TÜRKİYE TÜRKÇESİNİN BAZI DİL KARAKTERİSTİK ÖLÇÜTLERİNİ KULLANARAK VİGENERE ŞİFRESİ İLE ŞİFRELEME VE KRİPTANALİZ

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

In this study, an aspect of encryption is investigated by using the Poly Alphabetic Substitution Method in particular Vigenere cipher and Turkish Alphabet. In addition, cryptanalysis is performed on encrypted sample text. Structural properties of Turkish language and some measurable characteristics used in Turkish language such as letter, digram, trigram, tetragram, pentagram and hexagram frequencies, index of coincidence, word length, first letter/last letter frequencies, and consonant/vowel, are used for cryptanalysis. It is concluded that the cryptanalysis processes depends on the language used in the encryption.

1. GİRİŞ

M.Ö. 400 yıllarından başlayarak 1976 yılına kadar geçen yaklaşık 2500 yıllık bir süreçte; şifreleme ve deşifreleme işlemlerinde aynı anahtarın kullanıldığı Simetrik Kriptosistemler kullanılmıştır. 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 [1,2].

Bu çalışmada Simetrik Kriptosistemin bir çeşidi olan Yerine-Koyma Metotlarından Vigenere şifresi (Çok Alfabeli Yerine-Koyma Metodu) incelenmiş ve Türk alfabesi kullanılarak bu metot ile şifreleme ve kriptanaliz üzerinde çalışılmıştır. Daha önceden İngiliz alfabesi kullanılarak yapılmış olan şifreleme ve kriptanaliz çalışmaları incelenip Türkiye Türkçesi ile karşılaştırıldığında yapılan şifrelemenin ve kriptanaliz işlemlerinin kullanılan dile bağlı olduğu sonucuna varılmıştır.

2. VİGENERE ŞİFRESİ İLE ŞİFRELEME VE DEŞİFRELEME

En yaygın çok alfabeli yerine koyma şifresi Vigenere' dir. Bu şifreleme yönteminde 26' ya 26 hücreden oluşan tablo 1' in İngiliz alfabesindeki harflere göre düzenlenmiş hali kullanır [3]. Bu tablo kullanılarak yapılan şifreleme işleminde açık metin harfleri tablonun en üst satırında, anahtar harfler de tablonun en sol sütununda aranır. Açık metin harflerine karşılık gelen anahtar kelimenin harflerinin kesişmesi ile şifreli metine ulaşılır. Örnek olarak CIPHER anahtar kelimesini kullanarak şifreleme işlemini gerçekleştirelim.

Açık Metin: DONT TELL ANYONE
Anahtar: CIPH ERCI PHER CI
Şifreli metin: FWCA XVNT PUCFPM

Açık metin harflerini ilk satırdan anahtar kelimenin harflerine ait alfabeyi de sol sütundan çıkartalım.

A-> ABCDEFGHIJKLMNOPQRSTUVWXYZ
C-> CDEFGHIJKLMNOPQRSTUVWXYZAB
I-> IJKLMNOPQRSTUVWXYZABCDEFGH
P-> PQRSTUVWXYZABCDEFGHIJKLMNO
H-> HIJKLMNOPQRSTUVWXYZABCDEFG
E-> EFGHIJKLMNOPQRSTUVWXYZABCD
R-> RSTUVWXYZABCDEFGHIJKLMNOPQ

Açık metindeki 'D' , C alfabesini kullanarak 'F' ile, 'O' , I alfabesini kullanarak W ile gösterilmiştir.

Deşifrelemede ise şifrelemedeki işlemin tersine şifreli metindeki harfler anahtar kelimenin harfleri ile kesiştirilip açık metine ulaşılır.

3. VİGENERE ŞİFRESİNİN KRİPTANALİZİ

Friedrich Kasiski bu şifreyi kırmak için bir metot geliştirdi. Bu metot anahtar kelimenin uzunluğunu bulmaya yöneliktir. Anahtar uzunluğunu belirlemek için yaygın olarak kullanılan Kasiski ve Rastlantı Dizini testi kullanılmıştır [4].

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 [5].

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' de alfabedeki harf sayısını göstermek üzere incelenen bir x katarı için rastlantı dizini aşağıdaki formülle verilir.

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

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 [4].

4. TÜRK ALFABESİ KULLANILARAK OLUŞTURULMUŞ VİGENERE TABLOSUNA GÖRE ŞİFRELEME

Türk alfabesinde 29 harf vardır. Buna göre Vigenere tablosu 29'a 29 hücreden oluşacaktır. Tablo 1'de gösterilen Türk alfabesi kullanılarak oluşturulmuş Vigenere tablosuna göre "DOĞA" anahtar kelimesini kullanarak aşağıdaki metini şifreleyelim. En üst satır açık metni, en sol sütun anahtar kelimeyi ve ikisinin kesişimi bize şifreli metni verecektir.

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."

Şimdi "DOĞA" anahtar kelimesini açık metnin altına harf harf yerleştirip metni şifreleyelim.

"Bu bölümde simetrik anahtar blok şifreleri **Do ğadoğad oğadoğad oğadoğa doğa doğadoğad** için uygulanmış iki güçlü kriptanaliz **oğad oğadoğadoğ ado ğadoğ adoğadoğado** tekniklerinden biri olan lineer kriptanaliz **ğadoğadoğadoğa doğa doğa doğado ğadoğadoğad** üzerinde duracağız. Diğer kriptanaliz tekniği **oğadoğad oğadoğado ğadoğ adoğadoğado ğadoğad** de Diferansiyel Kriptanalizdir. Lineer **oğ adoğadoğadoğ adoğadoğadoğad oğadoğ** Kriptanaliz DES üzerinde teorik bir saldırı **adoğadoğado ğad oğadoğad oğadoğ ado ğadoğad** olarak eurocrypt 93'te matsui tarafından or **oğadoğ adoğadoğa do ğadoğa doğadoğado ğa** taya çıkarılmış ve sonra DES'in pratik **doğa doğadoğado ğa doğad oğa do ğadoğa** olarak kriptanalizinde başarılı bir şekilde **doğado ğadoğadoğadoğad oğadoğad oğa doğadoğ** kullanılmıştır.
adoğadoğadoğad"

Şifreli Metin

"ej hööktdh 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 "

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
ÖPRSŞTUÜVYZABCÇDEFGĞHIİJKLMN O
PRSŞTUÜVYZABCÇDEFGĞHIİJKLMN OÖ
RSŞTUÜVYZABCÇDEFGĞHIİJKLMN OÖP
SŞTUÜVYZABCÇDEFGĞHIİJKLMN OÖPR
ŞTUÜVYZABCÇDEFGĞHIİJKLMN OÖPRS
TUÜVYZABCÇDEFGĞHIİJKLMN OÖPRSŞ
UÜVYZABCÇDEFGĞHIİJKLMN OÖPRSŞT
ÜVYZABCÇDEFGĞHIİJKLMN OÖPRSŞTU
VYZABCÇDEFGĞHIİJKLMN OÖPRSŞTUÜ
YZABCÇDEFGĞHIİJKLMN OÖPRSŞTUÜV
ZABCÇDEFGĞHIİJKLMN OÖPRSŞTUÜVY

5. TÜRK ALFABESİ İLE OLUŞTURULMUŞ VİGENERE TABLOSU KULLANILARAK ŞİFRELENMİŞ BİR METİNİN KRİPTANALİZİ

Vigenere kullanılarak şifrelenen Türkçe bir metnin kriptanalizi için önce anahtar kelimenin uzunluğunun belirlenmesi gereklidir. Anahtar kelimenin uzunluğunu bulmak için Kasiski Metodu ve Rastlantı Dizini metotları kullanılır. Daha sonra uygun bir anahtar kelime belirlenmeye çalışılır.

5.1. Kasiski Metodu

Kasiski testi gözleme dayanmaktadır. Şifreli metinde birden fazla meydana çıkan üç veya daha uzun karakterden oluşan oluşumların açık metinle ilişkisi olduğu görülür. Bu oluşumlar arasındaki mesafeler hesaplanır ve daha sonra bu mesafelerin bütün bölenleri bulunur. En fazla meydana çıkan bölen, anahtar uzunluğu yada diğer bir deyimle periyod hakkında bilgi verir [6].

Kasiski metodu bu metin üzerine uygulandığında ve C dilinde yazılmış bir program yardımı ile bu metindeki tekrarlar ile bu tekrarlar arasındaki mesafeler hesaplandığında aşağıdaki sonuçlar elde edilir.

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

Örneğimizde UZYT kısmı başlangıçtan sonra üç kez tekrarlamıştır. UZYT için başlangıç pozisyonları, bir önceki ile arasındaki mesafe ve bu mesafeye göre oluşan faktörler tablo 2'te verilmiştir.

Tablo 2. Faktörler

Başlangıç Pozisyonu	Bir önceki ile arasındaki mesafe	Faktörler
61		
133	72	2, 3, 4, 6, 8, 9, 12,18, 24, 36, 72
165	32	2, 4, 8, 16, 32
185	20	2, 4, 5, 10, 20

Yukarıdaki verilere göre en çok meydana gelen 2 ve 4 faktörleri anahtar uzunluğumuz (periyod) olabilir. Daha sonra seçilen her hangi bir anahtar uzunluğunun doğruluğunu desteklemek için Rastlantı Dizini (IC) testi yapılır.

5.2. 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. Tek harf dağılımlarından İngilizce için 0.077, Türkçe için 0.063 Rastlantı Dizini değeri elde edilmiştir. Kriptografide yalnız tek harfli dağılımlar(boşluk karakteri hariç) için IC değerinin bilinmesi çok önemlidir. Türkçe bir metin için IC=0.059, İngilizce bir metin için IC=0.065'tir [7].

Bu şifreli metin için anahtar uzunluğunu 4 kabul edelim. Tahmin edilen IC_E değeri *m* anahtar uzunluklu bir şifre için aşağıdaki formülle hesaplanır [6].

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

S= Şifreli metin uzunluğudur.
IC(KaynakDil)=0.0597 (Türkçe için)
IC(Rastgele Metin)=0.0344 (1/n formülünden hesaplanıyor. n, kullanılan alfabedeki harflerin sayısıdır. Bu değer Türkçe için 1/29 =0.0344'tür)[6].

Şifreli metinimizdeki toplam harf sayısı 341'dir. Tahmin edilen m=4 anahtar uzunluğu için IC(e) değeri yukarıdaki formül yardımıyla hesaplandığında;

$$IC_E = \frac{341-4}{4*(341-1)}0{,}0597 + \frac{(4-1)341}{4(341-1)}0{,}0344 = 0{,}04066$$

dır.

Daha önceden m=4 için hesaplanmış olan IC(Türkçe)=0,0407' dir [6]. Bizim hesapladığımız IC(E) değeri bu değerin sadece 0.0004 altındadır. Yani tahmin edilen m=4 anahtar uzunluğu doğrudur. O halde bu metinin Türk dili ile yazıldığını ve anahtar uzunluğunun bu şifreli metin için 4 olduğunu kabul edebiliriz. Ayrıca şifreli metinin Rastlantı Dizininin sonucuna göre bu metinin hangi şifreleme algoritması ile şifrelendiğine de karar verebiliriz [4]. Örneğimizdeki periyodunu tahmin ettiğimiz şifreli metinin Rastlantı Dizini sonucu 0,04066' dır. O halde bu metin çok alfabeli yerine koyma metodu ile şifrelenmiştir. Çünkü çok alfabeli yerine koyma ile şifrelenen metinin rastlantı dizini Türkçe için IC(Rastgele Metin)=0,0344' e daha yakın olur. Nedeni ise bu metot rastlantı dizinini değiştiren bir metottur [4]. Aksine tek alfabeli yerine koyma metodu ile şifrelenseydi 0,059'a yakın olacaktı. Biz bu metinin kolaylık olması açısından Vigenere ile şifrelendiğini kabul edip anahtar kelimeyi belirlemeye çalışalım.

6. ANAHTAR KELİMENİN BELİRLENMESİ

Klasik şifrelerin kriptanalizinde anahtar kelime belirlenirken o dilin harf, digram(ikili harf grubu), trigram, tetragram, pentagram ve hexagram sıklıkları, rastlantı dizini testi, kelime uzunluğu, ilk harf/son harf frekansları ve sesli/sessiz harf grupları gibi bazı karakteristik ölçütlerinden faydalanılabilinir [7,9].

6.1. Kriptanalitik Çalışmalar

IC(x) testinin sonucuna göre şifreli metinin Türk alfabesi ile yazıldığı gösterilmişti. Ayrıca kelime uzunluğu ortalamalarına da bakılırsa kullandığımız şifreli metin için kelime uzunluk ortalaması 5.57'dir. Türkçe için kelime uzunluk ortalaması 6.13'tür. İngilizce için bu ortalama 4.42'dir [7]. O halde bu ortalamalara göre de üzerinde çalıştığımız şifreli metin Türk alfabesi kullanılarak oluşturulmuştur. Kelime uzunluk dağılımlarındaki sıralamalara bakıldığında da Türkçe bir metin için daha önceden hesaplanmış uzunluk sıralamalarına uygun olduğu gözlemlenmiştir [8]. Örneğin bu şifreli metinde 2 harfli kelime 3 adet, 3 harfli kelime 4 adet, 4 harfli kelime 4 adet, 5 harfli kelime 3 adet, 6 harfli kelime 8 adet, 7 harfli kelime 5 adet ve 10 harfli kelime 3 adet ve bundan daha uzun olan kelimelerin sayısı giderek azalmaktadır. 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 höötdh 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 412341234123412341 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 [7]. 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 höötdh 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**lü**t**d**e **s**pm**e**t**z**i**k** **a**ua**ht**ğr **bl**ük **şi**l**rel**k**ri** i**i**i**n** **u**f**gul**ğ**nmı**b i**ki** müç**l**d k**ri**yt**anğliz** ce**k**n**p**k**le**zi**nd**k**n** **bi**zi **ol**ğn **li**ue**er** s**ripcanaşiz** **üger**i**ud**e **dçracğğız** ji**ğ**ez k**ri**yt**anğliz** ce**k**n**p**ğ**i** **d**k **dif**k**ran**ai**yeş** k**ri**yt**anğlizjir** **l**pn**ee**z k**ri**yt**anğliz** je**s** **üger**i**ud**e **t**ko**ri**s b**ir** a**ald**öu**ı** **oşara**s **eurücryyt** 93 **te** t**atsçi** **ta**z**afı**u**dan** ür**ta**fa **çısarışmış** ee **so**u**ra** **d**ks **in** yr**at**pk **olğrak** s**ripcanaşiud**e **bğşar**öl**ı** **b**pr **şesild**k k**ulşanışmışcır** "

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 [7]. Buna ilaveten “**şi**l**rel**k**ri”** kelimesinde son dört harfle baktığımızda “**lkri**” tetragramının, en çok kullanılan tetragramlardan biri olan “leri” olabileceğini tahmin edebiliriz [7].

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 [7]. 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 [7]. 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 ”

Deşifrelenen metin anlamlı bir şekilde çözülmüştür.

SONUÇ

Kriptanaliz çalışmaları esnasında şifreli metin üzerinde incelemeler yapılırken kullanılan dile özgü ikili, üçlü, dörtlü, beşli ve altılı harf gruplarının sıklıkları, rastlantı dizini testi, kelime uzunluğu, ilk harf/son harf frekansları ve sesli/sessiz harf grupları gibi bazı karakteristik ölçütlerden ve ayrıca o dile ait dilbilgisi kurallarından faydalanılabilinir. Buna dayanarak Çok alfabeli yerine koyma metodu olan Vigenere tablosuna göre yapılan şifreleme ve kriptanaliz işlemlerinin kullanılan dile bağlı olduğu sonucuna varılmıştır.

KAYNAKLAR

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

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

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

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

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

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

[7] 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.

[8] 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

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