj iiii ğöö eeı. bm roo uh ryy vkk bbi. Ooy vll pp öoy vü rtt mei. jjjğçv öl hh rvü gv aı ak öü. Tt ğr ou r ii bbi jz y zz j oo şpi. Ccc yy vü uuh. Vki rtt uuu pp öoy rüo rüü üü zrr.

3.3.1.1.5. Harflerin Yerine Okunuşlarının Konulması

Açık metindeki harflerin okunuşları sırayla bir düz ve bir ters olacak şekilde yazılarak şifrelenmiştir. Aşağıdaki tabloda harflerin okunuşlarının düz ve tersten yazılışları verilmiştir.

Tablo 34: Türk Alfabesindeki Harflerin Düz ve Ters Okunuşları

HARFLER	DÜZ HALİ İLE OKUNUŞLARI	TERS HALİ İLE OKUNUŞLARI
a	a	a
b	be	eb
c	ce	ec
ç	çe	eç
d	de	ed
e	e	e
f	fe	ef
g	ge	eg
ğ	Yumuşak ge	egkaşumuy
h	he	eh
ı	ı	ı
i	i	i
j	je	ej
k	ke	ek
l	le	el
m	me	em
n	ne	en
o	o	o
ö	ö	ö
p	pe	ep
r	re	er
s	se	es
ş	şe	eş
t	te	et
u	u	u
ü	ü	ü
v	ve	ev
y	ye	ey
z	ze	ez

Beizeime eyüeküemleüleügeümeüze ebielgeineine ene eyaekienienı aleemaek een meeşeehuer vee yeakeme oleanemea eeriesmeeke uzeemaenleareıneine ebieldeireedikleereinei teopeelaemaek beuneelaer ieçiendee deogeeruelaeyabieldeikeeleeriemiezi edoegreuleayeıpe egeeri ekaelaenlaaerıneı oeldeugeu geıbei teereek eetmeeke eve ebüetüen beuneelaerı aleelaehıen ieraedeesi eve eyaerdeımeıyeela edoegreuneune etaeliepleisei vee beileegeelik seeveedaehıesı ekiemseeleeree feayeedaalı oleesuen vee oenleareı beızee meümeeküen oelmeayeane ebaeşarıeya eyöenleeneedierseine edıeye eyaepmeakeetier.⁴³

3.3.1.1.6. Kelime Aralarına Bir Çeşit Harf Konulması

Açık metinde kelime aralarındaki boşluklara m harfi konulmuştur.

Bizimmyükümlülüğümüzmbilgininmenmyakınınmalmakmenmmeşhurmveyakınmola nınamerişmekmuzmanlarınınmbildirdiklerinimtoplamakmbunlarmiçindemdoğrulayabil diklerimizimdoğrulayıpmgerimkalanlarınınımolduğumgibimterkmetmekmvembütünmbun larımAllahınmiradesimvemyardımyılamdoğrununmtalıplisimvembilgelikmsevdalısimki mseleremfaydalımsunmvemonlarımbizemmümkünmolmayanmbaşarıyamyönlendirsın mdiyemyapmaktır.

3.3.1.1.7. Kelime Aralarına Çeşitli Harflerin Konulması

Açık metinde kelime aralarındaki boşluklara h, m ve y harfleri konulmuştur.

Bizimhyükümlülüğümüzmbilgininyenhyakınınmalmaknyenhmeşhurmveyyakınholanına merişmekyuzmanlarınınhbildirdiklerinimtoplamakybunlarhiçindemdoğrulayabildikleri miziyoğrulayıphgerimkalanlarınııyolduğuhgibimterkyetmekhvembütünybunlarıhAllahı nmiradesiyvehardımyılamdoğrununytalıplisihvembilgelikmsevdalısyıkimselerehfaydal ımsunıyvehonlarımbizeymümkünholmayanmbaşarıyayyönlendirsinhdiyemyapmaktır.

3.3.1.2. Sembol ile Yerine Koyma Örnekleri

⁴³ “ğ” harfini “yumuşak ge” olarak yazmak bu şifreleme yöntemini ele vereceği için “g” harfi olarak yazılmıştır.

3.3.1.2.1. Her Harf Yerine Bir Sembol Konulması

Açık metindeki harflerin yerine aşağıdaki tabloda kendileriyle eşleştirilen semboller konulmuştur.

Tablo 35: Türk Alfabesindeki Harflerin Semboller ile Temsil Edilmesi									
A	B	C	Ç	D	E	F	G	Ğ	H
⊞	χ	Φ	θ	Δ	Π	μ	υ	ℵ	η
I	İ	J	K	L	M	N	O	Ö	P
δ	ψ	ξ	β	ε	X	ω	Ξ	∪	∇
R	S	Ş	T	U	Ü	V	Y	Z	
⊗	Γ	τ	φ	ə	κ	&	α	◇	

χψϕψX ακβκXεκεκΝκXκ◇ χψευψωψω Πω ατβδωδωδ τεXτβ Πω XΠτηə⊗ &Π ατβδω Ξετωδωτ Π⊗ψτXΠβ ə◇Xτωετ⊗δωδω χψεΔψ⊗ΔψβεΠ⊗ψωψ φΞVετXτβ χəεετ⊗ ψθψωΔΠ ΔΞΝ⊗əετατχψεΔψβεΠ⊗ψXψϕψ ΔΞΝ⊗əεταδ∇ υΠ⊗ψ βτετωετ⊗δωδ ΞεΔəΝə υψχψ φΠ⊗β ΠφXΠβ &Π χκφκω χəεετ⊗δ τεεετηδω ψ⊗τΔΠΓψ &Π ατ⊗ΔδXδαετ ΔΞΝ⊗əωəω φτεψ∇εψΓψ &Π χψευΠεψβ ΓΠ&ΔτεδΓδ βψXΓΠεΠ⊗Π μταΔτεδ ΞεΓəω &Π Ξωετ⊗δ χψϕΠ XκXβκω ΞεXτατω χτττ⊗δατ α∪ωεΠωΔψ⊗Γψω ΔψαΠ ατ∇Xτβφδ⊗.

3.3.1.2.2. Sıklıkla Beraber Kullanılan Harflere Ortak Bir Sembol Konulması

Türkçede sıklıkla beraber kullanılan ve metinde geçen bu harflerin yerine aşağıdaki tabloda gösterilen semboller konulmuştur.⁴⁴

⁴⁴ 2.1'deki şifreleme baz alınarak oluşturulmuştur. Farkı genellikle beraber kullanılan harfler için de ayrıca sembollerin konulmasıdır.

En	Ve
Σ	Θ

$\chi\psi\phi\psi X$ $\alpha\kappa\beta\kappa X\epsilon\kappa\epsilon\kappa\aleph\kappa X\kappa\phi$ $\chi\psi\epsilon\upsilon\psi\omega\psi\omega$ Σ $\alpha\tau\beta\delta\omega\delta\omega\delta$ $\tau\epsilon X\tau\beta$ Σ $X\Pi\tau\eta\epsilon\Theta$ Θ $\alpha\tau\beta\delta\omega$
 $\Xi\epsilon\tau\omega\delta\omega\tau$ $\Pi\Theta\psi\tau X\Pi\beta$ $\epsilon\phi X\tau\omega\epsilon\tau\Theta\delta\omega\delta\omega$ $\chi\psi\epsilon\Delta\psi\Theta\Delta\psi\beta\epsilon\Pi\Theta\psi\omega\psi$ $\phi\Xi\nabla\epsilon\tau X\tau\beta$
 $\chi\omega\epsilon\tau\Theta$ $\psi\theta\psi\omega\Delta\Pi$ $\Delta\Xi\aleph\Theta\epsilon\tau\alpha\tau\chi\psi\epsilon\Delta\psi\beta\epsilon\Pi\Theta\psi X\psi\phi\psi$ $\Delta\Xi\aleph\Theta\epsilon\tau\alpha\delta\nabla$ $\upsilon\Pi\Theta\psi$
 $\beta\tau\epsilon\tau\omega\epsilon\tau\Theta\delta\omega\delta$ $\Xi\epsilon\Delta\epsilon\aleph\epsilon$ $\upsilon\psi\chi\psi$ $\phi\Pi\Theta\beta$ $\Pi\phi X\Pi\beta$ Θ $\chi\kappa\phi\kappa\omega$ $\chi\omega\epsilon\tau\Theta\delta$ $\tau\epsilon\epsilon\tau\eta\delta\omega$
 $\psi\Theta\tau\Delta\Pi\Gamma\psi$ Θ $\alpha\tau\Theta\Delta\delta X\delta\alpha\epsilon\tau$ $\Delta\Xi\aleph\Theta\epsilon\tau\omega\epsilon\omega$ $\phi\tau\epsilon\psi\nabla\epsilon\psi\Gamma\psi$ Θ $\chi\psi\epsilon\upsilon\Pi\epsilon\psi\beta$ $\Gamma\Pi\&\Delta\tau\epsilon\delta\Gamma\delta$
 $\beta\psi X\Gamma\Pi\epsilon\Pi\Theta\Pi$ $\mu\tau\alpha\Delta\tau\epsilon\delta$ $\Xi\epsilon\Gamma\epsilon\omega$ Θ $\Xi\omega\epsilon\tau\Theta\delta$ $\chi\psi\phi\Pi$ $X\kappa X\beta\kappa\omega$ $\Xi\epsilon X\tau\alpha\tau\omega$ $\chi\tau\tau\tau\Theta\delta\alpha\tau$
 $\alpha\cup\omega\epsilon\Pi\omega\Delta\psi\Theta\Gamma\psi\omega$ $\Delta\psi\alpha\Pi$ $\alpha\tau\nabla X\tau\beta\phi\delta\Theta$.

3.3.1.2.3. Kelime Aralarına Bir Çeşit Sembol Konulması

Açık metinde kelime aralarındaki boşluklara ϕ sembolü konulmuştur.

$\chi\psi\phi\psi X\phi\alpha\kappa\beta\kappa X\epsilon\kappa\epsilon\kappa\aleph\kappa X\kappa\phi$ $\chi\psi\epsilon\upsilon\psi\omega\psi\omega\phi$ $\Pi\omega\phi\alpha\tau\beta\delta\omega\delta\omega\delta\phi\tau\epsilon X\tau\beta\phi$ $\Pi\omega\phi X\Pi\tau\eta\epsilon\Theta$
 $\phi\&\Pi\phi\alpha\tau\beta\delta\omega\phi\Xi\epsilon\tau\omega\delta\omega\tau\phi\Pi\Theta\psi\tau X\Pi\beta\phi\epsilon\phi X\tau\omega\epsilon\tau\Theta\delta\omega\delta\omega\phi\chi\psi\epsilon\Delta\psi\Theta\Delta\psi\beta\epsilon\Pi\Theta\psi\omega\psi\phi$
 $\Xi\nabla\epsilon\tau X\tau\beta\phi\chi\omega\epsilon\tau\Theta\phi\psi\theta\psi\omega\Delta\Pi\phi\Delta\Xi\aleph\Theta\epsilon\tau\alpha\tau\chi\psi\epsilon\Delta\psi\beta\epsilon\Pi\Theta\psi X\psi\phi\psi\phi\Delta\Xi\aleph\Theta\epsilon\tau\alpha\delta\nabla$
 $\phi\upsilon\Pi\Theta\psi\phi\beta\tau\epsilon\tau\omega\epsilon\tau\Theta\delta\omega\delta\phi\Xi\epsilon\Delta\epsilon\aleph\epsilon\phi\upsilon\psi\chi\psi\phi\phi\Pi\Theta\beta\phi\Pi\phi X\Pi\beta\phi\&\Pi\phi\chi\kappa\phi\kappa\omega\phi\chi\omega\epsilon\tau\Theta\delta$
 $\phi\tau\epsilon\epsilon\tau\eta\delta\omega\phi\psi\Theta\tau\Delta\Pi\Gamma\psi\phi\&\Pi\phi\alpha\tau\Theta\Delta\delta X\delta\alpha\epsilon\tau\phi\Delta\Xi\aleph\Theta\epsilon\tau\omega\epsilon\omega\phi\tau\epsilon\psi\nabla\epsilon\psi\Gamma\psi\phi\&\Pi\phi\chi\psi\epsilon$
 $\upsilon\Pi\epsilon\psi\beta\phi\Gamma\Pi\&\Delta\tau\epsilon\delta\Gamma\delta\phi\beta\psi X\Gamma\Pi\epsilon\Pi\Theta\Pi\mu\tau\alpha\Delta\tau\epsilon\delta\phi\Xi\epsilon\Gamma\epsilon\omega\phi\&\Pi\phi\Xi\omega\epsilon\tau\Theta\delta\phi\chi\psi\phi\Pi\phi X$
 $\kappa X\beta\kappa\omega\phi\Xi\epsilon X\tau\alpha\tau\omega\phi\chi\tau\tau\tau\Theta\delta\alpha\tau\phi\alpha\cup\omega\epsilon\Pi\omega\Delta\psi\Theta\Gamma\psi\omega\phi\Delta\psi\alpha\Pi\phi\alpha\tau\nabla X\tau\beta\phi\delta\Theta$.

3.3.1.2.4. Kelime Aralarına Çeşitli Sembollerin Kullanılması

Açık metinde kelime aralarındaki boşluklara ϕ , $\angle$, ∞ ve ζ sembolleri konulmuştur.

$\chi\psi\phi\psi X\phi\alpha\kappa\beta\kappa X\epsilon\kappa\epsilon\kappa\aleph\kappa X\kappa\phi$ $\angle\chi\psi\epsilon\upsilon\psi\omega\psi\omega\in\Pi\omega\zeta\alpha\tau\beta\delta\omega\delta\omega\delta\phi\tau\epsilon X\tau\beta\angle\Pi\omega\in X\Pi\tau\eta\epsilon$
 $\Theta\zeta\&\Pi\phi\alpha\tau\beta\delta\omega\angle\Xi\epsilon\tau\omega\delta\omega\tau\in\Pi\Theta\psi\tau X\Pi\beta\zeta\epsilon\phi X\tau\omega\epsilon\tau\Theta\delta\omega\delta\omega\phi\chi\psi\epsilon\Delta\psi\Theta\Delta\psi\beta\epsilon\Pi\Theta\psi\omega\psi$
 $\angle\phi\Xi\nabla\epsilon\tau X\tau\beta\in\chi\omega\epsilon\tau\Theta\zeta\psi\theta\psi\omega\Delta\Pi\phi\Delta\Xi\aleph\Theta\epsilon\tau\alpha\tau\chi\psi\epsilon\Delta\psi\beta\epsilon\Pi\Theta\psi X\psi\phi\psi\angle\Delta\Xi\aleph\Theta\epsilon\tau$

αδ∇αυΠ⊗ψζβτετετε⊗δωδρΞεΔεΝε∠υψχψαφΠ⊗βζΠφΧΠβφ&Π∠χκφκωαχεω
ετ⊗δζτεετηδωρψ⊗τΔΠΓψ∠&Παατ⊗ΔδΧδαετζΔΞΝ⊗εωεω∠φτεψ∇εψΓψα&
ΠζχψευΠεψβφΓΠ&ΔτεδΓδ∠βψΧΓΠεΠ⊗ΠαμταΔτεδζΞεΓεωφ&Π∠Ξεετ⊗δαχ
ψ∠ΠζΧκΧβκω∠ΞεΧταατωαχττ⊗δατζα∪εΠωΔψ⊗ΓψωφΔψαΠ∠ατ∇Χτβφδ
⊗.

3.3.1.3. Sayı ile Yerine Koyma Örnekleri

3.3.1.3.1. Harflerin Yerine Sayı Karşılıklarının Konulması

Açık metindeki harflerin yerine sayısal sistemde denk oldukları sayı değerleri konulmuştur. Şifre, tablo 27’de verilen değerler kullanılarak hazırlanmıştır.

910400103 40607060350605060100060360400 91050700107101 57 40907030730730
905039070 57 35248200 1005 409070307 205090730790, 52001023570
840039075090200307307 9105060010200600107050520010710, 80206509039070
9875090200 109001076005
6002010002008509040909105060020705052001031040010
6002010002008509040306 700520010 709050907509020030730 2050600810008
70010910 80520070 5803570 1005 96080607 987509020030 905050904307
1020090600550010 1005 409020060030330405090 6002010002008787
809050106501050010 105 910507005501070 500510060090503050030
7010350055052005 19040600905030 205050087 1005 2075009020030 9104005
360370607 205039040907 990290200304090 403007505760010200500107 60010405
40906390708030200.

3.3.1.3.2. Harflerin Yerine Yeni Belirlenen Sayısal Değerlerin Konulması

Açık metindeki harflerin yerine yeni belirlenen sayı değerleri konulmuştur. Bu değerler aşağıdaki tabloda gösterilmiştir.

Tablo 36: Türk Alfabesindeki Harflerin Rastgele Sayısal Değerler ile Temsil Edilmesi

F	Ş	M	H	E	P	N	U	B	İ
60	4	700	200	900	80	1000	8	40	50
O	I	Y	L	Ü	K	T	A	V	R
400	7	100	9	20	70	90	30	300	5
Ö	Z	S	D	G	C	Ç	Ğ	J	
2	3	10	500	800	1	600	6	-	

4050350700 100207020700920920620700203 40509800501000501000 9001000
100307071000710007 3097003070 9001000 700900420085 300900 100307071000
40093010007100030 900550470090070 8370030100093057100071000
4050950050550050709900550100050 90400809307003070 40810009305
50600501000500900 50040065893010030405095005070990055070050350
500400658930100780 800900550 703093010009305710007 4009500868 800504050
90900570 9009070090070 300900 402090201000 408100093057 30993020071000
505305009001050 300900 10030550077007100930 500400658100081000
9030950809501050 300900 4050980090095070 109003005003097107
70507001090099005900 60301005003097 40091081000 300900 400100093057
40503900 7002070070201000 400970030100301000 40304305710030
100210009900100050050510501000 50050100900 100308070030709075.

3.3.1.4. Kelime ile Yerine Koyma Örnekleri

3.3.1.4.1. Harflerin Yerine Sayısal Değerlerinin Okunuşlarının Konulması

Açık metindeki harflerin yerine denk oldukları sayısal değerlerin okunuşları konulmuştur. Her harf virgül ile birbirinden ayrılmıştır.

Tablo 37: Türk Alfabesindeki Harflere Atanan Sayısal Değerlerin Okunuşları

F	Ş	M	H	E	P	N
Bir	İki	Üç	Dört	Beş	Altı	Yedi
U	B	İ	O	I	Y	L
Sekiz	Dokuz	On	Yirmi	Otuz	Kırk	Elli
Ü	K	T	A	V	R	Ö
Altmış	Yetmiş	Seksen	Doksan	Yüz	İki yüz	Üç yüz
Z	S	D	G	C	Ç	Ğ
Dört yüz	Beş yüz	Altı yüz	Yedi yüz	Sekiz yüz	Dokuz yüz	Bin
J						
-						

Dokuz, on, dört yüz, on, üç, kırk, altmış, yetmiş, altmış, üç, elli, altmış, elli, altmış, bin, altmış, üç, altmış, dört yüz, dokuz, on, elli, yedi yüz, on, yedi, on, yedi, beş, yedi, kırk, doksan, yetmiş, otuz, yedi, otuz, doksan, elli, üç, doksan, yetmiş, beş, yedi, üç, beş, iki, dört, sekiz, iki yüz, yüz, beş, kırk, doksan, yetmiş, otuz, yedi, yirmi, elli, doksan, yedi, otuz, yedi, doksan, beş, iki yüz, on, iki, üç, beş, yetmiş, sekiz, dört yüz, üç, doksan, yedi, elli, doksan, iki yüz, otuz, yedi, otuz, yedi, dokuz, on, elli, altı yüz, on, iki yüz, altı yüz, on, yetmiş, elli, beş, iki yüz, on, yedi, on, seksen, yirmi, altı, elli, doksan, üç, doksan, yetmiş, dokuz, sekiz, yedi, elli, doksan, iki yüz, on, dokuz yüz, on, yedi, altı yüz, beş, altı yüz, yirmi, bin, iki yüz, sekiz, elli, doksan, kırk, otuz, altı, yedi yüz, beş, iki yüz, on, yetmiş, doksan, elli, doksan, yedi, elli, doksan, iki yüz, otuz, yedi, otuz, yirmi, elli, altı yüz, sekiz, bin, sekiz, yedi yüz, on, dokuz, on, seksen, beş, iki yüz, yetmiş, beş, seksen, üç, beş, yetmiş, yüz, beş, dokuz, altmış, seksen, altmış, yedi, dokuz, sekiz, yedi, elli, doksan, iki yüz, otuz, doksan, elli, elli, doksan, dört, otuz, yedi, on, iki yüz, doksan, altı yüz, beş, beş yüz, on, yüz, beş, kırk, doksan, iki yüz, altı yüz, otuz, üç, otuz, kırk, elli, doksan, altı yüz, yirmi, bin, iki yüz,

sekiz, yedi, sekiz, yedi, seksen, doksan, elli, on, altı, elli, on, beş yüz, on, yüz, beş, dokuz, on, elli, yedi yüz, beş, elli, on, yetmiş, beş yüz, beş, yüz, altı yüz, doksan, elli, otuz, beş yüz, otuz, yetmiş, on, üç, beş yüz, beş, elli, beş, iki yüz, beş, bir, doksan, kırk, altı yüz, doksan, elli, otuz, Yirmi, elli, beş yüz, sekiz, yedi, yüz, beş, yirmi, yedi, elli, doksan, iki yüz, otuz, dokuz, on, dört yüz, beş, üç, altmış, üç, yetmiş, altmış, yedi, yirmi, elli, üç, doksan, kırk, doksan, yedi, dokuz, doksan, iki, doksan, iki yüz, otuz, kırk, doksan, kırk, üç yüz, yedi, elli, beş, yedi, altı yüz, on, iki yüz, beş yüz, on, yedi, altı yüz, on, kırk, beş, kırk, doksan, altı, üç, doksan, yetmiş, seksen, otuz, iki yüz.

3.3.1.4.2. Harflerin Yerine Bir Kategoriye Ait İsimlerin Konulması

Açık metindeki her harfin yerine ilişkilendirilmiş oldukları kuş isimleri konulmuştur. Bu isimler aşağıdaki tabloda gösterilmiştir. Kelimeler arasındaki boşluklar ise “guguk” ismi ile temsil edilmiştir.

Tablo 38: Türk Alfabesindeki Harflerin Kuş İsimleri ile Temsil Edilmesi

F	Ş	M	H	E
Serçe	Saka kuşu	Bülbül	Çayır kuşu	Ebabil
P	N	U	B	İ
Martı	Karatavuk	Ağaçkakan	Kumru	Doğan
O	I	Y	L	Ü
Telli turna	Karga	İbibik	Gökkuzgun	Yeşilbaş
K	T	A	V	R
Tahtalı	Kanarya	Güvercin	Ulu doğan	Muhabbet Kuşu
Ö	Z	S	D	G
Baykuş	Turdus	Kızılgerdan	Şahin	Sığırcık
C	Ç	Ğ	J	Boşluk
Saksağan	Kırlangıç	Kartal	-	Guguk

Kumru doğan turdus doğan bülbül guguk ibibik yeşilbaş tahtalı yeşilbaş bülbül gökkuzgun yeşilbaş gökkuzgun yeşilbaş gökkuzgun yeşilbaş bülbül yeşilbaş turdus guguk kumru doğan gökkuzgun sığırcık doğan karatavuk doğan karatavuk guguk ebabil karatavuk guguk ibibik güvercin tahtalı karga karatavuk karga karatavuk karga guguk güvercin gökkuzgun bülbül güvercin tahtalı guguk ebabil karatavuk guguk bülbül ebabil saka kuşu çayır kuşu ağaçkakan muhabbet kuşu guguk ulu doğan ebabil guguk ibibik güvercin tahtalı karga karatavuk guguk telli turna gökkuzgun güvercin karatavuk karga karatavuk güvercin guguk ebabil muhabbet kuşu doğan saka kuşu bülbül ebabil tahtalı guguk ağaçkakan turdus bülbül güvercin karatavuk gökkuzgun güvercin muhabbet kuşu karga karatavuk karga karatavuk guguk kumru doğan gökkuzgun şahin doğan muhabbet kuşu şahin doğan tahtalı gökkuzgun ebabil muhabbet kuşu doğan karatavuk doğan guguk kanarya telli turna martı gökkuzgun güvercin bülbül güvercin tahtalı guguk kumru ağaçkakan karatavuk gökkuzgun güvercin muhabbet kuşu guguk doğan kırlangıç doğan

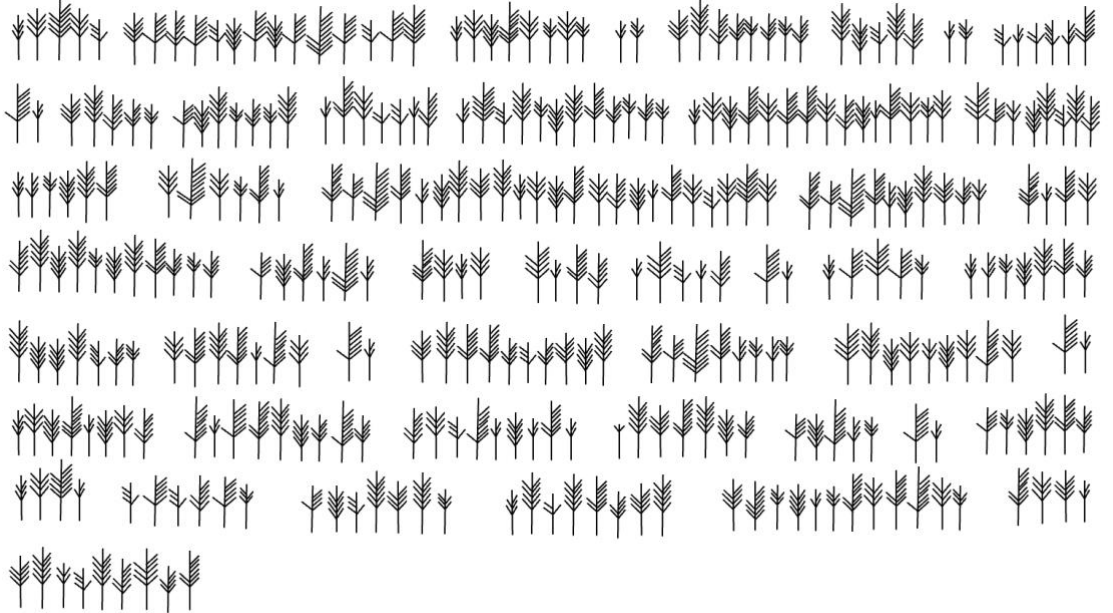
karataavuk şahin ebabil guguk şahin telli turna kartal muhabbet kuşu ağaçkakan gökkuzgun güvercin ibibik güvercin kumru doğan gökkuzgun şahin doğan tahtalı gökkuzgun ebabil muhabbet kuşu doğan bülbül doğan turdus doğan guguk şahin telli turna kartal muhabbet kuşu ağaçkakan gökkuzgun güvercin ibibik karga martı guguk sığırcık ebabil muhabbet kuşu doğan guguk tahtalı güvercin gökkuzgun güvercin karataavuk gökkuzgun güvercin muhabbet kuşu karga karataavuk karga guguk telli turna gökkuzgun şahin ağaçkakan kartal ağaçkakan guguk sığırcık doğan kumru doğan guguk kanarya ebabil muhabbet kuşu tahtalı guguk ebabil kanarya bülbül ebabil tahtalı guguk ulu doğan ebabil guguk kumru yeşilbaş kanarya yeşilbaş karataavuk guguk kumru ağaçkakan karataavuk gökkuzgun güvercin muhabbet kuşu karga guguk güvercin gökkuzgun gökkuzgun güvercin çayır kuşu karga karataavuk guguk doğan muhabbet kuşu güvercin şahin ebabil kızılgerdan doğan guguk ulu doğan ebabil guguk ibibik güvercin muhabbet kuşu şahin karga bülbül karga ibibik gökkuzgun güvercin guguk şahin telli turna kartal muhabbet kuşu ağaçkakan karataavuk ağaçkakan karataavuk guguk kanarya güvercin gökkuzgun doğan martı gökkuzgun doğan kızılgerdan doğan guguk ulu doğan ebabil guguk kumru doğan gökkuzgun sığırcık ebabil gökkuzgun doğan tahtalı guguk saka kuşu ebabil ulu doğan şahin güvercin gökkuzgun karga kızılgerdan karga guguk tahtalı doğan bülbül kızılgerdan ebabil gökkuzgun ebabil muhabbet kuşu ebabil guguk serçe güvercin ibibik şahin güvercin gökkuzgun karga guguk telli turna gökkuzgun kızılgerdan ağaçkakan Karataavuk guguk ulu doğan ebabil guguk telli turna karataavuk gökkuzgun güvercin muhabbet kuşu karga guguk kumru doğan turdus ebabil guguk bülbül yeşilbaş bülbül tahtalı yeşilbaş karataavuk guguk telli turna gökkuzgun bülbül güvercin ibibik güvercin karataavuk guguk kumru güvercin saka kuşu güvercin muhabbet kuşu karga ibibik güvercin guguk ibibik baykuş karataavuk gökkuzgun ebabil karataavuk şahin doğan muhabbet kuşu kızılgerdan doğan karataavuk guguk şahin doğan ibibik ebabil guguk ibibik güvercin martı bülbül güvercin tahtalı kanarya karga muhabbet kuşu.

3.3.1.5. Dalı Alfabe ile Yerine Koyma Örneği

Açık metindeki her harfin yerine dalı alfabenin harfleri konulmuştur. Aşağıdaki tabloda Türk alfabesindeki harflere karşılık gelen dalı harfler gösterilmiştir.

Tablo 39: Türk Alfabesindeki Harflerin Dallı Alfabe ile Temsil Edilmesi

F	Ş	M	H	E	P
					
N	U	B	İ	O	I
					
Y	L	Ü	K	T	A
					
V	R	Ö	Z	S	D
					
G	C	Ç	Ğ	J	
				-	

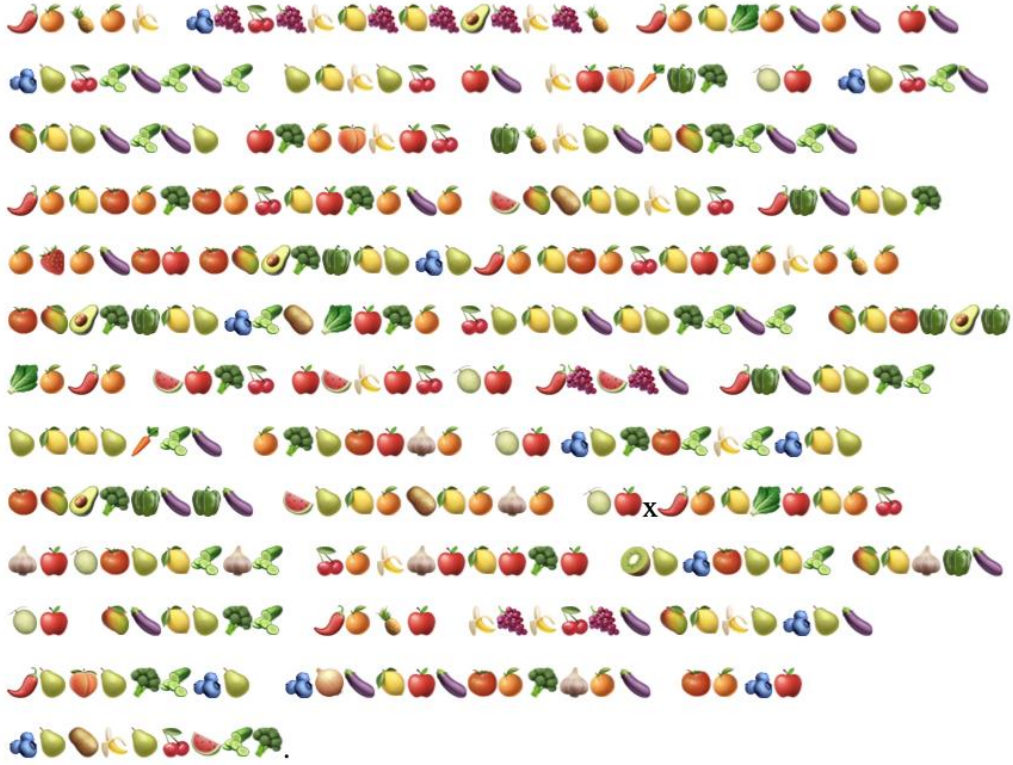


3.3.1.6. Sembolik Resimler ile Yerine Koyma Örneği

Açık metindeki her harf bir meyve veya sebze ismi ile eşleştirilmiştir. Her harfin yerine aşağıdaki tabloda gösterildiği şekilde kendisi ile eşleştirilen meyve veya sebze emoji konulmuştur.

Tablo 40: Türk Alfabesindeki Harflerin Meyve ve Sebze Emojileri ile Temsil Edilmesi

Harf	Şekil	Türkçe
F		Kivi
Ş		Şeftali
M		Muz
H		Havuç
E		Elma
P		Patates
N		Patlıcan
U		Dolmalık Biber
B		Kırmızı Biber
İ		Mandalina
O		Mango
I		Salatalık
Y		Yaban mersini
L		Limon
Ü		Üzüm
K		Kiraz
T		Karpuz
A		Armut
V		Kavun
R		Brokoli
Ö		Soğan
Z		Ananas
S		Sarımsak
D		Domates
G		Marul
C		Hindistan Cevizi
Ç		Çilek
Ğ		Avokado
J	-	-



3.3.1.7. Harflerin Çevresindeki Harflere Göre Yer Değiştirme Örnekleri

Açık metindeki kelimeler tekli, ikili ve yedili olacak şekilde ayrılarak aşağıdaki şekilde şifrelenmiştir.

3.3.1.7.1. Tek Kelime İçerisinde

- Kelimenin baştaki harflerinin sırayla kendilerine karşılık gelen sondaki harfleriyle değiştirilmesi:

Mizib zümüğölülmüküy niniglib ne mınıkay kamla ne ruhşem ev nıkay anınalo kemşire nınıralnamzu inirelkidridlib kamalpot ralnub edniçi izimirelkidlibayalurğod pıyalurğod ireg ınıralnalak uğudlo ibig kret kemte ev nütüb ıralnub ınhalla isedari ev alyımıdray nunurğod isilpilat ev kileglib ısıladves erelesmik ıladıyaf nuslo ev ıralno ezib nükmüm nayamlo ayıraşab nisridnelnöy eyid rıtıkampay.

- Kelimenin son harfinin en başa yazılması:

Mbizi zyükümlülüğümü nbgini ne ıyakının kalma ne rmeşhu ev nyakı aolanın kerişme nuzmanlarını ibildirdiklerin ktoplama rbunla eçind idoğrulayabildiklerimiz pdoğrulayı iger ıalanların uolduğ igib kter ketme ev nbütü ıbunlar nallahı iirades ev ayardımyıl ndoğrunu italiplis ev kbgeli ısevdalıs ekimseler ıfaydal nolsu ev ıonlar ebiz nmümkü nolmaya abaşarıy nyönlendirsı ediy ryapmaktı.

c. Kelimenin ilk harfi ile son harfinin yerlerinin değiştirilmesi:

Mizib zükümlülüğümüy nilginib ne ıakınıy klmaa ne reşhum ev nakıy alanına krişmee nzmanlarınıu iildirdiklerinb koplamat runlab eçindi ioğrulayabildiklerimizd poğrulayıd ierg ıalanlarınk ulduğ iibg kert ktmee ev nütüb ıunlarb nllahıa iradesi ev aardımıyly noğrunud ialiplist ev kilgelib ıevdalıss eimselerk ıaydalf nlsuo ev ınlaro eizb nümüküm nlmayao aaşarıyb nönlendirsıy eıyd rapmaktıy.

d. Kelimenin ilk harfi ile üçüncü harfinin yer değiştirilmesi:

Zibim küyümlülüğümüz libginin en kayınıny mlaak en şemhur ve kayın alonına ireşmek mzuanlarının libdirdiklerini potlamak nublar içinde ğodrulayabildiklerimizi ğodrulayıp regi lakanlarını dlouğu bigi retk mteek ve túbün nubları llaahın aridesi ve raydımyıla ğodrunun latiplisi ve libgelik vesdalısı mikselere yafdalı sloun ve lnoarı zibe mümkün mlouyan şabarıya nöylendirsın yide paymaktır.

e. Kelimedeki harflerin ikişerli olarak ayrılması ve her ikili harfin bir önceki iki harfin önüne getirilmesi:

Zibim küyüümlümüğüz lgbiiinin en kıyanını maalk en şhmeur ve kıyan anolına işermek mauzarnlının ldbidiirerklini pltoakam nlbuar iniçde ğrdoayulilabkldiimerizi ğrdoayulıp rige lakaarnlını duolğu bigi rkte meetk ve túbün nlbuarı laalhın adiresi ve rdyayımla ğrdounun litaispli ve lgbiiikel vdseısalı mskierele ydfaalı suoln ve laonrı zebi mkmüün maolyan şabayarı nlyödieninrs yedi pmyatıakr.

f. Kelimedeki çift sıradaki harflerle tek sıradaki harflerin yerlerinin değiştirilmesi:

İbizm üyüklmlüğümüüz ibglkini ne ayıkının laamk ne emhşru ev ayıkn lonanıa reşiemk zuamlıranını ibdlriidlkreini otıpmaka ublnra çinied odrğluyabaliidlkremizii odrğluyapı egir akallıranıı louduğ igib etkr teemk ev übütn ublnraı laalıhn ridasei ev aydrımıyıal odrğnunu atillpsii ev ibglleki esdvlasıı iksmleree afdylaı lousn ev noalıı ibez ümkmnü loamayn abaşıray öylneidsrni idey aympkayıtr.

g. Kelimenin baştaki harflerinden sonra sırayla sondaki harflerinin getirilmesi:

Bmiiz yzüükmüümğlüül bniilngi en yıankıın aklam en mreuşh ve ynaık oalnın ekreimş unzımnarınlı biinlidrierldki tkoapmla bruanı ieçdin diozğirmuilraeylakbiidl dpoiğyraul gier kıanlıarnal oulğdu giib tker ektem ve bnüüt biurnal anlılha iirsaed ve yaalrydım dnouğnrı tiasliilp ve bkiillge sıesvıdla keirmesle fıalyad onlus ve onrla beiz mnüümk onlamya baayşıar ynöinsleind deiy yıatpkmka.

h. Kelimenin sonundaki harflerin sırayla baştaki harflerinin önüne getirilmesi:

Mbiiz zyüümküügmüllü nbiinlig ne ıynaıkını kaalm ne rmuehş ev nyıak aonlıan keermiş nuıznmıarnal ibniilrdeilrkdi ktaompal rbauln eidçni idzoıgmriurlealykaibdil pdıoyğarlu igre ıknaılraanl uoğlud igbi ktre keetm ev nbüüt ibruanl nıılhlı iisread ev aylayrıdmı nduonğur itsaillip ev kbiilleg ısseıvılda ekriemlse ıflaayd noulı ev ıornal ebzi nmüümk noalyma abyasıra nyiösnrliedn edyi yıatpkmka.

3.3.1.7.2. İki Kelime Arasında

a. Birinci kelimenin ilk harfi ile ikinci kelimenin ilk harfinin değiştirilmesi:

Yizim bükümlülüğümüüz eilginin bn aakınıını ylmak mn eeşhur ye vakın elanına orişmek bzmanlarının uildirdiklerini boplamak tunlar dçinde ioğrulayabildiklerimizi goğrulayıp deri oalanlarını klduğu tibi gerk vtmekek ee bütün bunları illahın aradesi ye vardımıyla toğrunun dalıplisi be vilgelik kevdalıısı simselere oaydalı flsun oe vnları mize bümkün blmayan oaşıarıya dönlendirsın yiye yapmaktır

b. Birinci kelimenin son harfi ile ikinci kelimenin son harfinin deęiřtirilmesi:

Biziz ykmllęmm bilginin en yaknnk almaı er meřhun v yake olannk eriřmea uzmanlarınıı bildirdiklerinn toplamar bunlak iindi doęrulayabildiklerimize doęrulayı gerp kalanlarını olduęı gibk teri etmee v btı bunlarn Allahıı iradesn va yardımıyla doęrunui taliplisn v bilgelie sevdalıse kimseleri faydaln olsun vı onlare bizn mmke olmayaa bařarıyn ynlendirsie diyn yapmaktır.

c. Birinci kelimenin ilk harfi ile ikinci kelimenin son harfinin deęiřtirilmesi:

zizim ykmllęmb, nilginin eb kaknnı almay, rn meřhue ne yakv klanına eriřmeo izmanlarının bildirdiklerini roplamak bunlat iinde doęrulayabildiklerimizi ioęrulayp gerd ualanlarını olduęk gibi terg etmek ve tn bunlarb illahın iradesa ae yardımıylv ioęrunun taliplisd ke bilgeliv eevdalısı kimselers naydalı olsuf ıe onlarv nize mmkb almayan bařarıyo enlendirsın diyy yapmaktır.

d. Birinci kelimenin son harfi ile ikinci kelimenin ilk harfinin deęiřtirilmesi:

Biziy mkmllęmz bilginie nn yaknna ılmak em neřhur vy eakn olanıne ariřmek uzmanlarınb nildirdiklerini toplamab kunlar iindd eoęrulayabildiklerimizi doęrulayg peri kalanlarıno ıldıęu gıbt ierk etmev te btb nunları Allahıı nradesi vy eardımıyla doęrunut naliplisi vb eilgelik sevdalısk iimselere faydalo ılsun vo enları bizm emkn olmayab nařarıya ynlendirsid niye yapmaktır.

e. Birinci kelimenin ilk harfi ile ikinci kelimenin ilk harfi, birinci kelimenin son harfi ile de ikinci kelimenin son harfinin deęiřtirilmesi:

yiziz bkmllęmm eilginin bn aaknnk ylmaı mr eeřhun yn vake elannk oriřmea bzmanlarınıı uildirdiklerinn boplamar tunlak dindi ioęrulayabildiklerimize goęrulayı derp oalanlarını klduęı tibk geri vtmeek btı bunlarn illahıı aradesn ya vardımıyla

toğrunui daliplisn bk vilgelie kevdalıse simseları oaydaln flsui oı vnlare mizn bümüküe blmayaa oaşarıyn dönleldirsie yiyn yapmaktır.

- f. Birinci kelimenin ilk harfi ile ikinci kelimenin son harfi, birinci kelimenin son harfi ile de ikinci kelimenin ilk harfinin değiştirilmesi:

ziziy mükümlülüğümüb nilginie nb kakınına ılmay rm neşhue ny eakıv klanıne arişmeo izmanlarını b nildirdiklerini roplamab kunlat içindd eoğrulayabildiklerimizi ioğrulayıg perd ualanlarıno ılduğk kibt ierg etmev te iütüb nunlarb illahıı nradesa ay eardımıylyv ioğrunut naliplisd kb eilgeliv eevdalısk iimselers naydalo ılsuf io enlarv nizm eümüküb almayab naşarıyo eönlendirsid niyy yapmaktır.

3.3.1.7.3. Bir Kelime Grubu İçerisinde

Açık metindeki kelimeler öncelikle yedili kelime gruplarına ayrılmıştır. Her grubun ilk harfi yazıldıktan sonra üç harf atlanarak sıradaki harf yazılmıştır. Gruptaki tüm harfler bitene kadar bu işlem tekrar başa dönerek devam ettirilmiştir.

Bmülmınnııaiüüüügenlnkğlynemznaiüaküküyilmızbi
Muynnemzlnrlnhalaealıivorurdeşinbrenadrşnekimkiıkaı
Tabaiduadeiolpiaroalnğyiıdaelındllmrgnuebruknrrlylkaiaikrçgmıozap
oğbrmeüıuttbbrgkvudeüaitukılınlee
Ahrsylğulieidemdniiaeranllıusidtlaaarvvpnyo
Besaisryıuorgeimeasniksldnaileolvellivdlkıelfa
bmümnaalinemıenyşyniykzobydiaüarıaianymrdkersalöpt

3.3.1.8. Harflerin Kendi Pozisyonuna Göre Yer Değiştirmesi Örneği

Açık metindeki her harf açılarını değiştirilerek tekrar yazılmıştır.

Bizim yüümlülüğümüz bilgii e yaııı alma e meşhu ve yaı olaıa eışme uzmaları biliilerii toplama bula içie oğulayabilileimizi oğulayıp gei alalarını oluğu gibi te etme ve bütü bulai Allahı iaesi ve yaımıyla oğuu taliplisi ve bilgeli sevalısı imselee fayalı olsu ve olaı bize mümkün olmaya başayıya yöleisi iye yapmatı.

3.3.1.11.2. Yazılışları Benzer Olan Harflerin Tek Bir Harf Üzerinden Temsil Edilmesi ile

Açık metinde noktasız halde yazılışları aynı olan harfler, belirlenen ortak bir harf tarafından temsil edilmiştir. Aşağıdaki tabloda gösterildiği üzere bu şifrede “Ç”, “Ğ”, “İ”, “Ö”, “Ş” ve “Ü” harfleri kullanılmamıştır.

Tablo 41: Yazılışları Benzer Olan Türk Alfabesindeki Harflerin Ortak Bir Harf ile Temsil Edilmesi

A	B	C	Ç	D	E	F	G	Ğ	H
O	P	Z	Z	I	U	B	T	T	Y
I	İ	J	K	L	M	N	O	Ö	P
M	M	E	G	V	A	C	H	H	N
R	S	Ş	T	U	Ü	V	Y	Z	
D	K	K	J	F	F	R	S	L	

Pmlma sfgfavfvtfafll pmvtmcmc uc sogmcmcm ovaog uc aukyfd ru sogmc hvocmco
udmkaug flaocvodmcmc pmvınnımgvudmcm jhnvoaog pfcevod mzmciu
ihtdfvosopmvımgvudmamlm ihtdfvosmn tudm govocvodmcm hvıftf tmpm judg ujaug ru
pfjfc pfevonm ovvoymc mdoiukm ru sodımamsvo ihtdfcfc jovmnvmkm ru pmvtuvmg
kurıovmkm gmakuvudu bosıovm hvkfc ru hevodm pmlu afagfc hvaosoc pokodmso
shcvucımdkmc ımsu sonaogjmd.

3.3.1.11.3. Yazılışları Benzer Olmayan Harflerin Tek Bir Harf Üzerinden Temsil Edilmesi ile

Açık metinde yazılışları benzer olmayan bazı harfler belirlenen ortak bir harf tarafından temsil edilmiştir. Aşağıdaki tabloda gösterildiği üzere bu şifrede “C” ve “N” harfleri “O” harfi ile, “E” ve “K” harfleri “A” harfi ile, “M” ve “U” harfleri “L” harfi ile, “R” ve “Z” harfleri ise “I” harfi ile temsil edilmiştir. Dolayısıyla şifreli metinde “C”, “K”, “M” ve “R” harfleri kullanılmamıştır.

Tablo 42: Türk Alfabesindeki Bazı Harflerin Ortak Bir Harf Tarafından Temsil Edilmesi

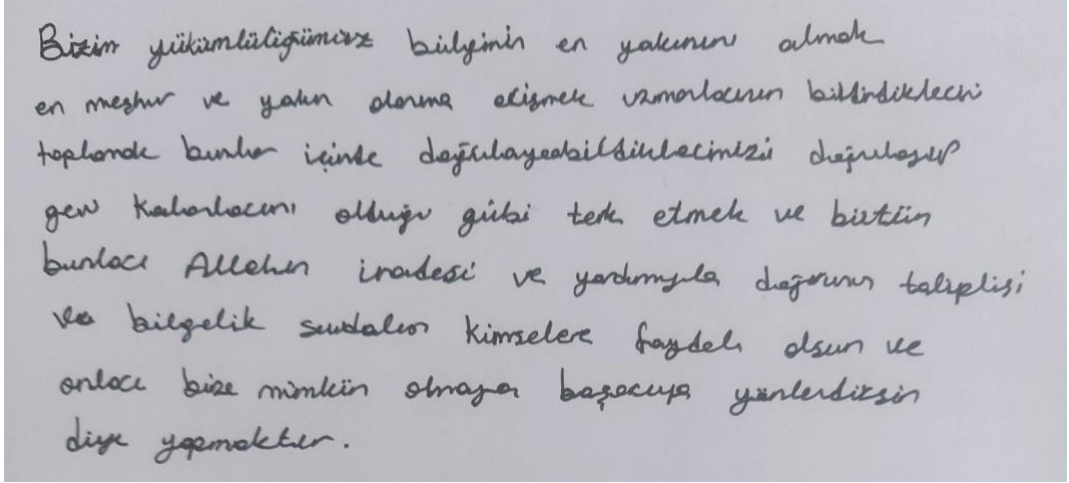
A	B	C	Ç	D	E	F	G	Ğ	H
Z	D	O	S	B	A	H	P	Ş	Y
I	İ	J	K	L	M	N	O	Ö	P
T	Ö	U	A	G	L	O	Ü	J	V
R	S	Ş	T	U	Ü	V	Y	Z	
I	İ	E	F	L	Ğ	N	Ç	I	

Döiöl çğağlgggğşğlğ dögpöoöo ao çzatotot zglza ao laeylı na çzato ügzotoz aıöelaa lızogzıtoto dögböiböagaiöoö füvgzlza dlogzı ösöoba büşılgzçzdögböagaiölöiö büşılgzçtv paiö azgzogzıtöt ügblşl pödö faia aflaa na dğfğö dlogzıt zggzyto öızbaiö na çzvbtlçgz büşılolo fzgövgöiö na dögpagöa ianbzgtit aöliagaıa hzçbzgt ügilo na üogzıt böia lğlağö üglzçzo bzezıtçz çjogaoböiioö böça çzvlzaftı.

3.3.1.12. Ayrı Yazılan Harfleri Birleştirme Örneği

Şifre, Türk alfabesindeki harflerin kendisinden sonra gelen harflerle birleştirilerek yazılması ile oluşturulmuştur.

Resim 5: Ayrı Yazılan Harflerin Birleştirilmesi



3.3.2. Şifrenin Gizlenmesine Dayalı Şifreleme Örnekleri

Kurgulayarak yapılan şifreleme başlığı altında ele alınan yöntemlerde harflerin sayısal değerinden kelime üretme yöntemi dışındaki tüm yöntemlerin örneklendirilmesinde “Bir işaret bekliyorum” cümlesinin şifrelemesi yapılmıştır.

3.3.2.1. Bir Kategori ile İlişkilendirme Örnekleri

3.3.2.1.1. Harflerin Farklı Kategoriye Ait İsimlerle İlişkilendirilmesi

Aşağıdaki tabloda Türk alfabesindeki harflerin eşleştirildikleri kategori isimleri verilmiştir. Her kategori ismi eşleştirilmiş olduğu harf ile başlamaktadır. Bu yöntem ile oluşturulan şifreli metinlerde, harfler eşleştirilmiş oldukları kategorilere ait bir isim ile temsil edilmekte ve sadece mesajın harfleri kadar isim bulunmaktadır.

Tablo 43: Türk Alfabesinin Harflerine Karşılık Gelen Kategori İsimleri

Harf	Kategorisi
A	Aksesuar/ Akraba/ Araba/ Ağaç isimleri
B	Bitki/ Baharat/ Böcek isimleri
C	Cami/ Coğrafi bölge isimleri
Ç	Çalgı aleti/ Çiçek isimleri
D	Dil/ Din isimleri
E	Eşya isimleri
F	Fobi çeşitleri/ Futbol takımları/ Film isimleri
G	Gün isimler, Gök cisimleri
Ğ	-
H	Hayvan/ Hobi/ Hastalık isimleri
I	Irk isimleri
İ	İçecek/ İlaç isimleri
J	-
K	Kıyafet/ Kitap/ Kişi isimleri
L	Lehçe isimleri
M	Maden/ Meslek/ Meyve isimleri
N	Nehir isimleri
O	Organ/ Ozan isimleri
Ö	Ölçü birimleri
P	Para birimleri
R	Renk isimleri
S	Spor, Sebze
Ş	Şarküteri ürünleri/ Şehir isimleri
T	Taşıt isimleri
U	Unvan isimleri
Ü	Ülke isimleri
V	Vitamin isimleri
Y	Yemek isimleri
Z	Zaman ifadeleri

3.3.2.1.1.1. Bir Kısıtlamaya Bağlı Kalmadan Yapılan Şifreleme

Şifre, sırasıyla “Bir işaret bekliyorum” cümlesindeki 19 harfin mensup olduğu kategoriye ait isimlerle kurgulanan bir metinden oluşmaktadır. Yöntem herhangi bir kısıtlamaya bağlı kalmadan oluşturulduğu için 19 harfin her biri kendi kategorisinde herhangi bir harf ile başlayan bir isim ile temsil edilmiştir. Bu 19 harf için kullanılan isimler aşağıdaki tabloda gösterilmiş ve şifreli metinde kalın olarak yazılmıştır.

Tablo 44: Bir Kısıtlamaya Bağlı Kalmadan Yapılan Şifrelemede Kullanılan Kelimeler

Harf	Kategori	Kullanılan Kelime
B	Bir baharat ismi	Tarçın
İ	Bir içecek ismi	Çay
R	Bir renk ismi	Kırmızı
İ	Bir içecek ismi	Şerbet
Ş	Bir şehir ismi	Bursa
A	Bir akraba ismi	Hala
R	Bir renk ismi	Beyaz
E	Bir eşya ismi	Bardak
T	Bir taşıt ismi	Araba
B	Bir bitki ismi	Kuşburnu
E	Bir eşya ismi	Kitap
K	Bir kıyafet ismi	Hırka
L	Bir lehçe ismi	Mısır Arapçası
İ	Bir içecek ismi	Çay
Y	Bir yemek ismi	Çorba
O	Bir organ ismi	Karaciğer
R	Bir renk ismi	Siyah
U	Bir unvan ismi	Doktor
M	Bir meyve ismi	Üzüm

Tarçınları **çayına** koyarken biraz ileride duran **kırmızı** bir **şerbet** dikkatini çekti. **Bursa**'daki **halası** getirmiş olmalıydı. Hemen **beyaz** bir **bardağa** döküp tadına baktı ama beğenmedi. Tadının değişmesi için **Arabada** duran **kuşburnunu** getirip içerisine koydu ve önündeki **kitabı** okumaya devam etti. Üşümek için **hırkasını** giymeye gittiğinde içindekilerin **Mısır Arapçasıyla** yazılmış olabileceğini düşündü. Geri döndüğünde artık **çayı** soğumuştur sıcak bir **çorbanın** kendisine daha iyi geleceğini düşündü. İçtikten sonra **karaciğerine** faydası olduğunu bildiği **siyah** ve aynı zamanda **doktorunun** da tavsiyesi olan **üzümlerden** biraz yedi.

3.3.2.1.1.2. Alfabenin Bir Harfine Bağlı Kalarak Yapılan Şifreleme

Şifre, sırasıyla “Bir işaret bekliyorum” cümlesindeki 19 harfin mensup olduğu kategoriye ait isimlerle kurgulanan bir metinden oluşmaktadır. Kısıtlama için alfabedeki “K” harfi seçilmiştir. Dolayısıyla 19 harfi temsil eden tüm isimler kendi kategorisine ait olmak üzere “K” harfi ile başlamıştır. Bu harfler için kullanılan isimler aşağıdaki tabloda gösterilmiş ve şifreli metinde kalın olarak yazılmıştır.

Tablo 45: Bir Kısıtlamaya Bağlı Kalarak Yapılan Şifrelemede Kullanılan Kelimeler

Harf	Kategori	Kullanılan Kelime
B	Bir böcek ismi	Kelebek
İ	Bir içecek ismi	Kahve
R	Bir renk ismi	Kahverengi
İ	Bir içecek ismi	Kahve
Ş	Bir şehir ismi	Kütahya
A	Bir akraba ismi	Kardeş
R	Bir renk ismi	Kahverengi
E	Bir eşya ismi	Kapı
T	Bir taşıt ismi	Kayık
B	Bir bitki ismi	Kaktüs
E	Bir eşya ismi	Kâğıt
K	Bir kıyafet ismi	Kazak
L	Bir lehçe ismi	Kuzey Afrika Arapçası
İ	Bir içecek ismi	Kefir
Y	Bir yemek ismi	Karnıyarık
O	Bir organ ismi	Kalp
R	Bir renk ismi	Kırmızı
U	Bir unvan ismi	Kral
M	Bir meyve ismi	Kiraz

Uçan **kelebekleri** seyrederken **kahvesinden** bir yudum alarak **kahverenginin** adını **kahveden** aldığı ne kadar da manidar diye söylendi. **Kütahya**’dan gelen **kardeşi** de çok seviyordu **kahverengi**yi. Kalktı, **kapıya** doğru yönelerek **kayığ**ına gitmek istediğini söyledi. Tam çıkarken **kaktüsün** yanında duran **kâğıdı** gizlice alarak **kazağının** içerisine yerleştirdi ve yola koyuldu. Ulaştığında oldukça yorgun görünüyordu. Zor anlaşılan **Kuzey Afrika Arapçası** ile **kefir** içmek ve **karnıyarık** yemek istediğini söyledi. **Kalbi** keyifle yemesine pek müsaade etmese de **kırmızı** ve sanki bir **kral** için özel olarak hazırlanmış gibi görünen **kirazların** servis edildiğini görünce keyfi yerine geldi.

3.3.2.1.1.3. Normal Alfabe Dizilişine Bağlı Kalarak Yapılan Şifreleme

Şifre, sırasıyla “Bir işaret bekliyorum” cümlesindeki 19 harfin mensup olduğu kategoriye ait isimlerle kurgulanan bir metinden oluşmaktadır. 19 harf kendi kategorisine ait olmak şartıyla Türk alfabesinin diziliş sırasıyla başlamıştır. Bu harfler için kullanılan isimler aşağıdaki tabloda gösterilmiş ve şifreli metinde kalın olarak yazılmıştır.

Tablo 46: Normal Alfabe Dizilişine Göre Kullanılan Kelimeler

Harf	Kategori	Kullanılan Kelime
B	Bir bitki ismi	Adaçayı
İ	Bir içecek ismi	Boza
R	Bir renk ismi	Cam göbeği
İ	Bir içecek ismi	Çay
Ş	Bir şehir ismi	Denizli
A	Bir akraba ismi	Enişte
R	Bir renk ismi	Fil dişi rengi
E	Bir eşya ismi	Gözlük
T	Bir taşıt ismi	Helikopter
B	Bir bitki ismi	Isırgan
E	Bir eşya ismi	İbrik
K	Bir kıyafet ismi	Jile
L	Bir lehçe ismi	Kazak Türkçesi
İ	Bir içecek ismi	Limonata
Y	Bir yemek ismi	Mantı
O	Bir ozan ismi	Neşet Ertaş
R	Bir renk ismi	Orman yeşili
U	Bir unvan ismi	Öğretmen
M	Bir meyve ismi	Portakal

Her tarafı saran **adaçayı** kokusu içtiğim **bozanın** tadını da değiştirmişti. Arkamı döndüğümde ne olduğunu bilmediğim **cam göbeği** rengindeki bir **çay**, **Denizli**'den gelen **eniştemin**, **fil dişi** rengindeki **gözlüğünün** üzerine döküldü. O sırada **helikopter** sesini andıran bir ses duydum, ne olduğunu anlamak için dışarı baktığımda yerdeki **ısırganların** kurduğunu gördüm. Sulamak için **ibriği** aldım ve **jilemi** giydim. Yan taraftan **Kazak Türkçesine** benzer konuşmalar duyuluyordu, ancak fazlasıyla unuttuğumu ve pek bir şey anlamadığımı fark ettim. **Limonata** ve **mantı** ikram etme niyetiyle **Neşet Ertaş**'ı ve **orman yeşili** rengini çok seven **öğretmenimi** yemeğe davet etmiştim. Topladığı **portakalları** getirerek davetime icabet etmesi beni fazlasıyla memnun etti.

3.3.2.1.1.4. Sayısal Alfabe Dizilişine Bağlı Kalarak Yapılan Şifreleme

Şifre, sırasıyla “Bir işaret bekliyorum” cümlesindeki 19 harfin mensup olduğu kategoriye ait isimlerle kurgulanan bir metinden oluşmaktadır. 19 harf kendi kategorisine ait olmak şartıyla sayısal alfabesinin diziliş sırasıyla başlamıştır. Bu harfler için kullanılan isimler aşağıdaki tabloda gösterilmiş ve şifreli metinde kalın olarak yazılmıştır.

Tablo 47: Sayısal Alfabe Dizilişine Göre Kullanılan Kelimeler

Harf	Kategori	Kullanılan Kelime
B	Bir bitki ismi	Fesleğen
İ	Bir içecek ismi	Şalgam
R	Bir renk ismi	Mor
İ	Bir içecek ismi	Hibiskus çayı
Ş	Bir şehir ismi	Edirne
A	Bir ağaç ismi	Pelit Ağacı
R	Bir renk ismi	Nar kırmızısı
E	Bir eşya ismi	Urgan
T	Bir taşıt ismi	Bisiklet
B	Bir bitki ismi	İğde
E	Bir eşya ismi	Olta
K	Bir kişi ismi	İlgın
L	Bir lehçe ismi	Yakut Türkçesi
İ	Bir içecek ismi	Limonata
Y	Bir yemek ismi	Üzümlü Pilav
O	Bir organ ismi	Karaciğer
R	Bir renk ismi	Turuncu
U	Bir unvan ismi	Animatör
M	Bir meyve	Vişne

Bir süredir içindeki **fesleğenlerin** demlenmesini beklediği **şalgam suyuna** baktı ve renginin hafif **mora** çalmaya başladığını fark etti. Tadına baktı, tam istediği gibi **hibiskus çayının** tadına benzemeye başlamış, istediği kıvama gelmişti. Teslim etmek için **pelit ağaçlarının** arasından geçerek **Edirne'ye** doğru yola çıktı. Yorulduğu zaman **nar kırmızısına** boyadığı bir **urganla** sardığı **bisikletini iğdelerin** arasında bırakarak mola verdi. Uzaktan **oltasını** garip bir şekilde tutarak kendisine doğru gelen **İlgın'ı** gördü. **Yakut Türkçesi** ile bir şeyler mırıldanıyor, ne dediği anlaşılmıyordu. Pek umursamadı çünkü her zaman olduğu gibi kendi kendine konuşarak önünden geçip gidecekti. Yanında **limonata** ve **üzümlü pilav** getirmişti, **karaciğerine** zarar verdiğini bile bile hızlı bir şekilde yemeğe başladı. Birden **turunculara** bürünen bir **animatörün**, **vişnelerle** yaptığı gösteri aklına geldi. Ne kadar da yetenekliydi.

3.3.2.1.2. Harflerin Aynı Kategoriye Ait İsimlerle İlişkilendirilmesi

3.3.2.1.2.1. Harflerin Arazi ve Ölçü Birimleri ile İlişkilendirilmesi

Açık metindeki harfler arazi ölçü birimleri ile temsil edilmiştir. Sayısal değerleri 1-9 arasında olan harfler m² ile, 10-90 arasında olan harfler aşır ölçü birimi ile, 100-1000 arasında olan harfler ise kafız ölçü birimi ile, 1000'den sonra gelen sayılar ise cerîb ölçü birimi ile temsil edilmektedir. Aşağıda verilen tabloya göre metindeki ölçü birimlerinin sırası takip edildiği zaman “bir işaret bekliyorum” cümlesini verecektir.

Tablo 48: Türk Alfabesindeki Harflerin Arazi Ölçü Birimleri ile Temsil Edilmesi						
F	Ş	M	H	E	P	N
1 m ²	2 m ²	3 m ²	4 m ²	5 m ²	6 m ²	7 m ²
U	B	İ	O	I	Y	L
8 m ²	9 m ²	1 aşır	2 aşır	3 aşır	4 aşır	5 aşır
Ü	K	T	A	V	R	Ö
6 aşır	7 aşır	8 aşır	9 aşır	1 kafız	2 kafız	3 kafız
Z	S	D	G	C	Ç	Ğ
4 kafız	5 kafız	6 kafız	7 kafız	8 kafız	9 kafız	1 cerîb
J						
-						

Kıralamış olduğun tarlaman ekim bilgisini unutma ya da karıştırma olasılığına karşı sana yazılı olarak anlatıyorum. İlk olarak girişin hemen sağındaki **9 metrekare ve 1 aşirlik** yere elma ekilecek. Eğer hemen karşıdaki taşlarla çevrili alana ne olacak diye soracak olursan, o halde bil ki şimdilik oraya bir şey yapılmayacak çünkü orada geçen seneden kalan **2 kafızlık** kiraz bulunmaktadır. Bu alanın hemen yanındaki **1 aşirlik** yere muz ekilecek fakat yanında **2 metrekarelik** ekime uygun olmayan bir alan bulunmakta orası mecburen boş kalacak. Muz ekilecek alanın hemen karşısında **9 aşır ve 2 kafızlık** olmak üzere ayrılmış iki ayrı alan bulunmakta, bu alanlara deneme amaçlı bu bölgede az bulunan erik ve kivi ekilecek. Eğer bu iki meyveden istenilen verim alınamazsa birleştirilip bu

alana da muz ekilecek. Çeşmenin yanındaki **5 metrekarelik** alan yanındaki **8 aşirlik** alan ile birleştirilerek ayva ekimi yapılacak. Sağındaki **9 metrekarelik** alan ise gerekli malzemelerin konulması için depo olarak kullanılacak. Çeşmenin tam karşısında kalan **5 metrekarelik** alanda senin dinlenmen için bir kulübe bulunuyor. En uçtaki **7 aşirlik** alana da bana en çok kazandıracak ürün olan hurma ekilecek, bu alanın hemen bitişiğinde **5 aşirlik** ayva ekimi için ayrılan alan bulunmaktadır. Çıkış kapısının hemen sağında kalan **1 aşir** ve **4 aşir** olarak ayrılmış yerler birleştirilerek üzüm ekilecek. Bu alanın tam karşısında yer alan ve toplam **2 aşir** ve **2 kafiz** olan yer ise kardeşimindir oraya dokunulmayacak. Son olarak orta kısımda gördüğün **8 metrekare** ve **3 metrekare** olarak ayrılmış yerlerle komşumun oğlu ilgilenecek. İşte tüm tarlanın planını olabildiğince açıklayıcı bir şekilde yazmaya çalıştım. Senin için tekrar hayırlı olmasını dilerim.

3.3.2.1.2.2. Harflerin Para Birimleri ile İlişkilendirilmesi

Açık metindeki harfler dinar miktarı ile temsil edilmektedir. Sayısal değerleri 1-9 arasında olan harfler tam dinar ile, 10-90 arasında olan harfler çeyrek dinar ile, 100-1000 arasında olan harfler ise yarım dinar ile temsil edilmiştir. Örneğin “h” harfi 4 tam dinar, “y” harfi 4 çeyrek dinar, “z” harfi ise 4 yarım dinar olarak yazılmaktadır. Bu eşleştirmeler kurgulanarak bir metin içerisine yerleştirilmiştir. Metindeki dinarların sırası takip edildiği zaman “bir işaret bekliyorum” cümlesini verecektir.

Tablo 49: Türk Alfabesindeki Harflerin Para Birimi ile Temsil Edilmesi

F	Ş	M	H	E
1 Dinar	2 Dinar	3 Dinar	4 Dinar	5 Dinar
P	N	U	B	İ
6 Dinar	7 Dinar	8 Dinar	9 Dinar	1 Çeyrek Dinar
O	I	Y	L	Ü
2 Çeyrek Dinar	3 Çeyrek Dinar	4 Çeyrek Dinar	5 Çeyrek Dinar	6 Çeyrek Dinar
K	T	A	V	R
7 Çeyrek Dinar	8 Çeyrek Dinar	9 Çeyrek Dinar	1 Yarım Dinar	2 Yarım Dinar
Ö	Z	S	D	G
3 Yarım Dinar	4 Yarım Dinar	5 Yarım Dinar	6 Yarım Dinar	7 Yarım Dinar
C	Ç	Ğ	J	
8 Yarım Dinar	9 Yarım Dinar	1/8 Dinar	-	

Sevgili kardeşim,

Mektubunu aldığıma ve iyi olmana çok sevindim. Allah afiyetini daim eylesin. Mektubunda benden istediğin meşhur davet yemeğinin yapılışını sana anlatacağım. Bu yemek, içinde kullanılan malzemelerin çokluğundan dolayı her zaman yapılabilecek bir yemek değildir bu nedenle ne kadar harcaman gerektiğini bilmen için malzemelerin miktarlarını sana fiyat türünden söyleyeceğim ki bilip ona göre hazırlığını yapabilesin. İlk olarak **9 dinarlık** soğanı ve **1 çeyrek dinarlık** pırasayı al, dış kabuklarını soy, yıka ve yumuşayana kadar suda pişir. Yeterince yumuşadıktan sonra soğumaya bırak ve küçük hale getirene kadar güzelce doğra. Şimdi aynı kapta **2 yarım dinarlık** havucu küçük parçalara ayırarak çok az bir su içerisinde haşla ve üzerine **1 çeyrek dinarlık** roka ve 2

dinarlık sarımsakları küçülterek ekle. Daha sonra tüm bu malzemeleri birbiri ile iyice karıştırarak bir kenarda beklet.

Başka bir kapta fiyatı **9 çeyrek dinar** kadar tutacak patlıcanları soy, dört parçaya ayır ve tuzlu suyun içerisinde pişir, yeterince yumuşadıktan sonra iyice ez. Bir havanda **2 yarım dinarlık** tarçın ile **5 dinarlık** kişnişi ez ve bir tutam tuz ekleyerek hepsini karıştır. Şimdi söyleyeceklerim biraz pahalı olabilir ama yemeğin asıl tadını verecek olan bu kısımdır bu yüzden şimdi sayacağım malzemeleri koymayı kesinlikle tavsiye ederim. Yaklaşık **8 çeyrek dinar** kadar kuru incir ve **9 dinar** kadar bademi sıcak suyun içerisinde bekleterek yumuşat. Bademlerin soyulmuş ve ikiye ayrılmış olmasına dikkat et. Sonra içerisine yumuşaması daha kolay olan **5 dinar** kadar hünnap ile **7 çeyrek dinar** kadar kuru üzümü de ekleyerek hepsini tekrar karıştır. Daha sonra hepsini sudan çıkar ve ezmiş olduğun patlıcanların üzerine dök.

Ardından **5 çeyrek dinar** kadar kuzu etini alarak orta büyüklükte parçalara ayır ve üzerine az bir miktar yağ koyarak pişirmeye başla fakat eğer etin kötü kokulu kısımları var ise onları önceden sıyırmalısın. Ayrı bir kapta **1 çeyrek dinarlık** sirke ile **4 çeyrek dinarlık** balı iyice karıştır sonra üzerine **2 çeyrek dinarlık** kekik, **2 yarım dinarlık** karabiber ve **8 dinarlık** safran serpererek hepsini tekrar karıştır ve pişmiş et parçalarının üzerine dök. Bu haliyle eti bir süre demlemeye bırak. Et yeterince demlendikten sonra üzerine ilk kısımda söylediğim soğanlı karışım ile karıştır. Son olarak bu etli karışımı daha önceden hazırladığın patlıcanlı karışımın üzerine dök böylece yemeğin hazır olacak. Eğer istersen en son üzerine **3 dinar** kadar turunc yaprağı da serpiştirerek servis edebilirsin.

Gördüğün gibi kardeşim bu yemeği yapmak oldukça zahmetli olsa da tadı bir kez tadanların bir daha unutamayacağı kadar güzeldir. Misafirlerine gönül rahatlığı ile ikram edebilirsin. Allah'ın rahmeti ve bereketi üzerine olsun.

3.3.2.1.2.3. Harflerin Haftanın Gün ve Saatleri ile İlişkilendirilmesi

Açık metindeki harfler haftanın gün ve saatleri ile temsil edilmiştir. Tüm harfler 7 gruba ayrılmış ve her grup haftanın bir günü ile ilişkilendirilmiştir. Harfler ise bulunduğu gruptaki sıra numarasına göre mensup olduğu günün saati ile temsil edilmektedir. Aşağıdaki tabloda harflerin gün ve saatleri belirtilmiştir. Metindeki gün ve saatlerin sırası takip edildiği zaman “bir işaret bekliyorum” cümlesini verecektir.

Tablo 50: Türk Alfabesindeki Harflerin Haftanın Gün ve Saatleri ile Temsil Edilmesi

HARF	GÜN	SAAT
D	Pazartesi	13:00
P	Pazartesi	14:00
T	Pazartesi	15:00
Y	Pazartesi	16:00
A	Pazartesi	17:00
N	Salı	13:00
O	Salı	14:00
R	Salı	15:00
Ü	Salı	16:00
I	Salı	17:00
U	Çarşamba	13:00
V	Çarşamba	14:00
C	Çarşamba	15:00
E	Çarşamba	16:00
F	Perşembe	13:00
H	Perşembe	14:00
Z	Perşembe	15:00
K	Perşembe	16:00
Ö	Cuma	13:00
Ğ	Cuma	14:00
M	Cuma	15:00
L	Cuma	16:00
B	Cumartesi	13:00
İ	Cumartesi	14:00
Ç	Cumartesi	15:00
J	Cumartesi	16:00
S	Pazar	13:00
G	Pazar	14:00
Ş	Pazar	15:00

Cumartesi günü saat 1'de yola çıkmayı planladığım yolculuğuma son anda çıkan ufak bir aksaklıktan dolayı gecikerek **cumartesi günü saat 2**'de çıkmış bulundum.

Yine de arkadaşına söz vermiş olduğum vakitte yani **salı günü saat 3**'te evlerine varabildim. Birlikte güzel bir yemek yiyip biraz hasret giderdikten sonra şehri dolaşmaya çıktık. Garip hissediyordum çünkü son gelişimden beri onca zaman geçmesine rağmen sanki hiçbir şey değişmemiş, her şey bıraktığı gibi kalmıştı. **Cumartesi günü saat 2**, artık birbirimize veda vaktimiz gelmişti. Hoşça kal canım dostum seni özleyeceğim dedim. **Pazar günü saat 3** ve benim o kadim şehre varmama çok az kaldı. Heyecanlıyım çünkü gidenlerin hayranlıkla anlattığı bu şehri ilk defa görme imkanına sahip olacağım. Kalacak güvenilir bir yer bulduktan hemen sonra gezmeye koyulma niyetindeyim. Burada **pazartesi günü saat 5'e** kadar vaktim olacak bu yüzden iyi bir şekilde değerlendirmem gerekiyor. Bu şehir gerçekten gezenlerin anlattıkları kadar varmış, ben de gördüklerimi imkânı olmayanlara anlatmak istiyorum ki onlar da öğrensinler. Artık bu şehirden ayrılma vakti geldi. Şimdi tekrar yola çıkma zamanı. **Salı günü saat 3**! Ne kadar da çabuk geçiyor zaman. Bana yola çıkalı sanki çok az bir zaman geçmiş gibi geliyor. Yollardayım, şimdiden anlatacak çok şey var ancak dönünce hepsini tek tek yazabileceğim. **Çarşamba günü saat 4**, küçük bir kasabaya geldim. Burası aslında planımda yoktu ama kendimi pek iyi hissetmediğim ve dinlenmeye ihtiyacım olduğu için biraz burada kalmaya karar verdim. **Pazartesi günü saat 3**, şimdi daha iyi hissediyorum, bu küçük kasabanın havası bana çok iyi geldi, burada güzel bir insana da rastladım. Kendisi buranın yerlisiymiş, sağ olsun benimle ilgilendi ve bazı ihtiyaçlarımı karşılamam için yardımcı oldu. Onu daha yakından tanımak ve teşekkür etmek istediğimi söyledim kabul etti, **cumartesi günü saat 1**'te merkezdeki caminin önünde buluşmak için sözleştik. Buraların yabancısı olduğum için beni evine davet etti ve bir bal şerbeti ikram etti. Biraz sohbet ettik ona ne iş yaptığını sordum, ticaretle uğraştığını bunun için sık sık kasabadan ayrıldığını söyledi. Ona bir dahaki yolculuğunu sordum, hemen bu **çarşamba günü saat 4** gibi çıkacağını söyledi. Desene bir daha görüşemeyeceğiz dedim, helalleştik ve evinden ayrıldım. **Perşembe günü saat 4** şimdi bu güzel kasabadan ayrılıyorum, yolda başıma bir şey gelmez ve sağ salım varabilirsem inşallah tekrar yazarım. **Cuma günü saat 4**'seyahatimin son şehrine sağ salım ulaştım ama henüz kalacak yer bulamadım ama en son uğradığım yer bana yarın yani **cumartesi günü saat 2**'te gelmemi söyledi. Bu gece artık bir şekilde başımın çaresine bakacağım. Şimdi ertesi günden bildiriyorum gece tahminimden daha serin geçti biraz üşüdüm ama şu an gayet iyiyim. Son durağım olan bu şehirde güzelce vakit geçirmeyi umuyorum. Gitmeden **pazartesi günü saat 4**'te en büyük halamın oğlu ile

görüŖeceęim. **Salı gn saat 2** ya da **salı gn saat 3** gibi Ŗehirden ayrılmayı planlıyorum. Kk bir gecikme ile **arŖamba gn saat 1**'te yola ıkmıŖ oldum. Nihayet **cuma gn saat 3**'te evime dnmŖ **bulunuyorum**. Gzelce dinlendikten sonra unutmadan bu seyahatimde tm grdklerimi ve baŖımdan geen her Ŗeyi ayrıntılı bir Ŗekilde yazacaęım.

3.3.2.1.2.4. Harflerin Kitap İsimleri ile İliŖkilendirilmesi

Aık metindeki harfler kitap isimleri ile temsil edilmiŖtir. Her harf bir kitap ismi ile eŖleŖtirilmiŖ ve kurgulanarak bir metin ierisine yerleŖtirilmiŖtir. Metindeki kitap isimlerinin sırası takip edildięi zaman "bir iŖaret bekliyorum" cmlerini verecektir.

Tablo 51: Harflerinin Kitap İsimleri ile Temsil Edilmesi

HARF	KİTAP İSMİ	MÜELLİF
F	Kitâbü Mîzânî'l-hikme	El-Hâzinî
Ş	Tezkiretü'l-kehhâlîn fi'l-'ayn ve emrâzihâ	Ali bin İsa-el-Kehhar
M	El Câmi-u'l Beyn'el İlmî ve El-Amelî'en Nâfi fî Sınâ'atî'l Hiyel	Cezerî
H	El-Hâvî fi't-tıb	Ebû Bekr er-Râzî
E	El-Cemâhir fî ma'rifeti'l-cevâhir	Bîrûnî
P	Kitâbü'l-Menâzır	İbnü'l-Heysem
N	Kitâb fîmâ yahtâcü ileyhi'l-küttâb ve'l-'ummâl min 'ilmi'l-hisâb	Bûzcânî
U	Risâle fi'l-berâhîn 'alâ mesâ'ilî'l-cebr ve'l-mukâbele.	Ömer hayyâm
B	El-Mûcezz fi't-tıb	İbnü'n-Nefîs
i	El-Câmi' li-müfredâtî'l-edviye ve'l-acziye	İbnü'l-Baytâr
O	Kitâbü'l-Muhtaşar fî hisâbî'l-cebr ve'l-mukâbele	Hârezmî
I	Kitâbü San'atî'l-usturlâb	Kûhî
Y	Kitâbü'l-Hey'e	Bitrûcî
L	Ebvâb lâ yestacnî men yerûmü 'amele'l-usturlâb	Mecrîtî
Ü	Risâle fî cedveli'd-dağa'ik.	İbn Irâk
K	Zîc-i İlhanî	Tûsî
T	Mürücü'z-zeheb ve me'âdinü'l-cevher	Mes'ûdî
A	Hayat'ül Hayvan el-Kübra	Demîrî
V	el-Faḥrî fi'l-cebr ve'l-mukâbele.	Kerecî
R	Kitâbü't-Taşrîf li-men 'aceze 'ani't-te'lîf	Zehrâvî
Ö	Mesâlihu'l-ebdân ve'l-enfûs	Ebû Zeyd el-Belhî
Z	Kitâbü'z-Zîc.	Bettânî
S	el-Kânûn fi't-tıb	İbn Sînâ
D	Kitâbü'l-Mesâ'ilî'l-'adediyye	Ebû Ca'fer el-Hâzin
G	Uyûnü'l-enbâ' fî ṭabaḳatî'l-etibbâ	İbn Ebu Usaybia
C	Sûretü'l-arz	İbn Havkal
Ç	Kitâbü'l-Filâha	İbnü'l-Avvâm
Ğ	Acâ'ibü'l-mahlûkât ve garâ'ibü'l-mevcûdât.	Kazvînî
J	-	-

Kardeşim benden faydalı ilim için bazı tavsiyeler istedin. Ben de aklıma öncelikli olarak gelenleri memnuniyetle paylaşacağım. Bu eserleri bulduğun zaman altından daha kıymetli bir şey bulduğunun farkında ol ve ona göre sevin, ama sadece sevinmek yetmez anladıklarını uygulaman, üzerine üretmen ve bunları da paylaşman gerekir. Bu sorumluluğu bilersen bereketini de görürsün.

Eğer sağlık alanında çalışmak istersen **el-Mûcezz fi't-tıbb** adlı kitaptan başlayabilirsin. Bu kitapta tıp ilmine dair hem teorik hem pratik pek çok bilgi bulabilir, çeşitli ilaç tarifleri ve organlarla hastalıkların ilişkileri gibi faydalı bilgiler edinebilirsin. İkinci olarak **el-Câmi' li-müfredâtî'l-edviye ve'l-acziye** adlı eseri okumanı tavsiye ederim. Bu kitapta Akdeniz, Ortadoğu ve Anadolu'nun birçok bölgesinde yetişen bitkilerden hangi ilaçların yapılabildiğini ve bu ilaçların hastalıkları önlemede ne derece etkili olduklarını hakkında bilgi sahibi olabilirsin. Senin de bildiğin gibi hastalıklar bu hayatın bir gerçeğidir ve onlarla baş edebilmenin en güzel yolu onlara etki eden ilaçları kullanmaktır. Eğer hala bu alanda çalışmaya kararlı isen **Kitâbü't-Taşrîf li-men 'aceze 'ani't-te'lîf** kitabını mutlaka temin etmeye çalış, içindekileri ben anlatmakla bitiremem. Sen kendin gör, fazlasıyla şaşıracaksın. Özellikle **el-Câmi' li-müfredâtî'l-edviye ve'l-acziye** kitabı ile okumanı tavsiye derim. Bunun dışında **Tezkiretü'l Kehhalin fi'l Ayn ve Emraziha** adlı eser genel sağlık bilgilerinin yanında çok önemli bir organ olan göze dair kapsamlı bilgiler sunmaktadır. İmkânın olursa mutlaka bakmanı tavsiye ederim.

Eğer insanın dışına çıkmak istersen bir tür hayvanlar ansiklopedisi gibi düşünebileceğin **Hayat'ül Hayvan el-Kübra** isimli esere bakabilirsin, bu eserde müellif incelediği birçok hayvana dair gözlemlerini aktarmaktadır. Daha önce bahsettiğim **Kitâbü't-Taşrîf li-men 'aceze 'ani't-te'lîf** eseri gibi oldukça detaylıdır. Hangi tür ilimle uğraşırsan uğraş genel kültürünü iyi bir seviyede tutmaya çalışmalı ve bunun için çeşitli okumalar yapmalısın. **El-Cemâhir fi ma 'rifeti'l-cevâhir** adlı eserden ahlak, siyaset, psikoloji ve tarih gibi genel kültür konularını okuyabilirsin. Bununla birlikte **Mürûcû'z-zehab ve me'âdinü'l-cevher** isimli eser de tarih, kültür, coğrafya ve birçok konu açısından oldukça zengindir, ufkunu genişletmen için okumanı tavsiye ederim. **El-Mûcezz fi't-tıbb** ve **el-Cemâhir fi ma 'rifeti'l-cevâhir** eseri gibi çok anlaşılır şekilde yazılmıştır.

Eğer daha teknik alanlara yönelmek istersen **Zîc-i İlhânî** adlı eserden takvimlerin bilgileri, gezegenlerin yerleri, yerleşim merkezlerinin koordinatları ve namaz vakitleri gibi astronomiye dair birçok meseleyi öğrenebilirsin. Bu bilgiler yaşadığın evreni daha iyi

anlamana ve daha düzenli bir hayat sürmene yardımcı olacaktır. Birçok amaçta kullanılan usturlap aletinin teknik yapımı ve nasıl kullanıldığına dair bilgi edinmek istersen de *Ebvâb lâ yestacnî men yerûmü 'amele'l-usturlâb* isimli eserden yardım alabilirsin. *El-Câmi' li-müfredâtî'l-edviye ve'l-acziye* eseri gibi alanında yazılmış en iyi eserlerden biridir. Belirli bir düzeye geldikten sonra ise astronomi alanında bazı yenilikler içeren ve sana farklı bakış açıları kazandıracak olan *Kitâbü'l-Hey'e*'yi okuyabilirsin. Matematikle ilgilenmek istersen *Kitâbü'l-Muhtaşar fî hisâbi'l-cebr ve'l-mukâbele* adlı eser tam bir baş ucu kitabıdır, günlük hayatta ihtiyaç duyacağın hesaplamalar için sana oldukça yardımcı olacaktır. Söylemeyi unuttum *Kitâbü't-Taşrîf li-men 'aceze 'ani't-te'lîf* eserinde teorik bilginin yanında tedavi yöntemleri ile alakalı pek çok aletin bilgisini de öğreneceksin. Denklerin sınıflandırılması ve çözüm yöntemleri için ise *Risâle fî'l-berâhîn 'alâ mesâ'ili'l-cebr ve'l-mukâbele* isimli esere bakmanı öneririm. Son olarak *El-Câmi-u'l Beyn'el İlmi ve El-Ameli'en Nâfi fî Sınâ'ati'l Hiyel* isimli bu kitapta günlük hayatta farklı amaçla kullanılan birçok aletin nasıl yapılacağına dair teknik bilgileri ve bu aletlerin kullanım amaçlarını öğrenebilirsin. Teorik bilgilerden ziyade pratik bilgileri içeren bu eserin anlatımı da gayet açıklayıcı ve güzeldir.

Benim verebileceğim tavsiyeler şimdilik bu kadar, sen bu yola girdikten sonra zamanla yenilerinden haberdar olacak ve neyin senin için daha faydalı olacağına kendin karar vereceksin inşallah. Allah ilmini artırsın.

3.3.2.2. Harflerin Sayısal Değerlerinin Bir Metin İçerisine Yerleştirilmesi Örneği

“Bir işaret bekliyorum” cümlesindeki harflerin sayısal değerleri sırasıyla aşağıdaki metin içerisine yerleştirilmiştir.

Tek bir periyotta, Merkür Güneş'in etrafında **9** kere döner, Venüs **10** kere döner, Dünya **200** kere döner, Mars **10** kere döner, Jüpiter **2** kere döner, Satürn **90** kere döner. Diğer periyotta, Merkür Güneş'in etrafında **200** kere döner, Venüs **5** kere döner, Dünya **80** kere döner, Mars **9** kere döner, Jüpiter **5** kere döner, Satürn **70** kere döner. Üçüncü periyotta, Merkür Güneş'in etrafında **50** kere döner, Venüs **10** kere döner, Dünya **40** kere döner, Mars **20** kere döner, Jüpiter **200** kere döner, Satürn **8** kere döner. Bu yüzden **3** periyot kullanılır.

3.3.2.3. Mesajın Başka Bir Bağlam İçerisine Yerleştirilmesi Örnekleri

3.3.2.3.1. İlk Harfler ile

Aşağıdaki metinde her kelimenin ilk harfi sırayla “bir işaret bekliyorum” cümlesindeki harflerle başlamaktadır.

Bir ince ruhlu içli şair, akşam rüzgârı eşliğinde tahliline başladı. Edebiyat kitaplarının listesini inceleyerek yazdı. Okudukça rahledekileri umudu mayalandı.

3.3.2.3.2. İkinci Harfler ile

Aşağıdaki metinde her kelimenin ikinci harfi sırayla “bir işaret bekliyorum” cümlesindeki harflerden oluşmaktadır.

Abartı hislerin arkasında bir aşk sancısı aranır. Derine atmak abes gelirken, ukde olan hisler ayıplanma korkusunu eriterek durulmazsa, imkansızlaşırlar.

3.3.2.3.3. Sonuncu Harfler ile

Aşağıdaki metinde her kelimenin son harfi sırayla “bir işaret bekliyorum” cümlesindeki harflerle bitmektedir.

Gayb alemi acayıptır, aceleci adanış fazla acıtır. Özellikle üst gayb ahirette somutlaşarak bütünsel aciziyeti epey fiyasko hissettirir. Bunu söylemeliydim.

3.3.2.3.4. Belirli Harfler ile

Aşağıdaki metinde her üç kelimede bir, birinci kelimenin birinci harfi, ikinci kelimenin ikinci harfi, üçüncü kelimenin üçüncü harfi sırayla “bir işaret bekliyorum” cümlesindeki harflere denk gelecek şekilde oluşmaktadır.

Bilgi gizleme, her inançta aşikâr olarak reddedilmiştir. Detay katılarak bağımsız kelimelerin sokulması lafı gizleme sayılmaktadır. O arkadaş abukluklara meyletmemelidir.

3.3.2.3.5. Kelimelerin Ayrılması ile

Aşağıdaki metinde sırayla her cümleinin ilk kelimesi “bir işaret bekliyorum” cümlesini vermektedir.

Bir çözüm arıyorum. İşaret edilirse bulacağım. Bekliyorum umutla görebilmeyi.

3.3.2.4. Harflerin Sayısal Değerlerine Denk Yeni Kelimelerin Üretilmesi Örneği

Aşağıdaki şifreli metinde nokta ile ayrılan kelimelerin harflerinin sayısal değerlerinin toplamı açık metindeki her harfin sayısal değerine denk olacak şekilde hazırlanmıştır.

Bir grup arasında gizli bir buluşma yapılacağı ve buluşma saatinin şifreli olarak iletilmesi gerektiğini varsayalım. Buluşma saati “üç” olarak kabul edilirse tablo 27’deki harflerin sayısal değerlerine göre aşağıdaki şekilde bir şifreleme yapılabilir.

“İyi. Zamanlama benim işim şefi⁴⁵”

⁴⁵ Erkek ismi.

Tablo 52: “Üç” Mesajındaki Harflerin Sayısal Değerlerine Karşılık Kelime Üretme

Mesaj	Sayısal Değer	Şifre	Sayısal Değer
Ü	60	İyi	10+40+10
Ç	900	Zamanlama benim işim Şefi	400+90+3+90+7+50+90 +3+90+9+5+7+10+3 +10+2+10+3+2+5+1+10
Üç	960	İyi. Zamanlama benim işim Şefi	10+40+10+400+90+3+90 +7+50+90+3+90+9+5+7 +10+3+10+2+10+3+2+5 +1+10

SONUÇ

Kriptoloji alanında kaleme alındığı bilinen ilk eserin yazarı Kindî, antik bilimsel eserlerde anlamı bilinmeyen pek çok sembol bulunduğunu ve bu yüzden şifre çözümlemenin, bilimsel çalışmalarda ilerleyebilmek için öğrenilmesi gereken bir uğraş olduğunu ifade etmiştir. Bununla birlikte Kindî, bu antik eserlerin şifreleme ya da şifre çözümü yöntemlerine değinip değinmediği hakkında herhangi bir açıklama yapmamıştır. Kriptoloji tarihindeki ikincil kaynaklar da Kindî öncesinde yazıldığı tespit edilmiş bir eserin tespit edilmediğini bildirir. Bu açıdan Kindî'nin şifrelemeye dair eseri, şifreleme yöntemlerini sınıflandırması, frekans analizi yöntemini tanıtmaması ve Arap harflerinin birleşme ya da birleşmeme durumlarını inceleyerek dilin yapısal özelliklerini ele alması bakımından kriptoloji bilimine dair özgün katkılar sağlamıştır. İslam medeniyetinde kriptoloji çalışmalarının Kindî'nin eserinden ibaret kalmadığını, hatta ilerleyen yüzyıllarda bir geleneğin oluştuğunu görmekteyiz. Nitekim İbn 'Adlān, İbn Duneynîr ve İbnu'd-Dureyhim bu tezde ele alınan eserleri yazdıkları gibi şifreleme ile ilgili başka eserlerinin de olduğunu söylemişlerdir. Mesela İbn 'Adlān, şifrenin gizlenmesi yöntemine dair ayrı bir çalışma hazırlama niyetinde olduğunu fakat şifre alfabelerinin oluşturulmasından bahsederken bu yöntemin başka eserlerde de yaygın olarak bulunduğunu ifade etmiştir. Yani eserlerinde şifrelemeden bahsederken olmayan bir şeyi, kimsenin ilgilenmediği bir konuyu ele alıyor gibi değil, halihazırda İslam medeniyetindeki literatürde aktif durumdaki bir konuda eser yazıyor gibi görünmektedirler ki bu da İslam medeniyetinde kriptoloji geleneğinin varlığını ortaya koyan delillerden kabul edilebilir.

Yaklaşık dokuzuncu yüzyılın ortaları itibarıyla başlayan bu süreci, aynı dönemde yoğunlaşan tercüme hareketleri ile dil ve matematik alanında yapılan gelişmelerin teşvik ettiği düşünülmektedir. Bunun yanı sıra İslam medeniyetinin geniş bir coğrafyaya yayılmasının ve Emevîler sonrasında birbiriyle rekabet halinde birçok devletin ortaya çıkışının getirdiği etkili yönetim ve haberleşme ihtiyacı da kriptoloji biliminin gelişebilmesi için tetikleyici bir faktör olmuştur. Özellikle matematiğin gelişimi burada dikkat çekicidir. Öyle ki konumlu, on tabanlı ve dokuz rakam ile sıfırın kullanıldığı sistemin işlem kabiliyetini artırması, şifreleme yöntemlerine de yansımıştır. Harflerin

ebced sisteminde denk oldukları sayısal değerlere çarpma ve bölme işlemleri uygulanarak tekrar harflere dönüştürülmesi ile şifrelerin zorluk derecesi artırılmıştır. Şifredeki harfler yerine denk oldukları sayıların okunuşlarının yazılması ya da parmak işaretleri ile gösterilmesi ise başka bir yöntem olarak kullanılmıştır. İbn Duneynır'ın Arap rakamlarının bir astronomi metni içerisine yerleştirilmesini önermesi ve bu yöntemi uygulayacak kişinin aritmetik ve astronomi konusunda bilgili olması gerektiğini belirtmesi de matematiksel bilimlerin şifreleme yöntemleri ile ilişkisine başka bir örnek olarak verilebilir.

İslam medeniyetinin coğrafi sınırlarının genişlemesi, Arap dilinin doğru bir şekilde öğrenilmesini sağlama amacını doğurmuş ve bu dilin kurallarının sistemli bir şekilde ortaya konması için çeşitli çalışmaların yolunu açmıştır. Bu çalışmaların yansımaları da şifreleme yöntemlerinde kendisini göstermiştir. Bu dildeki harflerin kullanım sıklıkları bilgisi, genellikle birlikte kullanılan harflerin sıklıkları bilgisi, çoğunlukla kelimelerin başında ve sonunda kullanılan harflerin bilgisi, belirlilik takısından önce gelen harflerin bilgisi ve harflerin art arda gelme durumlarının bilgisi gibi titiz çalışmaların ürünü olan Arap diline ait detaylar şifrelerin çözülmesini daha zorlaştırmak için birer ipucu niteliğinde kullanılmıştır. Zira şifreleme yöntemlerinde başarılı olmanın bir yolu da şifrenin, dilin gramerinin tüm detaylarının dikkate alınarak hazırlanmasıdır. Aksi takdirde, göz ardı edilen küçük bir detay şifrenin fazla zorlanılmadan açığa çıkmasına sebep olabilmektedir. Bu bakımdan şifrenin zor çözülebilir olması, çoğu zaman olağanüstü karmaşık bir şifreleme yöntemi kurulmasından kaynaklanmaz. Aksine, nispeten basit görünen bir yöntem, dilbilgisinin incelikleri sayesinde karmaşık hale gelir ve şifrelemeyi hakkettiği zorluğa ulaştırır. İşte bu yüzden bu çalışmada incelenen eserlerin müellifleri de dil bilgisi kurallarının iyi seviyede bilinmesini bu bilimde başarıya ulaşmanın şartlarından biri olarak zikretmişlerdir.

Bu çalışmada dikkat çekici olarak görülebilecek hususlardan biri, şifreleme yöntemlerinin sayısının fazlalığıdır. Her ne kadar tezde ele alınan çalışmaların müellifleri birçok farklı yöntemin kullanılmış olmasının amacına dair bir bilgi sunmasa da şifreleme yöntemlerinin neredeyse sayısız miktarda çoğaltılabileceğini öne sürmüşlerdir. Ele alınan bazı yöntemler birbirine çok yakın olsa bile, gerçekten küçük ayrıntılar sayesinde

farklılaşmış onlarca yöntem ortaya konmuş olması ve bunların teorik olarak yüzlerce farklı türe dönüştürülebilir nitelikte olmaları, kriptolojinin, özellikle de Arapça dilbilgisi yardımıyla ne kadar geniş bir alana dönüştüğünü göstermektedir.

Dikkat çekilmesi istenen konulardan biri şifreleme sınıflandırmalarında “şifrenin gizlenmesi yolu ile yapılan şifreleme” olarak adlandırdığımız steganografi yönteminin kullanılmasıdır. Satranç tahtası, delikli tahta, renkli boncuklar ve kâğıt katlama gibi araçlar ile mesajın gizli bir şekilde iletilmesinin yanı sıra metin steganografisinin daha çok öne çıktığı görülmektedir. Özellikle İbn Duneynîr’in detaylı olarak ele aldığı bu yöntemin, İbnu’d-Dureyhim tarafından eklenen kısıtlamalar ile daha özgün bir hale ulaştığı görülmektedir.

Üzerinde durulması gereken diğer bir nokta, eserleri değerlendirirken yazılış amaçlarının da göz önünde bulundurulması gerektiğidir. Örneğin İbn ‘Adlân’ın, eserini şifre çözümlemeleri üzerine pratik bir el kitabı niyetiyle yazması, eseri teferruattan uzak sadece belirli kuralları içermesi ile öne çıkarırken İbn Duneynîr ve İbnu’d-Dureyhim’in eserleri, şifreleme yöntemlerinin detaylı olarak ele alınması ile dikkat çekmektedir. Ayrıca İbn Duneynîr’in şiirsel şifrelemelere neredeyse düzyazıda yapılan şifrelemeler kadar yer vermesi şiirin kendi dönemindeki yaygın kullanımına güzel bir örnek teşkil etmektedir.

Sonuç itibarıyla incelenen üç eserden yola çıkılarak, 13. ve 14. yüzyıllarda İslam medeniyetindeki kriptoloji bilgisinin sistemli ve kapsamlı bir seviyeye ulaştığı görülmektedir. Ulaşılan bu seviyenin en somut örneği şifreleme yöntemlerinde gözlenebileceği için bu çalışmanın büyük bir kısmı bu yöntemlerin örneklerine ayrılmıştır. Yöntemler, aralarındaki benzerlik ve farkların daha iyi görülebilmesi için öncelikle bir sınıflandırılmaya tâbi tutulmuştur. Bu şekilde daha düzenli bir yapı içerisine yerleştirildikten sonra aslına bağlı kalınmaya çalışılarak Arapça örneklendirmeleri ardından bu örneklerin Türkçe uyarlamaları yapılmıştır. Örnekler için esas itibarıyla iki ana alt başlığa ayrılan sınıflandırmada, başlıklardan biri için kısa diğeri için uzun olmak üzere iki ayrı mesaj seçilmiştir. Dolayısıyla yöntemler arasındaki farkların daha net bir şekilde görülmesi amacıyla bu başlıkların altına düşen biri hariç tüm yöntemler için aynı

mesajın şifrelemesi yapılmıştır. Bununla beraber her yöntemin kendine özgü kısıtlaması olduğundan ortaya çıkan şifreleme örneklerinde kaçınılmaz olarak anlamsal bazı tuhafliklar ortaya çıkmış olsa da bu tuhafliklar en asgari seviyede tutulmaya çalışılmıştır. Benzer şekilde, Arapça şifreleme örnekleri ilk olarak Türkçe düşünülerek oluşturulmuş daha sonra Arapçaya tercüme edilmiştir. Ancak Arapçada isim ve sıfat tamlamaları gibi bazı gramer kuralları Türkçedekinin bütünüyle farklı olduğundan, bu durum şifreleme yaparken bazı örneklerde cümlelerin uzatılmasına ve anlamda zorlamaya neden olmuştur.

Bu çalışmada araştırma konusu olan üç yazarın da Musul doğumlu ve Memlukler devrinde yaşamış olmaları, kriptolojinin gelişiminde bölgesel ve dönemsel etkileri akla getirmektedir. Bu durumda şifreleme yöntemlerinin bölgelere göre değişiklik gösterip göstermediği ayrıca incelenmesi gereken bir çalışmanın konusudur. Bu konunun, ilgili dönemde farklı bölgelere ait yazılmış kriptoloji eserlerinin keşfedilmesi ile ileriki çalışmalarda açıklığa kavuşturulması umulmaktadır.

Bu çalışmanın kriptoloji tarihi çalışmalarına bir katkı sunması temenni edilmekte ve çalışmada konu dışı bırakılan şiirsel şifrelemeler de ayrıca incelenmeyi beklemektedir. Bununla birlikte ilerleyen zamanlarda konu ile ilgili yeni kaynaklar ortaya çıktıkça bu alandaki çalışmaların daha fazla detaylandırılabilmesi ümit edilmektedir.

KAYNAKÇA

- Açıl, C. (2019). Memlûklerin Kuruluş Sürecinde Memlûk-Moğol Mücadelesi. *Yayınlanmamış Yüksek Lisans Tezi. Marmara Üniversitesi, Sosyal Bilimler Enstitüsü, İslam Tarihi ve Sanatları Anabilim Dalı. İstanbul.*
- Akleylek, S., Akyıldız, E., & Çimen, C. (2012). *Şifrelerin Matematiği: Kriptografi*. Ankara: Odtü Yayıncılık.
- Alam, Y. M., at-Tayyan, M. H., & Mrayati, M. (2002). *Arabic Origins of Cryptology: al-Kindi's Treatise on Cryptanalysis* (Cilt 1). Riyadh: KFCRIS & KACST.
- Alam, Y. M., at-Tayyan, M. H., & Mrayati, M. (2003). *Arabic Origins of Cryptology: Ibn'Adlan's Treatise al-mu'allaf lil-malik al-'Asraf* (Cilt 2). Riyadh: KFCRIS & KACST.
- Alam, Y. M., at-Tayyan, M. H., & Mrayati, M. (2004). *Arabic Origins of Cryptology: Ibn ad-Durayhim's Treatise on Cryptanalysis* (Cilt 3). Riyadh: KFCRIS & KACST.
- Alam, Y. M., at-Tayyan, M. H., & Mrayati, M. (2005). *Arabic Origins of Cryptology: Ibn Dunaynir's Book: Expositive Chapters on Cryptanalysis* (Cilt 4). Riyadh: KFCRIS & KACST.
- Alam, Y. M., at-Tayyan, M. H., & Mrayati, M. (2007). *Arabic Origins of Cryptology- Two Treatises on Cryptanalysis: The Two Essays, The Treatise of ibn Wahab al-Katib* (Cilt 6). Riyadh: KFCRIS & KACST.
- Anderson, J. R., Kuhn, G. M., & Petitcolas, A. F. (1999). Information Hiding- A Survey. *Proceedings of the IEEE*, 87(7).
- Aslan, F. B. (2013). İslam Öncesi Dönemden Emevi Döneminin Sonuna Kadar Tercüme Faaliyetleri. *Eskiyeini*(27).
- Ayyıldız, M. N. (2019). Arap Dili Tarihi ve Arap Dili Gramerinin (Nahiv Sarf) Ortaya Çıkış Süreci. *Iğdır Üniversitesi İlahiyat Fakültesi Dergisi*(13).
- Bakkal, A. (2019). İslam Tarihinde Rasathaneler. *Bilimname*, 3.
- Blake, B. J. (2010). *Secret Language*. New York: Oxford University Press.
- Borda, M. (2011). *Fundamentals in Information Theory and Coding*. Chennai: Springer-Verlag Berlin Heidelberg.

- Burgu, A. (2017). Abbasiler'de Tercüme Faaliyetleri. Yayınlanmamış Yüksek Lisans Tezi. Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü, Tarih Anabilim Dalı., Konya.
- Cawthorne, N. (2018). *The History of Code Breaking*. New York: The Rosen Publishing Group.
- Cebbar, A. (2018). *İslam Bilim Tarihi- İslam Coğrafyasının Bilim Mirası Üzerine Konuşmalar*. İstanbul: Küre Yayınları.
- Churchhouse, R. (2004). *Codes and Ciphers-Julius Caesar, the Enigma and the Internet*. Cambridge: Cambridge University Press.
- Cimino, A. (2017). *The Story of Codebreaking From Ancient Ciphers to Quantum Cryptography*. Arcturus Publishing.
- Cobb, C. (2004). *Cryptography for Dummies*. Indianapolis: Wiley Publishing.
- Corbin, H. (2010). *İslam Felsefesi Tarihi-Başlangıçtan İbn Rüşd'ün Ölümüne*. İstanbul: İletişim Yayınları.
- Dağbaşı, G. (2013). Abbasi Dönemi Çeviri Faaliyetleri. *Eskiye*(27).
- Delfs, H., & Knebl, H. (2007). *Introduction to Cryptography Principles and Applications*. India: Springer-Verlag Berlin Heidelberg.
- Dereli, M. V. (2020). Arap Dili ve Edebiyatının İslam Medeniyeti için Önemi. *Necmettin Erbakan Üniversitesi İlahiyat Fakültesi Dergisi*, 49.
- Dooley, J. F. (2013). A Brief History of Cryptology and Cryptographic Algorithms. *Elektronik Kitap: Google Books*.
https://books.google.com.tr/books?id=d2O4BAAQBAJ&printsec=frontcover&hl=tr&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false Erişim: Aralık 2022. Springer.
- Fazlıoğlu, İ. (1993). *Cebir*. 17 Ocak 2023 tarihinde TDV İslâm Ansiklopedisi: <https://islamansiklopedisi.org.tr/cebiri> adresinden alındı
- Fazlıoğlu, İ. (1997). *Harizmi, Muhammed b. Mûsâ*. 18 Ocak 2023 tarihinde TDV İslâm Ansiklopedisi: <https://islamansiklopedisi.org.tr/harizmi-muhammed-b-musa> adresinden alındı
- Frary, M., & Pincock, S. (2021). *şifrelerin Gizemli Serüveni*. İstanbul: Ketebe Yayınları.
- Gaines, H. F. (2014). *Cryptanalysis a Study of Ciphers and Their Solution*. New York: Dover Publications.

- Gutas, D. (2020). *Yunanca Düşünce Arapça Kültür: Bağdat'ta Yunanca-Arapça Çeviri Hareketi ve Erken Abbasi Toplumu*. İstanbul: Kitap Yayınevi.
- Hamidullah, M. (2016). *İslam'a Giriş*. Ankara: Türkiye Diyanet Vakfı Yayınları.
- Haykıran, k. R. (2015). İlhanlılar Zamanında Kültür ve Eğitim. *Yayımlanmamış Doktora Tezi*. Ankara Üniversitesi, Sosyal Bilimler Enstitüsü, Tarih Anabilim Dalı. Ankara.
- Holden, J. (2017). *The Mathematics of Secrets*. Oxford: Princeton University Press.
- Ifrah, G. (2000). *The Universal History of Numbers: From Prehistory to the Invention of the Computer*. USA: John Wiley & Sons.
- Köroğlu, B. (2021). Kindî'nin Din ve Felsefe Uzlaştırma Metodu Üzerine: Arka Plan ve Kavramlar. *Beytulhikme an International Journal of Philosophy*.
- Kahn, D. (1973). *The Codebreakers, the Story of Secret Writing*. New York: The Macmillan Company.
- Kalın, İ. (2017). *Ben, Öteki ve Ötesi: İslam Batı İlişkilerine Tarihi Giriş*. İstanbul: İnsan Yayınları.
- Kaya, M. (2002). *Kindî, Ya'kûb b. İshak*. Nisan 2022 tarihinde TDV İslâm Ansiklopedisi: <https://islamansiklopedisi.org.tr/kindi-yakub-b-ishak> adresinden alındı
- Kaya, M. (2018). Kindî: İslam Dünyasının Felsefeyle Tanışması. M. C. Kaya, & M. C. Kaya (Dü.) içinde, *İslam Felsefesi- Tarih ve Problemler*. Ankara: Türkiye Diyanet Vakfı Yayınları.
- keleş, H. (2010). Memlükler'de Bilimsel, Sosyal ve Kültürel Hayat. *Yayımlanmamış Yüksek Lisans Tezi*. Gaziosmanpaşa Üniversitesi, Sosyal Bilimler Enstitüsü, Tarih Anabilim Dalı. Tokat.
- Lindberg, C. D., & Shank, H. M. (2013). *The Cambridge History of Science* (Cilt 2). New York: Cambridge University Press.
- Macrakis, K. (2014). *Prisoners, Lovers, and Spies: The Story of Invisible Ink from Herodotus to al-Qaeda*. the USA: Yale University Press.
- Madhekar, T., Narayan, K. R., Pandya, D., Thakare, B., & Thakkar, S. (2015, December). Brief History of Encryption. *International Journal of Computer Applications*, 131(9).

- Mollin, R. A. (2005). *Codes: The Guide to Secrecy From Ancient to Modern Times*. K. H. Rosen içinde, *Discrete Mathematics and Its Applications*. the USA: Chapman and Hall/CRC.
- Mselle, J. L., & Kondo, S. T. (2013). An Extended Version of the Polybius Cipher. *International Journal of Computer Applications*, 79, 31.
- Özgüdenli, O. G. (2020). *Moğollar*. Mart 2023 tarihinde TDV İslâm Ansiklopedisi: <https://islamansiklopedisi.org.tr/mogollar> adresinden alındı
- Rashed, R. (2015). *Classical Mathematics from Al-Khwarizmi to Descartes*. New York: Routledge.
- Sezgin, F. (2015). *İslam'da Bilim ve Teknik, Arap-İslam Bilimleri Tarihine Giriş* (Cilt 1). Ankara: Türkiye Bilimler Akademisi.
- Singh, S. (2002). *The Code Book*. New York: Delacorte Press.
- Şirinov, A. (2012). *TÛSÎ, Nasîrüddin*. Mart 2023 tarihinde TDV İslâm Ansiklopedisi: <https://islamansiklopedisi.org.tr/tusi-nasiruddin> adresinden alındı
- Türker, Ö. (2019). İslam Düşüncesinde İlimler Tasnifi. M. Arıcı içinde, *İlimleri Sınıflamak: İslam Düşüncesinde İlimler Tasnifi* (s. 63-73). İstanbul: Klasik Yayınları.
- Topuzoğlu, T. R. (1997). *Halîl b. Ahmed*. Ocak 2023 tarihinde TDV İslâm Ansiklopedisi: <https://islamansiklopedisi.org.tr/halil-b-ahmed> adresinden alındı
- Turabi, A. H. (2002). *KİNDÎ, Ya'kûb b. İshak*. Nisan 2022 tarihinde TDV İslâm Ansiklopedisi: <https://islamansiklopedisi.org.tr/kindi-yakub-b-ishak#2-musiki> adresinden alındı
- Unat, Y. (2013). *Zic-i İlhani*. Mart 2023 tarihinde TDV İslâm Ansiklopedisi: <https://islamansiklopedisi.org.tr/zic-i-ilhani> adresinden alındı
- Ülken, H. Z. (2020). *İslam Felsefesi-Eski Yunan'dan Çağdaş Düşünceye Doğru*. Ankara: Doğu Batı Yayınları.
- Yarbrough, L. (2013). Ibn al-Durayhim. D. Thomas, A. Mallet, J. P. Monferrer Sala, J. Pahlitzsch, M. Swanson, H. Teule, & J. Tolan içinde, *Christian-Muslim Relations. A Bibliographical History* (Cilt 5). Leiden: Brill Academic Publishers.
- Yazıcı, R. (2004, Aralık). Bilgi Değeri Açısından Cefr ve Ebced - Harfler ve Rakamlar Metafiziği. *Milel ve Nihal: İnanç, Kültür ve Mitoloji Araştırmaları Dergisi*(1).

Yiğit, İ. (2004). *Memlûkler*. Mart 2023 tarihinde TDV İslâm Ansiklopedisi:
<https://islamansiklopedisi.org.tr/memlukler> adresinden alındı