SİMETRİK KRİPTOSİSTEMLERDEN ÇOK ALFABELİ YERİNE KOYMA METODUNUN TÜRKİYE TÜRKÇESİNİN YAPISAL ÖZELLİKLERİNİ KULLANARAK KRİPTANALİTİK İNCELENMESİ

Derya ARDA[1] **Ercan BULUŞ**[2] **Tarık YERLİKAYA**[3]

[1,2,3]Bilgisayar Mühendisliği Bölümü
Mühendislik- Mimarlık Fakültesi
Trakya Üniversitesi, Edirne

[1]e-posta: deryaa@trakya.edu.tr [2] e-posta: ercanb@trakya.edu.tr
[3]e-posta: tarikyer@trakya.edu.tr

Anahtar sözcükler:Vigenere Şifresi, Kasiski Metodu, Rastlantı Dizini, Kriptanaliz, Türkçedeki BazıÖlçütler

ABSTRACT

Vigenere, the most common Poly Alphabetic Substitution Cipher, is still a practical encryption method that can be efficiently used for many applications. In this study, encryption and cryptanalysis of Vigenere cipher are performed in a way based on Turkish alphabet. Firstly, we have determined the identification and classification of cryptosystem used in cryptanalysis process. Secondly, we have employed the structural properties of Turkish and some measurements concerning Turkish through that process. Based on these observation; we have come the conclusion that both the structural properties and some measurements related the language are critical factors in cryptanalysis processes.

1. GİRİŞ

Kriptosistemler, şifreli metin olarak bilinen anlaşılmaz karakterler serisini açık metine dönüşümünü kullanan yazılım ve donanımın karmaşık bir kombinasyonudur. Şifreleme güvenli elektronik haberleşmenin can damarıdır. Ancak bir mesajın güvenliğinin daima baki kalacağı garantili değildir. Bir mesajın bütünlüğü ve güvenilirliği tek yönlü hash fonksiyonunun ve sayısal imzanın kulllanılmasını gerektirir. [1]

İki çeşit kriptosistem vardır. Bunlardan birisi Simetrik diğeri Asimetrik Kriptosistemlerdir. Simetrik Kriptosistemlerde şifreleme ve deşifreleme anahtarları aynıdır. Yani simetrik algoritmalarda tek anahtar kullanılır. Başlıca Simetrik Kriptosistemler; Yerine-koymalı (Substitution), Yer-değiştirmeli (Transposition), Yerine-koymalı ve Yer-değiştirmeli sistemlerin kombinasyonundan oluşan Ürün (Product), Akış (Stream) ve Blok (Block) kriptosistemler olarak sayılabilir [2,3]. Asimetrik Kriptosistemlerde ise şifreleme ve deşifrelemede farklı anahtarlar kullanılır.

Daha önceki çalışmalarımızda Türk alfabesini kullanarak Simetrik Kriptosistemin bir çeşidi olan Çok Alfabeli Yerine-Koyma Metodu ile şifreleme ve kriptanalizi incelemiştik. [4] Bu çalışmada kriptanaliz aşamasında hangi şifreleme tekniğinin kullanıldığı ve hatta hangi dil ile şifreleme yapıldığı hakkında fikir veren kriptosistemin kimliğinin ve sınıfının nasıl belirlenebildiği incelenmiştir. Daha sonra Türkçe'nin yapısal özellikleri baz alınarak kriptanalitik çalışmalar yapılmıştır. Sonuç olarak kriptanalitik incelemeler yapılırken şifreleme alfabesi, kullanılan dilin karakteristik özellikleri ve gramer yapısı önem kazanmıştır.

2. ÇOK ALFABELİ YERİNE KOYMA ŞİFRELERİ

Çok alfabeli yerine koyma şifresinde açık metin harfleri, farklı şekillerde oluşturulmuş olan şifreleme alfabesindeki harflerin yerleştirilmesine bağlı olarak şifrelenirler. Çok alfabeli şifre, bir anahtarla yönetilmiş olan yerine koyma kurallarıyla tek alfabeli şifrelerin bir kombinasyonu gibidir. Çok alfabeli ismi, ima edildiği gibi yalnız bir yerine birkaç şifreleme alfabesi kullanılarak meydana getirilmiştir. Bu metodun en yaygın kullanılan çeşidi Vigenere Şifresidir. [5]

3. VİGENERE ŞİFRESİ VE KRİPTANALİZİ

3.1 Vigenere Şifresi ile Şifreleme ve Deşifreleme

$A=(a_1, a_2,...,a_n)$ n-karakter uzunluğunda bir alfabe, $K=(k_1, k_2,...,k_m)$ m-karakter uzunluğunda bir anahtar ve $M=(m_1, m_2, ..., m_t)$ t-karakter uzunluğunda bir açık metin olsun. Buna göre Vigenere şifresi ile şifrelemeyi şu şekilde tanımlarız.

$$E_K(a_i) = (m_i + k_i \bmod n)$$

Deşifrelemesini ise

$$D_K(c_i) = (c_i - k_i \bmod n)$$

şeklinde tanımlarız.

Vigenere şifresi m adet kaydırma şifresi kullanır. Buradaki her k_i n adet tek alfabeli yerine koyma şifresi kullanılacağını belirler. [6] Vigenere şifresinde bu kurallar çerçevesinde oluşturulmuş bir tablo kullanılır. Bu tablo İngiliz alfabesi için 26' ya 26, Türk alfabesi için 29'a 29 hücreden oluşmuştur. Biz Türk alfabesi ile oluşturulmuş Vigenere tablosunu kullanarak şifreleme ve kriptanaliz üzerinde duracağız.

Tablo 1'de gösterilen Türk alfabesi kullanılarak oluşturulmuş Vigenere tablosuna göre "DOĞA" anahtar kelimesi ile aşağıdaki metini şifreleyelim. En üst satır açık metni, en sol sütun anahtar kelimeyi ve ikisinin kesişimi bize şifreli metni verecektir.

Tablo 1. Türk Alfabesi Kullanılarak Oluşturulmuş Vigenere Tablosu

ABCÇDEFGĞHIİJKLMNOÖPRSŞTUÜVYZ
BCÇDEFGĞHIİJKLMNOÖPRSŞTUÜVYZA
CÇDEFGĞHIİJKLMNOÖPRSŞTUÜVYZAB
ÇDEFGĞHIİJKLMNOÖPRSŞTUÜVYZABC
DEFGĞHIİJKLMNOÖPRSŞTUÜVYZABCÇ
EFGĞHIİJKLMNOÖPRSŞTUÜVYZABCÇD
FGĞHIİJKLMNOÖPRSŞTUÜVYZABCÇDE
GĞHIİJKLMNOÖPRSŞTUÜVYZABCÇDEF
ĞHIİJKLMNOÖPRSŞTUÜVYZABCÇDEFG
HIİJKLMNOÖPRSŞTUÜVYZABCÇDEFGĞ
IİJKLMNOÖPRSŞTUÜVYZABCÇDEFGĞH
İJKLMNOÖPRSŞTUÜVYZABCÇDEFGĞHI
JKLMNOÖPRSŞTUÜVYZABCÇDEFGĞHIİ
KLMNOÖPRSŞTUÜVYZABCÇDEFGĞHIİJ
LMNOÖPRSŞTUÜVYZABCÇDEFGĞHIİJK
MNOÖPRSŞTUÜVYZABCÇDEFGĞHIİJKL
NOÖPRSŞTUÜVYZABCÇDEFGĞHIİJKLM
OÖPRSŞTUÜVYZABCÇDEFGĞHIİJKLMN
ÖPRSŞTUÜVYZABCÇDEFGĞHIİJKLMNO
PRSŞTUÜVYZABCÇDEFGĞHIİJKLMNOÖ
RSŞTUÜVYZABCÇDEFGĞHIİJKLMNOÖP
SŞTUÜVYZABCÇDEFGĞHIİJKLMNOÖPR
ŞTUÜVYZABCÇDEFGĞHIİJKLMNOÖPRS
TUÜVYZABCÇDEFGĞHIİJKLMNOÖPRSŞ
UÜVYZABCÇDEFGĞHIİJKLMNOÖPRSŞT
ÜVYZABCÇDEFGĞHIİJKLMNOÖPRSŞTU
VYZABCÇDEFGĞHIİJKLMNOÖPRSŞTUÜ
YZABCÇDEFGĞHIİJKLMNOÖPRSŞTUÜV
ZABCÇDEFGĞHIİJKLMNOÖPRSŞTUÜVY

Açık Metin

"Bu bölümde simetrik anahtar blok şifreleri için uygulanmış iki güçlü kriptanaliz tekniklerinden biri olan lineer kriptanaliz üzerinde duracağız. Diğer kriptanaliz tekniği de Diferansiyel Kriptanalizdir. Lineer Kriptanaliz DES üzerinde teorik bir saldırı olarak EUROCRYPT 93'te MATSUİ tarafından ortaya çıkarılmış ve sonra DES'in pratik olarak kriptanalizinde başarılı bir şekilde kullanılmıştır."

"DOĞA" anahtar kelimesi ve bu tabloya göre şifrelenmiş metin aşağıda verilmiştir.

Şifreli Metin

"ej höoktdh hpmhizio ouakiğr ecük vzlrhckrm ziir jfgzcğnpyb ioz mügcd kuzytddğlmn ceodpköşzirskn ezzi scğn özuehğ srmgcaroşiç kgeuzudh sçrdpğğln jijşz kuzytddğlmn ceodpğm sk dmtkrddaicşş kuzytddğlmnjiu cpnhşz kuzytddğlmn jeü kgeuzudh ikouzs bmğ aaösöuı eşauos ezğücumyt 93 yş tayhçi yozaıyuddd üryofa gysauyşmlı ee üeurd sks md yrdipk scğrdb srmgcaroşiçzudh öğşdğöll öpr vşsiösk kzcşaryşmlıcıu "

3.2 Vigenere Şifresinin Kriptanalizi

Friedrich Kasiski bu şifreyi kırmak için bir metot geliştirdi. Bu metot anahtar kelimenin uzunluğunu bulmaya yöneliktir. Anahtar uzunluğunu belirlemek için yaygın olarak Kasiski ve Rastlantı Dizini testi kullanılır. [7]

3.1. Kasiski Metodu

Anahtar uzunluğunu bulmak için şifreli metinde tekrarlanmış gruplar arasındaki mesafeyi hesaplamada kullanılan bir metottur. Bu tekrarlar periyodu bulmak için kullanılmıştır. Bulunan periyot tahminini kuvvetlendirmek için Rastlantı Dizini Testi uygulanabilir [8].

3.2. Rastlantı Dizini Testi

Rastlantı Dizini (index of coincidence), karakterler dizgisinden rasgele seçilen iki karakterin birbirinin aynısı olma olasılığıdır.

$f_0, f_1 ... f_{25}$ belirli bir x katarında A,B,C,D,.....,Z'nin frekanslarını ve n metindeki toplam harf sayısını göstermek üzere incelenen bir x katarı için rastlantı dizini aşağıdaki formülle verilir.[7]

$$IC(x) = \frac{\sum_{i=0}^{25} \binom{f_i}{2}}{\binom{n}{2}} = \frac{\sum_{i=0}^{25} f_i(f_i - 1)}{n(n-1)}$$

Anahtar uzunluğu m biliniyorsa IC değeri şu formül ile hesaplanır.

$$IC_E = \frac{S-m}{m(S-1)}(IC(KaynakDil)) + \frac{(m-1)S}{m(S-1)}(IC(RastgeleMetin))$$

S= Şifreli metin uzunluğudur.
IC(KaynakDil)=0.0597 (Türkçe için)
IC(Rastgele Metin)=0.0344 [6].

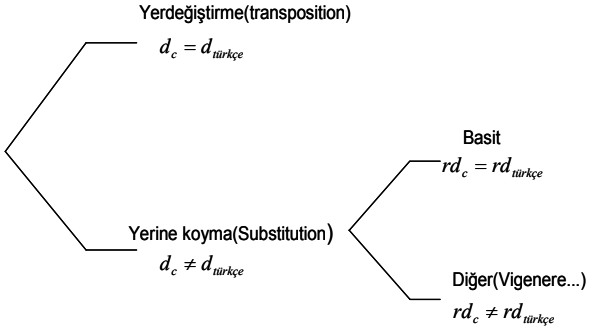
Eğer x, İngilizce metninin bir katarı ise, tahmin edilen IC(X)(index of coincidence) yaklaşık olarak 0.065'tir. Bu değer, İngiliz alfabesindeki harflerin olasılıklarının kullanılması ile hesaplanmıştır. Türkçe bir metin için IC=0,059' dur.[10]

4. SEÇİLMİŞ ŞİFRELİ METİN İÇİN KRİPTANALİZ AŞAMALARI

Biz burada elimizde bulunan sadece şifreli metinden faydalanarak şifreli metini çözmeye çalışacağız. Bunun için öncelikle hangi şifreleme tekniğinin kullanıldığı araştırılacaktır. Daha sonra ise hangi metot ile şifrelendiğinin analizi yapılacaktır. Ayrıca bu analizler sonucunda hangi dile ait alfabe ile şifreleme yapıldığına karar verilecektir.

4.1 Seçilmiş Şifreli Metinde Kullanılan Kriptosistemin Kimliğinin ve Sınıfının Belirlenmesi

Yerine koyma (substitution) şifreleri harflerin frekans dağılımını değiştirirken, yerdeğiştirme (transposition) şifreleri harflerin frekans dağılımını değiştirmezler.



$d_{türkçe}$ = Türkçe harf dağılımları
d_c = Şifreli metin harf dağılımları
$rd_{türkçe}$= Gram $d_{türkçe}$ (tek harfli dağılımı, ikili harf dağılımı gibi) [9]

Yukarıdaki şekilde gösterildiği gibi şifreli metinin harf frekans dağılımı, şifrelemede kullanılmış olan alfabenin harf frekans dağılımına yaklaşık olarak eşitse kullanılan kriptosistemin kimliği yerdeğiştirme şifresidir. Eğer bu dağılım eşit değilse yerine koyma metodu ile şifrelenmiştir.

Kriptosistemin sınıfı belirlenirken rd_c= $rd_{türkçe}$ eşitliğine bakılır. Eğer bu denklem eşitse basit yerine koyma metodu ile şifrelenmiştir. Bu tek alfabeli yerine koyma metodu olabilir. Aksine eşit değilse çok alfabeli yerine koyma metodu olabilir. Buna en yaygın kullanılan örnek olarak Vigenere şifresi ile şifrelenmiştir diyebiliriz. Çünkü tek harf dağılımlarına bakıldığında çok alfabeli yerine koyma metodu rastlantı dizinini değiştiren bir şifreleme metodudur. Tek alfabeli yerine koyma metodu ise rastlantı dizinini değiştirmez.

Kullanılan şifreli metinin dili için;
rd_c= $rd_{türkçe}$ $\Leftrightarrow$ IC=0.059 (Türkçe için rastlantı dizini)
$rd_c \neq rd_{türkçe}$ $\Leftrightarrow$ IC(Rastgele Metin)=0,0344' tür. [9]

Yukarıdaki şifrelenmiş örnekteki harflerin dağılımları ve olasılıkları hesaplanmıştır.

Toplam Harf Sayısı = 341

Harflerin Sıklıklarının Olasılıkları

Oluşumlar	Sıklıkları(Frekans)
A = 12	0.035191
B = 3	0.008798
C = 15	0.043988
Ç = 4	0.011730
D = 27	0.079179
E = 14	0.041056
F = 2	0.005865
G = 7	0.020528
Ğ = 17	0.049853
H = 11	0.032258
I = 5	0.014663
İ= 17	0.049853
J = 6	0.017595
K = 19	0.055718
L = 10	0.029326
M = 16	0.046921
N = 9	0.026393
O = 11	0.032258
Ö = 10	0.029326
P = 8	0.023460
R = 17	0.049853
S = 15	0.043988
Ş = 14	0.041056
T = 8	0.023460
U = 20	0.058651
Ü = 6	0.017595
V = 2	0.005865
Y = 14	0.041056
Z = 22	0.064516

Rastlantı Dizini = 0.041125

Bulunan bu sonuçlara göre şifreli metinde en sık kullanılan ilk beş harf sırasıyla " D, Z, U, K, Ğ-İ" dir. En az kullanılan harfler "F-V, B"dir.

Tablo 2' de Türk Alfabesindeki harflerin frekansları verilmiştir. Bu tabloya göre en sık kullanılan ilk beş harf sırasıyla "A, E, I, L, İ" dir. En az kullanılan harf "J"dir. [3]

Tablo 2 Türk alfabesindeki harflerin kullanım sıklıkları.

Harf	Olasılık(%)	Harf	Olasılık(%)
A	11.68	N	7.23
B	2.95	O	2.45
C	0.97	Ö	0.87
Ç	1.26	P	0.79
D	4.87	R	6.95
E	9.01	S	2.95
F	0.44	Ş	1.94
G	1.34	T	3.09
Ğ	1.13	U	3.43
H	1.14	Ü	1.99
I	8.27	V	0.98
İ	5.20	Y	3.37
J	0.01	Z	1.50
K	4.71		
L	5.75		
M	3.74		

Görüldüğü gibi ele alınan şifreli metinin harf dağılımları değişmiştir. O halde şifrelemede kullanılmış olan kriptosistemin kimliği Yerine Koymalı Şifreleme'dir diyebiliriz. Ayrıca bu şifreli metin için elde edilen rastlantı dizini sonucu IC=0,041125' dir. Elde edilen bu değer IC(Rastgele Metin)=0,0344 yakındır. $rd_c \neq rd_{türkçe} \Leftrightarrow$ IC(Rastgele Metin)=0,0344 idi. Sonuç olarak kullanılmış olan şifreli metinin sınıfı Çok Alfabeli Yerine Koyma Metodu' dur. Aynı şekilde bu metodun en çok kullanılan bir çeşidi olan Vigenere Şifresi bu şifrelemede kullanılmıştır diyebiliriz.

4.2. Türk Alfabesi ve Vigenere Tablosu Kullanılarak Şifrelenmiş Bir Metinin Kriptanalizi

Vigenere kullanılarak şifrelenmiş bir metini çözmek için öncelikle anahtar kelimenin uzunluğunun belirlenmesi gereklidir. Bunun için;

- Kasiski Metodu
- Rastlantı Dizini Testi

kullanılır.

4.2.1. Kasiski Metodu

Daha önce anlatıldığı gibi şifreli metinde birden fazla meydana çıkan üç veya daha uzun karakterler arasındaki mesafeler hesaplanır ve bütün bölenleri bulunur. En fazla meydana çıkan bölen, anahtar uzunluğu olabilir.[6]

Bu metodu şifreli metinimize uyguladığımızda programın sonucu bize aşağıda verileri verir.

Oluşumlar	Kaç kez tekrarladığı
Kuzy	4
Uzyt	4
Zytd	4
Ytdd	4
Tddğ	4
Ddğl	4

Örneğimizde DDĞL kısmı başlangıçtan sonra üç kez tekrarlamıştır. DDĞL için başlangıç pozisyonları, bir önceki ile arasındaki mesafe ve bu mesafeye göre oluşan faktörler tablo 3'te verilmiştir.

Tablo 3. Faktörler

Başlangıç Pozisyonu	Bir önceki ile arasındaki mesafe	Faktörler
65		
137	72	2, 3, 4, 6, 8, 9, 12,18, 24, 36, 72
169	32	2, 4, 8, 16, 32
189	20	2, 4, 5, 10, 20

Yukarıdaki verilere göre en çok meydana gelen 2 ve 4 faktörleri anahtar uzunluğu olabilir.

4.2.2. Rastlantı Dizini Testi

Rastlantı dizini kriptanalizde önemli uygulamalarla beraber aynı zamanda önemli bir dil parametresidir. Rastlantı Dizini (IC(x)) daha önce anlatıldığı gibi, rastgele seçilmiş iki katarın aynı olma olasılığıdır.[10]

4.1.bölümündeki program çıktısında IC=0.041125 değeri aşağıdaki formül kullanılarak hesaplanmıştır.

$$IC(x) = \frac{\sum_{i=0}^{25} \binom{f_i}{2}}{\binom{n}{2}} = \frac{\sum_{i=0}^{25} f_i(f_i - 1)}{n(n-1)}$$

Bulunan bu IC=0.041125 değerinin daha önceden farklı uzunluktaki anahtar değerleri için hesaplanmış olan IC değerleri ile kıyaslandığında m=4 anahtar uzunluğundaki IC değerine yakın olduğu gözlemlenir. m=4 uzunluğundaki IC(Türkçe)=0,0407'dir. [6] O halde incelediğimiz şifreli metin m=4 uzunluğunda bir anahtarla şifrelenmiştir.

5. TÜRKÇE'NİN BAZI ÖLÇÜTLERİNDEN FAYDALANILARAK ANAHTAR KELİMENİN BELİRLENMESİ

Klasik şifrelerin kriptanalizinde anahtar kelime belirlenirken kullanılan dile özgü ikili, üçlü, dörtlü, beşli ve altılı harf gruplarının sıklıkları, rastlantı dizini testi, ilk harf/son harf frekansları ve sesli/sessiz harf grupları gibi bazı karakteristik ölçütlerden ve

ayrıca o dile ait dilbilgisi kurallarından faydalanılabilinir. [10,12]
Şifreli metin IC(x) testinin verilerine göre Türk alfabesi ve Vigenere tablosu kullanılarak oluşturulduğu sonucuna varmıştık. Buna göre anahtar kelime şifreli metin üzerinde ayrıntılı bir gözlem, Türk Dil Bilgisi kuralları ve Türkiye Türkçesi için hesaplanmış ölçütlerden faydalanılarak belirlenmeye çalışılacaktır.

Anahtar uzunluğu 4 olan bir anahtar kelime için $K=(k_0, k_1, k_2, k_3)$ dir. Şifreli metin anahtar uzunluğu kadar alt gruplara bölünür.

Şifreli Metin:

“ej höökdth hpmhizio ouakiğr ecük vzlrhckrm 12 3412341 23412341 2341234 1234 123412341 ziir jfgzcğnpyb ioz mügcd kuzytddğlmn 2341 2341234123 412 34123 41234123412 ceodpköşzirskn ezzi scğn özuehğ srmgcaroşiç 34123412341234 1234 1234 123412 34123412341 kgeuzudh sçrdpğğln jijşz kuzytddğlmn ceodpğm 23412341234123412 34123 41234123412 3412341 sk dmtkrddaicşş kuzytddğlmnjiu cpnhşz 23 412341234123 41234123412341 234123 kuzytddğlmn jeü kgeuzudh ikouzs bmğ aaösöuı 41234123412 341 23412341 234123 412 3412341 eşauos ezğücumyt 93 yş tayhçi yozaıyuddd 234123 412341234 12 341234 1234123412 üryofa gysauyşmlı ee üeurd sks md yrdipk 341234 1234123412 34 12341 234 12 341234 scğrdb srmgcaroşiçzudh öğşdğöll öpr vşsiösk 123412 341234123412341 23412341 234 1234123 kzcşaryşmlıcıu ”
41234123412341

Şifreli metin üzerinde kısa olan n harfli gruplardan çözmeye başlamak işimizi daha kolaylaştıracaktır. Buna göre ;

“93 yş”, “ee” kalıplarını inceleyelim.

“93 yş” kalıbındaki “yş”den önce ayraç kullanılmış olması gereklidir. Çünkü Türkçede sayılardan sonra gelen ekler ayraçla ayrılır. Buna göre 93’yş=93’ ün olabilir, ya da 93’ yş=93’ te olabilir. Türkçede sessiz/sesli kelime modelleri incelendiğinde iki harfli sessiz/sesli kelime modeli %6.730 oranındadır. İki harfli sesli/sessiz kelime modeli ise %1.307 oranındadır [10]. Bu veriler göre “yş=te” olma olasılığı daha fazladır. Şifreli metin anahtar uzunluğu 4 olacak şekilde gruplanmıştı. Burada “yş=12” karşılık gelmektedir. Öyleyse vigenere tablosu yardımı ile bu harflere karşılık gelen anahtar kelimenin harflerini çözersek 12=DO olur. Buna göre şifreli metin üzerinde 12 gelen yere farzedilen DO anahtar kelimesinin harfleri yazılırsa metin şu şekilde olur.

“ej höökdth hpmhizio ouakiğr ecük vzlrhckrm **Do**34**do**34**d** **o**34**do**34**d** **o**34**do**34 **do**34 **do**34**do**34**d** ziir jfgzcğnpyb ioz mügcd kuzytddğlmn **o**34**d** **o**34**do**34**do**3 4**do** 34**do**3 4**do**34**do**34**do** ceodpköşzirskn ezzi scğn özuehğ srmgcaroşiç 34**do**34**do**34**do**34 **do**34 **do**34 **do**34**do** 34**do**34**do**34**d** kgeuzudh sçrdpğğln jijşz kuzytddğlmn ceodpğm **o**34**do**34**d** **o**34**do**34**do** 34**do**3 4**do**34**do**34**do** 34**do**34**d** sk dmtkrddaicşş kuzytddğlmnjiu cpnhşz **o**3 4**do**34**do**34**do**3 4**do**34**do**34**do**34**d** **o**34**do**3 kuzytddğlmn jeü kgeuzudh ikouzs bmğ aaösöuı 4**do**34**do**34**do** 34**d** **o**34**do**34**d** **o**34**do**3 4**do** 34**do**34**d** eşauos ezğücumyt 93 yş tayhçi yozaıyuddd **o**34**do**3 4**do**34**do**34 **do** 34**do**34 **do**34**do**34**do** üryofa gysauyşmlı ee üeurd sks md yrdipk 34**do**34 **do**34**do**34**do** 34 **do**34**d** **o**34 **do** 34**do**34 scğrdb srmgcaroşiçzudh öğşdğöll öpr vşsiösk **do**34**do** 34**do**34**do**34**do**34**d** **o**34**do**34**d** **o**34 **do**34**do**3 kzcşaryşmlıcıu ”
4**do**34**do**34**do**34**d**

Buna göre metni çözersek;

“**bu** hö**l**ü**t**d**e** **s**p**m**e**t**z**i**k **a**u**a**h**t**ğr **bl**ük **ş**i**l**r**el**k**r**i **i**i**i**n **u**f**g**u**l**ğ**n**m**ı**b **i**k**i** müç**l**d k**r**i**y**t**an**ğ**l**i**z** ce**k**n**p**k**l**e**z**i**nd**k**n** **bi**zi **ol**ğn **li**ue**e**r s**r**i**p**c**a**n**a**şi**z** **ü**g**e**r**i**u**d**e** **d**ç**r**a**c**ğğ**ı**z ji**ğ**ez k**r**i**y**t**an**ğ**l**i**z** ce**k**n**p**ğ**i** **d**k di**f**kr**a**n**a**i**y**eş k**r**i**y**t**an**ğ**l**i**z**j**i**r** **l**pn**e**e**z** k**r**i**y**t**an**ğ**l**i**z** je**s** **ü**g**e**r**i**u**d**e** **t**k**o**r**i**s** b**i**r** a**a**l**d**öu**ı** **o**şa**r**a**s** e**u**r**ü**c**r**y**y**t 93 **te** t**a**t**s**çi **t**a**z**a**f**ı**u**d**a**n** ür**t**a**f**a** **çı**sa**rı**şm**ış** ee **so**u**r**a **d**ks **in** y**r**a**t**pk **ol**ğ**r**a**k** s**r**i**p**c**a**n**a**şi**z**i**u**d**e** **b**ğş**a**r**ö**l**ı** **b**pr **ş**e**s**i**l**d**k** k**u**l**ş**a**n**ı**ş**m**ış**ç**ı**r ”

Gerçektende “12” yerine “DO” anahtar kelime parçasını yazdığımızda bir kaç yerde anlamlı kelimeler ve takılar göze çarpmaktadır. Mesela “**D**ks **in**” kalıbında “in” iki harfli grubunun “Dks’ den ayraçla ayrılan bir çekim eki olması gerekir. Çünkü Türkçede böyle iki harfli bir kelime yoktur. Aynı zamanda “in” Türkçede en sık kullanılan iki harfli gruplardan biridir. Ancak ayraç söz konusu olduğunda Türkçe bir metin için bu yapı uygundur. Ayrıca şifreli metin bu şekilde çözümlendiğinde ilk kelimenin “**Bu”** kelimesi olduğu gözükmektedir. “Bu” kelimesi Türkçede en sık kullanılan ilk yirmi kelimeden biridir [10]. Buna ilaveten “**ş**i**l**r**el**k**ri”** kelimesinde son dört harfle baktığımızda “**l**k**ri**” tetragramının, en çok kullanılan tetragramlardan biri olan “leri” olabileceğini tahmin edebiliriz [10].

Yarı çözülmüş bu şifreli metini yeniden incelediğimizde “**d**k=de veya **d**k=da” olabilir. Çünkü “de da” Türkçede en sık kullanılan ilk yirmi kelimelerden ikisidir. En sık kullanılan ilk harf/son harf frekansına bakılırsa ilk harf olarak kullanılmış olan “D” harfi %9.0 bir oranla ikinci sıradadır. En sık kullanılan son harf %15.2 sıklıkla “N” harfidir. Bunu %12.4 sıklıkla “E” harfi, %11.7 sıklıkla “A” harfi takip etmektedir [10]. Bu verilere göre “**d**k” kelimesindeki “k” harfinin “e” olma olasılığı daha yüksektir. Buna göre “k” harfi vigenere tablosuna

göre “ğ” anahtar harfi ile deşifrelenirse “e” meydana gelir. Şifreli metinde “**d**k=23” karşılık gelmektedir. O halde “3=ğ” dir. Yine şifreli metindeki “ee” bağlacı “34” sayılarına denk gelir. Bunu da bu şekilde çözümlersek “ee=34=ğ4=v4” olur. Burada “v4” kelimesinin Türkçede en sık kullanılan ilk yirmi kelime arasından iki harfli “v” harfi ile başlayan “ve” kelimesi olabileceğini, aynı zamanda son harf frekansına baktığımızda bunun %.12.4 sıklıkla ikinci sırada yer alan “e” harfi olabileceğini tahmin edebiliriz [10]. Vigenere tablosuna göre “ve” bağlacındaki “e” açık metin harfi “e” şifreli metin harfini “a” anahtar harfi ile oluşturabilir. Böylece “4” yerine “a” anahtar harfini kullanırız. Bu verilere göre anahtar kelimeyi daha düzgün bir şekilde aşağıdaki tabloda gösterelim.

Şifreli Metin	Y	Ş	E	E
Anahtar Uzunluğu	1	2	3	4
Açık Metin	D	E	V	E
Anahtar Kelime	D	O	Ğ	A

Şimdi bulunan anahtar kelimeye göre metni deşifrelersek aşağıdaki metini elde ederiz.

“bu bölümde simetrik-anahtar blok şifreleri için uygulanmış iki güçlü kriptanaliz tekniklerinden biri olan lineer kriptanaliz üzerinde duracağız diğer kriptanaliz tekniği de diferansiyel kriptanalizdir lineer kriptanaliz des üzerinde teorik bir saldırı olarak eurocrypt 93 te matsui tarafından ortaya çıkarılmış ve sonra des in pratik olarak kriptanalizinde başarılı bir şekilde kullanılmıştır ”

SONUÇ

Klasik şifrelerin kriptanalizinde şifrelemede kullanılan dilin bilinmesi çok önemlidir. Çünkü çözümleme aşamalarında o dilin frekans analizleri, ikili, üçlü, dörtlü, beşli ve altılı harf gruplarının sıklıkları, rastlantı dizini sonucu, ilk harf/son harf frekansları ve sesli/sessiz harf grupları gibi bazı karakteristik ölçütler ve ayrıca dile ait dilbilgisi kurallarından faydalanılır.

KAYNAKLAR

[1] Zwicke A. , “An Introduction to Modern Cryptosystems”, SANS Intitute 2003, http://www.giac.org/practical/GSEC/Andrew-Zwicke.GSEC.pdf

[2] Koltuksuz A. , Kriptografide Son Gelişmeler: Kuantum Kriptografi, 1. Sistem Mühendisliği ve Savunma Uygulamaları Sempozyumu, Ekim 1995, Ankara.

[3] Arda D. , Buluş E. , "Türk Alfabesi ve Yapısal Özellikleri Kullanılarak Tek Alfabeli Yerine Koymada Şifreleme ve Kriptanaliz", 20. Türkiye Bilişim Kurultayı, İstanbul, 2003.

[4] Arda D. , Buluş E. , Yerlikaya T. ,”Türkiye Türkçesi’ nin Bazı Dil Karakteristik Ölçütlerini Kullanarak Vigenere Şifresi ile Şifreleme ve Kriptanaliz” ELECO’2004 Elektrik-Elektronik-Bilgisayar Mühendisliği Sempozyumu ve Fuarı, Bursa, 2004.

[5] Polyalphabetic Substitution, http://hem.passagen.se/ten01/poly.htm/

[6] Dalkılıç M. , Güngör C. , “An Interactive Cryptanalysis Algorithm for the Vigenere Cipher”, Ege University, International Computer Institute, İzmir.

[7] Wıacek M, Knappenberger J, Basic Cryptography, La Salle University.

[8] CS442-Cryptography Techniques,2000 www.cs.uidaho.edu/~jimaf/cs442/lectures/crypto2.htm/

[9] Cryptography 2004, http://www.cs.chalmers.se/Cs/Grundutb/Kurser/Krypto/lect02_4.pdf

[10] Dalkılıç M.E. ., Dalkılıç G. , “Some Measurable Language Characteristics of Printed Turkish”, Proc. Of the XVI. İnternational Symposium on Computer and Inf.Sciences, pp.217-224,2001.

[11] Dalkılıç G. , Çebi Y. , “Türkçe Külliyat Oluşturulması ve Türkçe Metinlerde Kullanılan Kelimelerin Uzunluk Dağılımlarının Belirlenmesi”, DEÜ Mühendislik Fakültesi Fen ve Mühendislik Dergisi,Cilt:5, Sayı:1 sh.1-7, Ocak 2003

[12] Koltuksuz A. , “ Simetrik Kriptosistemler için Türkiye Türkçesinin Kriptanalitik Ölçütleri ve Ulusal Kriptolojik Standart Geliştirimi”, 1. Sistem Mühendisliği ve Savunma Uygulamaları Sempozyumu, Ekim 1995, Ankara.