Tanım 2.4. $R \neq \varnothing$ kümesi üzerinde tanımlı ikili işlem ve + ve $\sqcup$ olsun. Aşağıdaki aksiyomları sağlayan (R,+, $\sqcup$) cebirsel yapısına bir ***halka*** denir.

H1: (R,+) bir değişmeli gruptur.

H2: $\sqcup$ işleminin R de birleşme özelliği vardır.

H3: $\sqcup$ işleminin + işlemi üzerinde sağdan ve soldan dağılma özelliği vardır. $\forall a,b,c \in R$ için a(b+c)=ab+ac ve (a+b)c=ac+bc dir.

Bölüm 3

KLASİK ŞİFRELEMELER

Düşmanlar tarafından anlaşılmayacak mesaj metotları tarih boyu önemini korudu. Bu bölümde bilgisayar kullanılmadan önceki başlıca eski şifreleme sistemlerini incelenecektir. Bu şifreleme sistemleri bugün kullanılanlardan, özellikle bilgisayardaki düzenlemelerden yoksundur, fakat onlar birkaç önemli şifrelemeye örnektirler.

- Açık metin küçük harfle, şifreli metin ise büyük harfle verilecektir.
- Harflere sırayla sayılar atanır.

İngilizce metinler için harfler şu şekilde numaralandırılır.

a	b	c	d	e	f	g	h	i
0	1	2	3	4	5	6	7	8
j	k	l	m	n	o	p	q	r
9	10	11	12	13	14	15	16	17
s	t	u	v	w	x	y	z	
18	19	20	21	22	23	24	25	

…(1)

a=0 ile başlayıp z= 25 ile numaralanır, çünkü burada modüler aritmetik uygulanacağından dolayı ve İngilizce metinler için mod26 kullanılacağından a=0 ve z=25 olarak alınır.

- Boşluklar ve noktalama işaretleri atılır. Şifreyi çözdükten sonra her zaman boşlukları şifresiz metne koymak mümkündür. Eğer boşluk solda ise, iki seçenek vardır bu durumda mesaj daha fazla bilgi içerdiğinden çözümü daha da kolaylaşır.

Not: Bu bölümde, sayılar teorisi ile ilgili bazı kavramlar kullanılacaktır. Özellikle de modüler aritmetik kullanılacaktır.

3.1 ÖTELEME ŞİFRELEMESİ

Tanım 3.1. $\mathbf{Z}_m$ sınıflar arası toplama ve çıkarma işlemine göre bir halka olduğu bilindiğinden dolayı $0 \le K \le 25$ için y= χ +K (mod 26) şeklinde şifreleme fonksiyonu alınabilir. Bu fonksiyona **öteleme fonksiyonu** denir. Bu şekilde yapılan şifrelemeye **öteleme şifrelemesi** denir. İlk şifreleme sistemi Julius Cesar a aittir. Cesar K=3 alarak şifreleme yapmıştır. Cesar'ın göndermek istediği metin şu olsun.

gaul is divided into three parts
(galya üç bölüme ayrılır)

Fakat bunu Brutus un okumasını istemiyor. Her bir harfe üç öteleme uyguluyor. Böylece $a \to D$, $b \to E$, $c \to F$ gibi şifrelenirler. Son harften sonra başa döner. Yani $x \to A$, $y \to B$, $z \to C$ olur.

Harfler (1) deki gibi 0 dan 25 e kadar tamsayılarla sınıflandırılsın. K $0 \le K \le 25$ olarak tanımlanır. Burada K anahtar yada öteleme miktarıdır. Şifreleme yöntemi;

$$y \equiv \chi + K \pmod{26}$$

Açık metin bu kuralla şifrelenirse;

$g \to 6 \quad \to 6 + 3 \equiv 9 \pmod{26} \qquad 9 \to J$

$a \to 0 \quad \to 0 + 3 \equiv 3 \pmod{26} \qquad 3 \to D$

$u \to 20 \quad \to 20+3 \equiv 23 \pmod{26} \qquad 23 \to X$

$l \to 11 \quad \to 11+3 \equiv 14 \pmod{26} \qquad 14 \to O$

$i \to 8 \quad \to \ 8+3 \equiv 11 \pmod{26} \qquad 11 \to L$

$s \to 18 \ \to 18+3 \equiv 21 \pmod{26} \qquad 21 \to V$

$d \to 3 \quad \to \ 3+3 \equiv 6 \pmod{26} \qquad 6 \to G$

$e \to 4 \quad \to \ 4+3 \equiv 7 \pmod{26} \qquad 7 \to H$

$n \to 13 \ \to 13+3 \equiv 16 \pmod{26} \qquad 16 \to Q$

$t \to 19 \ \to 19+3 \equiv 22 \pmod{26} \qquad 22 \to W$

$o \to 14 \ \to 14+3 \equiv 17 \pmod{26} \qquad 17 \to R$

$h \to 7 \quad \to \ 7+3 \equiv 10 \pmod{26} \qquad 10 \to K$

$r \to 17 \ \to 17+3 \equiv 20 \pmod{26} \qquad 20 \to U$

$p \to 15 \ \to 15+3 \equiv 18 \pmod{26} \qquad 18 \to S$

JDXOLVGLYLGHGLQWRWKUHHSDUWV

elde edilir.

Şifre çözümü ise 3 harf geri gelinerek çözülür. Yani $A \to x$, $B \to y$, $C \to z$ gibi şifre çözülür. Yani;

$\chi \to y - K \pmod{26}$ dır.

JDXOLVGLYLGHGLQWRWKUHHSDUWV

Bu metni çözerken yukarıdaki çözücü fonksiyonda K=3 alınırsa;

gaul is divided into three parts

açık metnini elde ederiz. Şifreyi kırmak için 4 yöntem incelenir:

1) Sadece Şifreli Metin: Melih sadece şifreli metne sahiptir. Anahtar için 26 ihtimal vardır. Başka şifreleme metodunda ise mesaj çok uzunsa değişik harflerin bulunma sıklıkları incelenir. İngilizce metinlerde e harfinin görünme sıklığı en fazladır. L harfi şifreli metinde daha fazla görülsün e=4 ve L=11 olduğundan anahtar tahmin edilebilir. K=11–4 =7 dir.

2) Bilinen Açık Metin: Eğer sadece açık metinde şifreli metindeki bir harfe karşılık gelen bir harf biliniyorsa, anahtarı bulunabilir. Örneğin; Eğer t(=9) şifreli karşılığı D(=3) olsun, dolayısıyla anahtar $K \equiv 3\text{-}19 \equiv \text{-}16 \equiv 10 \pmod{26}$ dır.

3) Seçili Metin: Açık metinde a harfi seçilsin. Şifreli metin anahtarı verir. Örneğin; eğer şifreli metinde a harfine karşılık gelen harf H ise anahtar 7 dir.($K \equiv 0+7 \equiv 7 \pmod{26}$)

4) Seçili Şifreli Metin: Şifreli metinde A harfi seçilsin. Örneğin; Eğer açık metinde A harfine karşılık gelen harf h ise anahtar 19 olur.($K \equiv 0-7 \equiv -7 \equiv 19 \pmod{26}$)

Örnek: "sakarya university" kelimesini 3 öteleme yaparak şifreleyiniz ve şifreli metni açık metne çeviriniz. C++ da İngilizce harflere göre şifreleyip, şifreyi açık metne dönüştüren program yapınız. Ve bu kelimeye tüm 26 öteleme durumunu uygulanarak Maple9.0 da şifrelenişlerini elde ediniz.

Çözüm: Bu durumda $y= \chi+3 \pmod{26}$ ve $\chi= y-3 \pmod{26}$ şeklinde olur. (1) deki veriler yardımıyla;

$s \to 18 \to 18+3=21$	$21 \to V$
$a \to 0 \to 0+3=3$	$3 \to D$
$k \to 10 \to 10+3=13$	$13 \to N$
$r \to 17 \to 17+3=20$	$20 \to U$
$y \to 24 \to 24+3=27 \equiv 1 \pmod{26}$	$1 \to B$
$u \to 20 \to 20+3=23$	$23 \to X$
$n \to 13 \to 13+3=16$	$16 \to Q$
$i \to 8 \to 8+3=11$	$11 \to L$
$v \to 21 \to 21+3=24$	$24 \to Y$
$e \to 4 \to 4+3=7$	$7 \to H$
$t \to 19 \to 19+3=22$	$22 \to W$

Sakarya university

18 0 10 0 17 24 0 / 20 13 8 21 4 14 18 8 19 24

21 3 13 3 20 1 3 / 23 16 11 24 7 17 21 11 22 1

VDNDUBD XQLYHUVLWB

Bulunan şifreli metinde uygun anahtarı deneyerek bulmak suretiyle deşifre yapılsın.

K=1 ise $\chi= y-1 \pmod{26}$ den;

$V \to 21 \to 21-1=20$	$20 \to u$
$D \to 3 \to 3-1=2$	$2 \to c$

$N \rightarrow 13 \rightarrow 13-1=12$ $12 \rightarrow m$

$U \rightarrow 20 \rightarrow 20-1=19$ $19 \rightarrow t$

$B \rightarrow 1 \rightarrow 1-1=0$ $0 \rightarrow a$

$X \rightarrow 23 \rightarrow 23-1=22$ $22 \rightarrow w$

$Q \rightarrow 16 \rightarrow 16-1=15$ $15 \rightarrow p$

$L \rightarrow 11 \rightarrow 11-1=10$ $10 \rightarrow k$

$Y \rightarrow 24 \rightarrow 24-1=23$ $23 \rightarrow x$

$H \rightarrow 7 \rightarrow 7-1=6$ $6 \rightarrow g$

$W \rightarrow 22 \rightarrow 22-1=21$ $21 \rightarrow v$

Buradan açık metin;

“ucmctac wpkxgtukva” olarak elde edilir. O halde K=1 alınması uygun olmaz benzer şekilde K=2 için;

“tblbszb vojwfstjuz” olarak elde edilir. O halde K=2 olması da uygun olmaz. K=3 için ise

“Sakarya university” elde edilir o halde K=3 olur.

Sonuç: Böylece öteleme şifresinde şifreli metin deşifre edilirken K anahtarı deneme yanılma yöntemiyle tespit edilir.

C++

```
#include <iostream>
#include <string>
#include <wchar.h>
using namespace std;
int main()
{
	string str,newStr;
	int otelemeNum,len,flag;

	cout<<"Oteleme Sayisini Giriniz..\n";
	cin>>otelemeNum;

	cout<<"Sifreleme yapmak icin 1, Sifreyi cozmek icin 2 yazin.."<<endl;
```

3.2 AFİN ŞİFRELEMESİ

Öteleme şifresi biraz daha genelleştirilirse, α, β iki tamsayı ve ebob(α,26)=1 olup fonksiyon;

$$y \rightarrow \alpha x + \beta \pmod{26}$$

şeklinde tanımlanır. Bu fonksiyona ***afin fonksiyon*** denir. (α=1 hali öteleme şifresidir.) Afin fonksiyon ile şifrelenmiş metni deşifre ederken kullanılan $\alpha^{*}y - \alpha^{*}\beta \pmod{26}$ denklemine ***çözücü çekirdek*** denir.

Örneğin; α=9 ve β=2 alalım. Böylece fonksiyon; 9x + 2 olur. Açık metinde h(=7) harfini alınsın. Şifreli metinde h harfine karşılık gelen harf;

$$9*7+2 \equiv 65 \equiv 13 \pmod{26}$$

(1) den N(=13) olsun.

$$affine \rightarrow \text{CVVWPM}$$

olarak elde edilir.

Nasıl deşifre yapılır? y=9x+2 nin çözümü: $x=9^{-1}(y-2)$ dir. Ama mod 26 ile çalışıldığından dolayı 9^{-1} in yeniden düzenlenmesi gerekir. ebob(9,26)=1 olduğundan, 9^{-1} (9 un çarpmaya göre tersi) vardır. Öklid algoritması kullanılarak 9^{-1} i (9 un çarpmaya göre tersi) hesaplanabilir.

(9,26)=1 $\Rightarrow$ 9x + 26y = 1

26 = 9*2 + 8

9 = 8*1 + 1

8 = 1*8 + 0

1 = 9 – 8*1

1 = 9 – (26 – 9*2)

1 = 9* (3) + (-1) *26 $\Rightarrow$ x = 3 olarak bulunur.

9*3 ≡ 1 (mod 26) dır. Ve 3 sayısı 9 un mod 26 da çarpmaya göre tersidir. 9^{-1} yerine 3 yazılır. Böylece;

$$x \equiv 3(y-2) \equiv 3y - 6 \equiv 3y + 20 \pmod{26}$$

V(=21) harfi $3*21 + 20 \equiv 83 \equiv 5 \pmod{26}$ (1) de f(=5) olduğundan f e eşittir. Benzer şekilde CVVWPM şifreli metni *affine* olarak deşifre edilir.

13x+4 fonksiyonu kullanarak şifreleme yapılsın:

$$input \rightarrow \text{ERRER}$$

elde edilir.

Eğer aynı fonksiyonu kullanarak *input* yerine *alter* alınırsa;

$$alter \rightarrow \text{ERRER}$$

elde edilir.

Bu fonksiyon hata verir. Sadece bir tek açık metin elde edildiği sürece deşifre etmek mümkündür. Şifreli metne karşılık gelen açık metin bir tek veya bire bir olmalıdır. Yani bir şifreli metin deşifre edildiğinde bir tek açık metin elde edilmelidir. Eğer farklı açık metinler elde edilirse bu durumda çözüm yoktur.

Bu örnekte yanlış olan nedir? Eğer y=13x+4 hesaplanırsa mod 26 ya göre $x=13^{-1}(y - 4)$ elde edilir. Fakat mod 26 ya göre 13^{-1} in eşit olduğu sayı bulunamaz. Çünkü ebob(13,26)=2 $\neq$ 1 dir. Daha genel olarak ifade edilirse bu gösterir ki $\alpha x + \beta \pmod{26}$ birebir fonksiyondur $\Leftrightarrow$ ebob(α,26)=1 dir. Bu nedenle, $\alpha \alpha^{*} \equiv 1 \pmod{26}$ olması halinde deşifrelerken $x \equiv \alpha^{*} y - \alpha^{*} \beta \pmod{26}$ kullanılır. Böylece deşifre afin fonksiyon tarafından tamamlanır.

Şifreleme metodunun anahtarı (α, β) ikilisidir. α için 12 mümkün durum vardır ebob(α,26)=1 olmak üzere β için 26 mümkün durum vardır. Anahtarı bulmak için 12*26=312 seçenek vardır. Melih'in yapabileceği mümkün saldırılar;

1) Sadece Şifreli metin: Anahtar için 312 seçeneği incelemek öteleme şifrelemesinden daha geniş kapsamlı bir tarama yapmayı gerektirir ve uzun olabilir; ancak bilgisayarda daha kısa sürede yazılabilir. Burada harflere atanılan değerler dikkate alınarak anahtarı hesaplamak mümkün olabilir.

2) Bilinen Açık Metin: Açık metinden iki harfi, bu harflere şifreli metinde tekabül eden harfleri ve bu harflere atanılan değerleri bilmek anahtarı çözmede yeterli olabilir.

Açık metin *if* ile başlasın ve şifreli metinde karşılığı *PQ* olsun. i(=8), P(=15) ve f(=5), Q(=16) dir. Bu nedenle;

$$8\alpha + \beta \equiv 15 \quad \text{ve} \quad 5\alpha + \beta \equiv 16 \pmod{26}$$

denklemleri elde edilir.

Çıkarma işlemi yapılırsa;

$3\alpha \equiv -1 \pmod{26}$ elde edilir. Bunun çözümü;

26= 3*8 + 2

$3 = 2*1 + 1$

$1 = 3 - 2*1$

$1 = 3 - (26 - 3*8)$

$1 = 9*3 - 26$

$-1 = (-9)*3 + 26 \quad \Rightarrow \quad \alpha \equiv -9 \equiv 17 \pmod{26} \quad \Rightarrow \quad \alpha = 17$ olarak bulunur.

$8\alpha + \beta \equiv 15 \pmod{26}$ denklemini kullanırsak;

$8*17 + \beta \equiv 15 \pmod{26}$ olur ve $\beta = 9$ bulunur.

Açık metinde alacağımız iki harf *go* ve şifreli metindeki karşılığı TH olsun. Buradan;

$6\alpha + \beta \equiv 19 \pmod{26}$ ve $14\alpha + \beta \equiv 7 \pmod{26}$

denklemlerini elde ederiz. Çıkarma işlemi yapılırsa;

$-8\alpha \equiv 12 \pmod{26}$ elde edilir. ebob(-8,26)=2 olduğundan α nın iki çözümü vardır. $\alpha = 5, 18$ dir. β ya karşılık gelen değerler iki α değeri için de 15 dir.(Bu bir rastlantı değildir, her durumda β sadece bir değere karşılık gelir.) Anahtar için iki seçenek vardır.(5,15) veya (18,15) anahtar olabilirler. Ancak ebob(18,26) $= 2 \neq 1$ olduğundan (18,15) seçeneği çıkarılır. Bu nedenle anahtar (5,15) tir.

Eğer sadece bir harf biliniyorsa, α ve β arasında bir bağıntı elde edilir. Örneğin; açık metinde sadece *g* harfi varsa ve şifreli metinde bu harfe karşılık gelen harf *T* ise;

$6\alpha + \beta \equiv 12 \pmod{26}$ denklemini elde ederiz. α nın alacağı 12 seçenek vardır. Çünkü (α,26)=1 olmalıdır. O halde α için 12 durum vardır. Her α değerine karşılık bir tek β değeri bulunur. Bu nedenle, geniş aramada 12 anahtar denemesi yapılarak doğru anahtar elde edilir.

3) **Seçili Anahtar Metin:** Açık metinde *ab* harflerini alınsın. Şifreli metindeki ilk karakter, $\alpha*0 + \beta = \beta$ olur. İkinci karakter $\alpha + \beta$ olur. Bu şekilde anahtar bulunur.

4) **Seçili Şifreli Metin:** *AB* şifreli metinden seçilsin. Bu veri deşifre fonksiyonunda; $x = \alpha_1 y + \beta_1$ de yazılsın. Buradan y çözümünü ve şifreleme anahtarı bulunabilir.

Örnek: “Sakarya university” kelimesini 5x+15 afin fonksiyonu ile (1) deki numaralanışa göre şifreleyiniz ve şifreli metni açık metne çeviriniz. “Sakarya university” kelimesi için Maple9.0 da şifreli metni elde ediniz ve çözücü fonksiyonunu bularak şifreli metni deşifre ediniz.

Çözüm: $y \equiv 5x+15 \pmod{26}$ alarak “Sakarya” kelimesi şifrelensin. ebob(5,26)=1 olduğundan denklemin çözümü vardır.

s=18	$\rightarrow$	$y \equiv (5*18)+15 \equiv 105 \equiv 1 \pmod{26}$	$\rightarrow$	$1 \rightarrow B$	olur.
a=0	$\rightarrow$	$y \equiv (5*0)+15 \equiv 15 \pmod{26}$	$\rightarrow$	$15 \rightarrow P$	olur.
k=10	$\rightarrow$	$y \equiv (5*10)+15 \equiv 65 \equiv 13 \pmod{26}$	$\rightarrow$	$13 \rightarrow N$	olur.
r=17	$\rightarrow$	$y \equiv (5*17)+15 \equiv 100 \equiv 22 \pmod{26}$	$\rightarrow$	$22 \rightarrow W$	olur.
y=24	$\rightarrow$	$y \equiv (5*24)+15 \equiv 135 \equiv 5 \pmod{26}$	$\rightarrow$	$5 \rightarrow F$	olur.
u=20	$\rightarrow$	$y \equiv (5*20)+15 \equiv 115 \equiv 11 \pmod{26}$	$\rightarrow$	$11 \rightarrow L$	olur.
n=13	$\rightarrow$	$y \equiv (5*13)+15 \equiv 80 \equiv 2 \pmod{26}$	$\rightarrow$	$2 \rightarrow C$	olur.
i=8	$\rightarrow$	$y \equiv (5*8)+15 \equiv 55 \equiv 3 \pmod{26}$	$\rightarrow$	$3 \rightarrow D$	olur.
v=21	$\rightarrow$	$y \equiv (5*21)+15 \equiv 120 \equiv 16 \pmod{26}$	$\rightarrow$	$16 \rightarrow Q$	olur.
e=4	$\rightarrow$	$y \equiv (5*4)+15 \equiv 35 \equiv 9 \pmod{26}$	$\rightarrow$	$9 \rightarrow J$	olur.
t=19	$\rightarrow$	$y \equiv (5*19)+15 \equiv 110 \equiv 6 \pmod{26}$	$\rightarrow$	$6 \rightarrow G$	olur.

“Sakarya university” kelimesi;

“BPNPWFP LCDQJWBDGF” olarak şifrelenir.

“BPNPWFP LCDQJWBDGF” şu şekilde deşifre edilir. $y \equiv 5x+15 \pmod{26}$ dan

$x \equiv 5^{-1}(y-15) \pmod{26}$ çözücü çekirdek elde edilir. (5,26)=1 olup $5^{-1} \pmod{26}$ ya göre hesaplanır. Bölme algoritmasından;

$26=5*5+1$

$1=26-(5*5)$

$1=26+(-5)*5$

$-5 \equiv 21 \pmod{26}$

olup $5^{-1} \pmod{26}$ a göre 21 dir. O halde çözücü çekirdek;

$x \equiv 21(y-15) \pmod{26}$ olur. Buradan $x \equiv 21y+23 \pmod{26}$ elde edilir.

3.4 PLAYFAIR VE ADFX ŞİFRELEMESİ

Playfair ve ADFX şifrelemesi II. Dünya Savaşında İngilizler ve Almanlar tarafından kullanıldı. Playfair sistemi 1854 yılında Sir Charles Wheatsone tarafından bulundu ve bu sisteme arkadaşı olan Baron Playfair of St. Andrews in adını verdi.

Burada anahtar kelime *playfair* dir. Fakat bu anahtar kelime değişebilir. Tekrarlanan harfler çıkarılırsa *playfir* elde edilir. Ve İngilizce harfler arasında **(Tablo 1)** en az kullanılan j harfi çıkarılarak *playfir* ve *j* dışında kalan diğer harflerle 5x5 lik bir matris elde edilir. Bu matris;

p	l	a	y	f
i	r	b	c	d
e	g	h	k	m
n	o	q	s	t
u	v	w	x	z

……. (3.4.1)

Açık metin *meetatschoolhouse* olarak verilsin. Açık metindeki her harf ikişer ikişer gruplara bölünür. Eğer bir harf ikişerli olarak bölünemiyorsa ve aynı harf yan yana gelmişse ya x ilave edilir yada gruptan çıkarılır. Burada metnin sonuna x eklensin. O halde açık metin;

me et at th es ch ox ol ho us ex

olur.

İkişerli harflerin şifrelenmesi (3.4.1) matrisine göre yapılır.

- Eğer iki harf aynı satır veya aynı sütunda değilse, ortak satır ve sütundaki harf alınır. Mesela; *et* için 3. satır ile 5. sütunun arakesiti olan *M* harfi ve 4.satır ile 1.sütunun arakesiti olan *N* harfi alınır. Ve açık metindeki *et* ifadesi *MN* olarak şifrelenir.
- Eğer iki harf aynı satırda iseler o satır üzerinde bir sonraki harf alınır. *me* için m harfinin sağ yanında harf olmadığı için tekrar aynı satırda başa dönülür ve m harfi E harfi ile şifrelenir. e harfi ise bir yanındaki G ile şifrelenir. Böylece açık metindeki *me* ifadesi *EG* olarak şifrelenir.
- Eğer iki harf aynı sütunda ise o sütun üzerinde bir sonraki harf alınır. *ol* için o harfi ile aynı sütundaki bir sonraki harf olan V harfi ile şifrelenir. l harfi de aynı

sütundaki bir sonraki harf olan R harfi ile şifrelenir. Böylece açık metindeki *ol* ifadesi *VR* olarak şifrelenir.

Ve şifreli metin;

EG MN FQ QM KN BK SV VR GQ XN KV

olur.

Bu yöntemle yazılmış olan bir şifreli metin bu yöntemler uygulanarak deşifre edilir.

Örnek: Anahtar kelimeyi "Salı" olarak alınız ve "hakikat" kelimesini alfabemizdeki harflere göre şifreleyiniz ve şifreli metni deşifre ediniz.

Tablo 2. den yaralanarak en az kullanılan harfler olan "Ğ,J,Ö,P" harfleri çıkarılarak ve Salı ile başlayarak aşağıdaki veri elde edilir.

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

"Hakikat" kelimesi ikişer ikişer gruplara bölünsün ve eksik olan harfin yanına Ş yi eklensin.

HA Kİ KA TŞ

HA için;

Eğer iki harf aynı sütunda ise o sütun üzerinde bir sonraki harf alınır. Kuralından dolayı H yerine "O", A yerine ise "Ç" harfleri alınır.

Kİ için;

Eğer iki harf aynı satırda iseler o satır üzerinde bir sonraki harf alınır. Kuralından dolayı K yerine "M", İ yerine "K" alınır.

KA için;

Eğer iki harf aynı satır veya aynı sütunda değilse, ortak satır ve sütundaki harf alınır. Kuralından dolayı K yerine "H" , A yerine "I" alınır.

TŞ için:

Eğer iki harf aynı satırda iseler o satır üzerinde bir sonraki harf alınır. Kuralından dolayı T yerine "N", Ş yerine "T" alınır. Ve şifreli metin:

OÇ MK HI NT olur. Yani şifreli metin;

"OÇMKHINT" olarak bulunur. Bu metni deşifre işlemleri benzer yolla yapılır.

OÇ için;

Eğer iki harf aynı sütunda ise bir önceki harfler alınır. O halde O yerine "H", Ç yerine "A" alınır.

MK için;

Eğer iki harf aynı satırda ise bir önceki harfler alınır. O halde M yerine “K”, K yerine “İ” alınır.

HI için;

Eğer iki harf aynı satır ve sütunda değilse ortak satır ve sütundaki harfler alınır. O halde H yerine “K”, I yerine “A” alınır.

NT için;

Eğer iki harf aynı satırda ise bir önceki harfler alınır. O halde N yerine “T”, T yerine “Ş” alınır.

Böylece açık metin HAKİKATŞ olarak bulunur. Ancak buradaki Ş çıkartılır ve anlamlı bir kelime olan HAKİKAT bulunur.

ADFX şifrelemesi ise İngilizce harflerle 5*5 matris elde edilir. j harfi bu matrisin elemanı değildir. Çünkü j harfi (Tablo 1) de en az kullanılan harftir. Matrisin sütunları ADFX olarak seçilir. Matris;

	A	D	F	G	X
A	p	g	c	e	n
D	b	q	o	z	r
F	s	l	a	f	t
G	m	d	v	i	w
X	k	u	y	x	h

şeklinde verilsin. Açık metnin her bir harfi satır ve sütundaki iki harfin kesişimi olarak elde edilir. s harfi FA ve z harfi DG dir. Açık metin;

Sakarya University

olarak verilsin. Bu açık metin yukarıdaki bilgilerin ışığı altında

FA FF XA FF DX XF FF XD AX GG GF AG DX FA FX XF

olarak şifrelenir. Bu şifre tekrar düzenlenmek istenirse bir anahtar alınır. Anahtar *TÜRKİYE* olsun. Şifreli metindeki harfler sırasıyla;

T	Ü	R	K	İ	Y	E
F	A	F	F	X	A	F
F	D	X	X	F	F	F
X	D	A	X	G	G	G
F	A	G	D	X	F	A
F	X	X	F			

şeklinde düzenlensin. *TÜRKİYE* kelimesindeki harfler alfabetik sıraya göre düzenlenirse bu harflere karşılık gelen harfler de şu şekilde düzenlenir:

E	İ	K	R	T	Ü	Y
F	X	F	F	F	A	A
F	F	X	X	F	D	F
G	G	X	A	X	D	G
A	X	D	G	F	A	F
		F	X	F	X	

ve yeni şifreli metin;

FXFFFAAFFXXFDFGGXAXDGAXDGFAFFXFX

şeklinde elde edilir.

3.5 HILL ŞİFRELEMESİ

1929 yılında Lester S. Hill tarfından bulunan şifreleme tekniğidir. Şifrelenmiş metindeki her eleman açık metnin n tane elemanının lineer kombinasyonu şeklinde alınır. $x=(x_1, x_2,..., x_n)$, $y=(y_1, y_2,\ldots, y_n)$ şeklinde vektörler ve nxn biçiminde N matrisi(bir anahtar matris) elde edilir. x açık metindeki harflerin (1) de karşılık geldiği değerlerdir. Açık metni şifrelemek için;

$$y=x\,[N]_{nxn}$$

i çözmek gerekir. buradaki N matrisinin tersinin olması gerekir. Ancak matrisin tersinin olması için matrisin karesel (nxn biçiminde) ve $\det(N) \neq 0$ olmalıdır. Matrisin tersi deşifre etmede kullanılacaktır.

Şifreli metni deşifre etmek içinse;

$$x=y[N]^{-1}_{nxn} \qquad (\text{mod } 26)$$

i çözmek gerekir. Ayrıca deşifre işlemi yapılması için ebob (det(N),26)=1 ve $NN^{-1} \equiv 1 \pmod{26}$ olmalıdır.

n=3 olması halinde $x=(x_1, x_2, x_3)$, $y=(y_1, y_2, y_3)$ şeklinde vektörler ve 3x3 biçiminde N matrisi(bir anahtar matris) elde edilir. x üçer üçer bölünmüş açık metindeki harflerin (1) de karşılık geldiği değerlerdir. Açık metni şifrelemek için;

$$(y_1, y_2, y_3) =(x_1, x_2, x_3)\,[N]_{3x3} \qquad (\text{mod } 26)$$

i çözmek gerekir.

Örneğin; açık metin "*Takvim"* ve n=3 olsun. Bu metin

$y_1=x_1+ 4x_2+ 11x_3$

$y_2=2x_1+ 5x_2+ 9x_3$

$y_1=3x_1+ 6x_2+ 8x_3$

lineer denklem sistemiyle şifrelensin.

$$[y_1\ y_2\ y_3] = [\,x_1\ \ x_2\ \ x_3] \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{bmatrix} \qquad (\text{mod } 26)$$

"takvim" kelimesini üçerli gruplara bölünüp (1) deki değerleri 1*3 tipinde bir matris olarak yazılsın.Yani;

[t a k]=[19 0 10]

[v i m]=[21 8 12]

$$[19\ \ 0\ \ 10]\begin{bmatrix}1 & 2 & 3\\ 4 & 5 & 6\\ 11 & 9 & 8\end{bmatrix}=[129\ \ 128\ \ 137]\equiv[25\ \ 24\ \ 7]\ \ (\text{mod } 26)\qquad t,a,k\rightarrow Z,Y,H$$

$$[21\ \ 8\ \ 12]\begin{bmatrix}1 & 2 & 3\\ 4 & 5 & 6\\ 11 & 9 & 8\end{bmatrix}=[185\ \ 190\ \ 207]\equiv[3\ \ 8\ \ 25]\ \ (\text{mod } 26)\qquad v,i,m\rightarrow D,I,Z$$

“ZYHDIZ” olarak elde edilir.

Şifreli metni deşifre etmek içinse

$$(x_1, x_2, x_3) =(y_1, y_2, y_3)\ [N]^{-1}$$

i çözmek gerekir. Şifreli metni deşifre etmek içinse;

$$x=y[N]^{-1}_{nxn}\qquad (\text{mod } 26)$$

i çözmek gerekir. Deşifre işlemi yapılması için ebob(det(N),26)=1 ve $NN^{-1}\equiv 1$ (mod 26) olmalıdır.

$$\det(N)=|N|=\begin{vmatrix}1 & 2 & 3\\ 4 & 5 & 6\\ 11 & 9 & 8\end{vmatrix}=-3\equiv 23 \quad (\text{mod } 26)$$ ve ebob(23,26)=1 olduğundan 23x+26y=1

yazılabilir. Buradaki x in değeri 23^{-1} in değerine eşittir.

$26=23*1+3$

$23=3*7+2$

$3=2*1+1$

$1=3-2*1$

$1=3-(23-3*7)$

$1=8*3-23$

$1=8*(26-23)-23$

$1=8*26+(-9)*23$

$-9\equiv 17 \ \ (\text{mod } 26)$ olup 23^{-1} in değeri 17 dir.

$$[N]^{-1}=23^{-1}\begin{bmatrix}-14 & 11 & -3\\ 34 & -25 & 6\\ -19 & 13 & -3\end{bmatrix}\equiv 17\begin{bmatrix}12 & 11 & 23\\ 8 & 1 & 6\\ 7 & 13 & 23\end{bmatrix}\quad (\text{mod } 26)$$

$$[N]^{-1} \equiv \begin{bmatrix} 22 & 5 & 1 \\ 6 & 17 & 24 \\ 15 & 13 & 1 \end{bmatrix} \pmod{26}$$

Böylece $[N][N]^{-1} \equiv 1 \pmod{26}$ dır.

"ZYHDIZ" için [Z Y H]=[25 24 7] ve [D I Z]=[3 8 25] olup.

$$[x_1 \quad x_2 \quad x_3]=[25 \quad 24 \quad 7] \begin{bmatrix} 22 & 5 & 1 \\ 6 & 17 & 24 \\ 15 & 13 & 1 \end{bmatrix} \equiv [19 \quad 0 \quad 10] \pmod{26}$$

$$[x_1 \quad x_2 \quad x_3]=[3 \quad 8 \quad 25] \begin{bmatrix} 22 & 5 & 1 \\ 6 & 17 & 24 \\ 15 & 13 & 1 \end{bmatrix} \equiv [21 \quad 8 \quad 12] \pmod{26}$$

Buradan "takvim" elde edilir.

Örnek: $N = \begin{bmatrix} 5 & 3 \\ 6 & 7 \end{bmatrix}$ matrisini kullanarak "Matematik" kelimesini şifreleyiniz ve şifreli metni deşifre ediniz.

"matematik" kelimesini ikişerli gruplara bölünüp (2) deki değerleri 1×2 tipinde bir matris olarak yazılsın.Yani;

[m a]=[15 0]

[t e]=[23 5]

[t i]=[23 11]

[k j]=[13 12]

$$[15 \quad 0] \begin{bmatrix} 5 & 3 \\ 6 & 7 \end{bmatrix} = [75 \quad 45] \equiv [17 \quad 16] \pmod{29} \quad m,a \rightarrow O,N$$

$$[23 \quad 5] \begin{bmatrix} 5 & 3 \\ 6 & 7 \end{bmatrix} = [145 \quad 104] \equiv [0 \quad 17] \pmod{29} \quad t,e \rightarrow A,O$$

$$[23 \quad 11] \begin{bmatrix} 5 & 3 \\ 6 & 7 \end{bmatrix} = [181 \quad 146] \equiv [7 \quad 1] \pmod{29} \quad t,i \rightarrow G,B$$

$$[13 \quad 12] \begin{bmatrix} 5 & 3 \\ 6 & 7 \end{bmatrix} = [21 \quad 7] \pmod{29} \quad k,j \rightarrow S,G$$

Şifreli metin; "ONAOONGBSG" olur.

Deşifre işlemi yapılması için ebob(det(N),29)=1 ve $NN^{-1} \equiv 1 \pmod{29}$ olmalıdır.

$\det(N)=|N|=\begin{vmatrix} 5 & 3 \\ 6 & 7 \end{vmatrix}=17 \pmod{26}$ ve ebob(17,29)=1 olduğundan 17x+29y=1 yazılabilir.

Buradaki x in değeri 17^{-1} in değerine eşittir.

29=17*1+12

17=12*1+5

12=5*2+2

5=2*2+1

1=5-2*2

1=5-(2* (12-5*2))

1=5*5-2*12

1=5* (17-12)-2*12

1=5*17-7*12

1=5*17-7* (29-17)

1=12*17-7*29

olup 17^{-1} in değeri 12 dir.

$$[N]^{-1}=17\text{-}1\begin{bmatrix} 7 & -3 \\ -6 & 5 \end{bmatrix} \equiv 12\begin{bmatrix} 7 & 26 \\ 23 & 5 \end{bmatrix} \equiv \begin{bmatrix} 26 & 22 \\ 15 & 2 \end{bmatrix} \pmod{29}$$

$$[N]^{-1} \equiv \begin{bmatrix} 26 & 22 \\ 15 & 2 \end{bmatrix} \pmod{29}$$

Böylece $[N][N]^{-1} \equiv 1 \pmod{29}$ dır.

"ONAOONGBSG" için [O N]=[17 16] , [A O]=[0 17], [G B]=[7 1] ve [S G]=[21 7] olup.

$$[x_1 \quad x_2]=[17 \quad 16]\begin{bmatrix} 26 & 22 \\ 15 & 2 \end{bmatrix} \equiv [15 \quad 0] \pmod{29}$$

$$[x_1 \quad x_2]=[0 \quad 17]\begin{bmatrix} 26 & 22 \\ 15 & 2 \end{bmatrix} \equiv [23 \quad 5] \pmod{29}$$

$$[x_1 \quad x_2]=[7 \quad 1]\begin{bmatrix} 26 & 22 \\ 15 & 2 \end{bmatrix} \equiv [23 \quad 11] \pmod{29}$$

$$[x_1 \quad x_2]=[21 \quad 7]\begin{bmatrix} 26 & 22 \\ 15 & 2 \end{bmatrix} \equiv [13 \quad 12] \pmod{29}$$