b) Şimdi de $n = 2^k$ olsun. O zaman binom katsayıları

$$\binom{n}{m} = \text{çift sayı} \equiv 0, \quad (m = 1, 2, \ldots, n-1)$$

olduğundan

$$\begin{aligned} B^{n^2} &\equiv (B^{n-1} + I)^n \equiv B^{n(n-1)} + I \Rightarrow \\ I &\equiv B^{n^2} + B^{n^2-n} \equiv B^{n^2-n}(B^n + I) \\ &\equiv B^{n^2-n} B^{n-1} \equiv B^{n^2-1} \end{aligned}$$

olur, bu da ulaşmak istediğimiz sonucu gerektirir.

c) Şimdi de $n = 2^k + 1$ olsun. Yine $B^n \equiv B^{n-1} + I$ olduğunu ve $n-1$ in ilk ve sonuncu dışındaki binom katsayılarının çift sayı, dolayısıyla mod 2 ye göre 0 olduğunu kullanarak

$$\begin{aligned} B^{n^2-1} &\equiv (B^{n+1})^{n-1} \equiv (B(I + B^{n-1}))^{n-1} \\ &\equiv (B + B^n)^{n-1} \equiv B^{n-1} + B^{n(n-1)} \\ &\equiv B^{n-1} + B^{n^2-n}. \end{aligned}$$

Buradan

$$\begin{aligned} B^{n-1} &\equiv B^{n^2-n} + B^{n^2-1} \equiv B^{n^2-n}(I + B^{n-1}) \\ &\equiv B^{n^2-n} B^n \equiv B^{n^2} \end{aligned}$$

olur. $\det B \equiv 1 \not\equiv 0$ olduğu için B matrisinin tersi vardır. Son satırı $B^{-(n-1)} = (B^{n-1})^{-1}$ ile çarparak $B^{n^2-n+1} \equiv I$ elde edilir, bu da göstermek istediğimiz eşitliği gerektirir.

KRİPTOLOJİ

Hüseyin Altındiş *

Eski çağlardan beri haberleşmelerde gizlilik üzerinde önemle durulan bir sorundur. Gizlilikten amaç gönderilen bir mesajı ilgili alıcısından başka kimsenin anlamamasıdır.

Gizlilik sistemlerine girmeden önce konu ile ilgili bir kaç terminolojiyi açıklayalım. Gizlilik sistemlerinin bağlı olduğu bilim dalı **kriptoloji** olarak adlandırılır. Gizli şekle çevrilecek mesaj **açık metin**, bir takım özel dönüşümler uygulayarak açık metindeki harfleri değiştirme işlemi **şifreleme**, şifrelenmiş metin de **şifre metin** olarak adlandırılır. Şifre metninin tekrar anlaşılır hale getirilmesine de **deşifre** etme denir. Kriptografi ise gizlilik sistemlerinin tasarım ve araçları ile ilgili kriptolojinin bir parçasıdır.

İlk olarak, modüler aritmetiğe dayanan ve Julius Ceasar'a kadar uzandığı bilinen, **karakter** veya **monografik** şifrelemeden söz edeceğiz. Bu tür şifrelemede **açık metin**deki her bir harf başka bir harfe dönüştürülerek **şifre metin** elde edilir.

Bunu yaparken de herbir harf bir sayıya dönüştürülür. Hangi dilden mesaj gönderilecekse o dilin standart alfabesi kullanılabilir. Türk alfabesini kullanarak aşağıdaki tabloyu oluşturalım.

Tablo 1

Harf	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
Sayı Değeri	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

Bu tabloya noktalama işaretleri, semboller, rakamlar ilave edilebilir, fakat basit olması açısından sadece harflerle yetinelim. Monografik şifrelemede her bir harf farklı bir harfe dönüştürüldüğüne göre 29! farklı dönüşüm yapılabilir. Ceasar alfabedeki her bir harfi kendinden 3 sonra gelen harfle değiştirerek şifre metnini elde etmiştir. Dolayısıyla Ceasar şifreleme metodu için

$$C \equiv P + 3 (\text{mod } 29), \quad 0 \leq C \leq 28$$

bağıntısı kurulabilir. Buradaki P, **açık metin**deki her bir harfin sayısal değeri, C de **şifre metin**de bu harflere karşılık gelen sayısal değerdir. Bu karşılık getirme Tablo 2'de verilmiştir.

*Erciyes Üniversitesi Matematik Bölümü

Tablo 2

Açık Metin P	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Şifre Metin C	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	0	1	2
	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C

Şimdi Ceasar şifresi ile "Lütfen ödemeleri durdurunuz" mesajını şifreleyelim. Önce bu mesajı beş harften oluşan gruplara ayıralım. Bunu yapmakla bazı kelimelerin tanınma olasılığını önlemiş oluruz.

LÜTFE NÖDEM ELERİ DURDU RUNUZ

Şimdi Tablo 1 kullanılarak harfler sayısal eşitliklerine çevrilirse

14 25 23 6 5 16 18 4 5 15 5 14 5 20 11 4 24 20 4 24 20 24 16 24 28

elde ederiz. $C \equiv P + 3 (\text{mod } 29)$, $0 \leq C \leq 28$ bağıntısını kullanırsak;

17 28 26 9 8 19 21 7 8 18 8 17 8 23 14 7 27 23 7 27 23 27 19 27 2

bulunur ki bu şifre metninin sayısal karşılığıdır. Bu rakamlar tekrar harflere dönüştürülerse şifre metni

OZVHĞ PSGĞÖ ĞOĞTL GYTGY TYPYC

olarak ortaya çıkar. Alıcı bu mesajı deşifre ederken önce harfleri sayısal eşitliklerine çevirir, daha sonra

$$P \equiv (C - 3) (\text{mod } 29), \quad 0 \leq P \leq 28$$

bağıntısı ile açık metin sayısal olarak elde edilir, rakamların harflere dönüştürülmesi ile de mesaj beşli gruplar olarak ortaya çıkar, artık bu gruplardan anlamlı bir cümle çıkartmak zor değildir.

Şimdi de Ceasar şifresi ile şifrelenmiş

ÇPOÇÜ ÖÇUÇİ OÇPGK

mesajı deşifre edelim. Harfler sayısal eşitliklerine çevrilirse

3 19 17 3 25 18 3 24 3 11 17 3 19 7 13

elde edilir, $P \equiv C - 3 (\text{mod } 29)$, $0 \leq P \leq 28$ bağıntısı kullanılırsa

0 16 14 0 22 15 0 21 0 8 14 0 16 4 10

olarak bulunur. Sayıları harflere dönüştürürsek

ANLAŞ MASAĞ LANDI

olur, uygun şekilde düzenlenirse "Anlaşma sağlandı" şeklinde mesaj ortaya çıkar.

Ceasar şifreleme yöntemi Shift dönüşümleri olarak bilinen

$$C \equiv P + k (\text{mod } 29), \quad 0 \leq C \leq 28$$

dönüşümler ailesinden birisidir. Buradaki k bir sabit olup 29 farklı şekilde seçilebilir $k \equiv 0 \ (\text{mod } 29)$ seçilirse $C \equiv P \ (\text{mod } 29)$ olur ki bu durumda her harf yine kendisine dönüşmüş olur. Bu şifreleme yöntemi oldukça basit olduğundan bazı olumsuz yönleri de vardır.

$$C \equiv aP + b \ (\text{mod } 29), \quad 0 \leq C \leq 28$$

şeklindeki dönüşümler ilgin Dönüşümler olarak bilinirler ve daha geneldirler. Burada a ve b tamsayılar olup $(a, 29) = 1$ dir.[1] $a = 1$ seçilirse Shift dönüşümleri elde edilir. $(a, 29) = 1$ olduğundan P ve $C, (\text{mod } 29)$ a göre komple kalan sistemi üzerinden değerler alabilirler. Euler'in Φ fonksiyonu hatırlanacak olursa a için $\Phi(29) = 28$ farklı seçim düşünülebilir, keza b için de 29 farklı seçim söz konusu olduğuna göre toplam $28.29 = 812$ farklı bu çeşit dönüşüm yapılabilir.

İlgin dönüşümü ile bir mesaj şifrelendi ise alıcı

$$P \equiv \overline{a}(C - b)(\text{mod } 29), \quad 0 \leq P \leq 28$$

bağıntısı ile **açık metni** elde eder ki burada $\overline{a}$ a nın $(\text{mod } 29)$ a göre tersidir.[2] Örnekleyecek olursak ilgin dönüşümünde $a = 7, b = 10$ seçerek herhangi bir mesajı şifrelemek isteyelim. Şifre metnini

$$C \equiv 7P + 10 \,(\text{mod } 29), \quad 0 \leq C \leq 28$$

bağıntısından elde ederiz ki harfler arasındaki bağıntı Tablo 3'te verilmiştir.

Tablo 3

Açık Metin P	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Şifre Metin C	10	17	24	2	9	16	23	1	8	15	22	0	7	14	21	28	6	13	20	27	5	12	19	26	4	11	18	25	3
	I	O	U	C	H	N	T	B	J	M	Ş	A	G	L	S	Z	F	K	R	Y	E	Ğ	P	V	D	P	Ö	Ü	Ç

Bu tablonun nasıl teşkil edildiğini görmek istersek, örneğin **açık metin**deki Ş harfinin sayısal eşiti 22 dir, $C \equiv 7.22 + 10 = 162 \equiv 19 \,(\text{mod } 29)$ olur, 19 P harfinin sayısal değeridir.

Mesajımız "FIRTINA YAKLAŞIYOR" olsun. Bunu önce beşli grupları ayıralım.

FIRTI NAYAK LAŞIY OR

Sayısal eşitliklerini yazarsak;

6 10 20 23 10 16 0 27 0 13 14 0 22 10 27 17 20

olur, yukarıdaki bağıntı kullanılırsa

23 22 5 26 22 6 10 25 10 14 21 10 19 22 25 13 5

değerleri elde edilir. Bu sayılarda harflere dönüştürülürse

TŞEVŞ FIÜIL SIPŞÜ KE

olur, mesajımız bu şekilde gönderilir. Alıcı bu mesajı deşifre ederken

$$P \equiv 25 \,(C - 10) \,(\text{mod } 29)$$

bağıntısını kullanır, buradaki 25, 7 nin 29 modülüne göre tersidir.

Aynı bağıntı ile şifrelenmiş

ĞIÜŞŞ IEVNK EAĞAZ NGIGS IEŞPA TENSN ZNHNC KLLDS SIFŞP SŞHŞE

Mesajı deşifre etmeyi de okuyucuya bırakıyorum.

Monografik şifrelemede önemli bir diğer yöntem de Vigenere Şifrelemesidir. Şöyle uygulanır: n harften oluşan anahtar bir kelime seçilir, bu kelimenin harflerinin dizisi $1_1, 1_2, \ldots, 1_n$ ve sayısal değerleri de $k_1, k_2, \ldots, k_n$ olsun. **Açık Metin** n uzunluğunda bloklara ayrılır. Sayısal değerleri $p_1, p_2, \ldots, p_n$ olan Açık Metinin harflerinin blokları şifrelenirken

$$c_1 \equiv p_1 + k_1 \,(\text{mod } 29), \quad 0 \leq c_1 \leq 28$$

$i = 1, 2, \ldots, n$ bağıntısı kullanılarak Şifre Metninin harf bloklarının $c_1, c_2, \ldots, c_n$ sayısal değerleri bulunur. Örnek; "GİZLİ" kelimesini anahtar kelime olarak seçelim ve "BU ZARFI AÇMAYINIZ" mesajını şifreleyelim. Önce mesajımızı anahtar kelimemizin uzunluğu kadar bloklara ayıralım.

[1] (a, b) a ve b sayılarının en büyük ortak böleni gösterir.

[2] 29 sayısı asal olduğundan $\mathbb{Z}_{29} \setminus \{0\}$ çarpmaya göre gruptur. Bkz. Matematik Dünyası, **3/4**, "Wilson Teoremi".

BUZAR FIAÇM AYINI Z

ilk blok şifrelenirken $p_1 = 1\ (B)$, $k_1 = 7\ (G)$ alınarak $c_1 \equiv 8 \pmod{29}$ bulunur, $p_2 = 24$, $k_2 = 11$ alınarak c_2 için 6 bulunur. Benzer olarak c_3, c_4, c_5 bulunursa ilk blok sayısal değerler olarak 8 6 27 14 2 şeklinde elde edilir. Aynı işlemler diğer bloklar için tekrarlanırsa Şifre metnimiz sayısal değerler olarak

8 6 27 14 2 13 21 28 17 26 7 9 9 1 21 6

elde edilir. Bu sayılar da harflere dönüştürülürse Şifre metni

ĞFYLC KSZOV GHHBS F

olarak ortaya çıkar. Deşifre ederken de $p_1 \equiv c_1 - k_1 \pmod{29}$ bağıntısı kullanılır.

Anahtar kelime olarak "kalem" kelimesini seçerek "birlik kuşatmayı kaldırsın" mesajının şifrelenmesi de okuyucuya bırakılmıştır.

Blok Şifreler

Monografik şifrelemede Açık metindeki her bir harfe şifre metninde bir harf karşılık getiriliyordu. Aynı bir harfin sık sık kullanılması hem bir takım yanlışlıklara sebep olabilir, hem de şifrenin çözülmesine sebep olabilir. Bu tür olumsuzlukları gidermek için **Blok** veya **Poligrafik Şifreler** denilen ve 1930 yıllarında Hill tarafından geliştirilen bir yöntemden söz edelim. Böyle şifrelemelerde açık metin istenilen uzunlukta bloklara ayrılır. Önce ikili şifreleri görelim. Yapacağımız ilk iş mesajı iki harften oluşan bloklara ayırmak, gerekirse mesajın sonuna bir harf ilave edilebilir. Örneğin, "Petrol Ramanda Çıkarılır" mesajını şifreleyelim. Mesaj ikili bloklara ayrılırsa

PE TR OL RA MA ND AÇ IK AR IL IR

Bu harfler sayısal eşitliklerine çevrilirse,

19 5	23 20	17 14	20 0	15 0	16 4
0 3	10 13	0 20	10 14	10 20	

Buradaki her bir ikili blokun P_1P_2 değeri şifre metninin C_1C_2 değerine döndürülür. Eğer

$$\begin{aligned} C_1 &\equiv 5P_1 + 17P_2 (\text{mod } 29) \\ C_2 &\equiv 4P_1 + 15P_2 (\text{mod } 29) \end{aligned} \qquad (*)$$

gibi bir Şifreleme sistemi kullanılırsa 19 5 bloku 8 6 bloğuna, 23 20 bloğu da 20 15 bloğuna döndürülür. Bu şekilde bütün bloklar döndürülürse

6 6	20 15	4 17	13 22	17 2	3 8
22 16	10 3	21 10	27 18	13 21	

sayısal değerleri elde edilir. Bunlarda harflere dönüştürüldüğünde şifre metni olarak

FF RM DO KŞ OC ÇĞ ŞN IÇ SI YÖ KS

elde edilir. Alıcıya bu şekilde ulaşan bu mesajı anlamlı bir hale getirelim. Bunu yaparken de aşağıdaki teoremden faydalanalım.

Teorem. $m > 0, a, b, c, d, e, f \in Z, \delta = ad - bc$ ve $(\delta, m) = 1$ olmak üzere

$$\begin{aligned} ax + by &\equiv e (\text{mod } m) \\ cx + dy &\equiv f (\text{mod } m) \end{aligned}$$

kongrüans sisteminin (mod m) ye göre

$$\begin{aligned} x &\equiv \overline{\delta}(de - fb) (\text{mod } m) \\ y &\equiv \overline{\delta}(af - ce) (\text{mod } m) \end{aligned}$$

şeklinde tek çözüme sahiptir. Burada $\overline{\delta}, \delta$ nın mod m ye göre tersidir.

Bu teoreme göre C_1C_2 şifre blokuna karşılık gelen P_1P_2 açık metin blokunu bulmak için

$$\begin{aligned} P_1 &\equiv 27C_1 + 19C_2 \pmod{29} \\ P_2 &\equiv 16C_1 + 9C_2 \pmod{29} \end{aligned} \qquad (**)$$

bağıntısını kullanmalıyız. Bu bağıntı her bir C_1C_2 bloğu için tekrarlanarak bütün P_1P_2 blokları elde edilir, böylece mesaj deşifre edilmiş olur.

Bu vermeye çalıştığımız ikili şifreleme sistemi matrisler kullanılarak da ifade edilebilir. Yukarıda verdiğimiz $(*)$ sistemini matris formunda yazarsak;

$$\begin{bmatrix} C_1 \\ C_2 \end{bmatrix} = \begin{bmatrix} 5 & 17 \\ 4 & 15 \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \end{bmatrix} \pmod{29}$$

elde edilir. $(**)$ sistemi için de

$$\begin{bmatrix} P_1 \\ P_2 \end{bmatrix} = \begin{bmatrix} 27 & -19 \\ 16 & 9 \end{bmatrix} \begin{bmatrix} C_1 \\ C_2 \end{bmatrix} \pmod{29}$$

formu kullanılabilir.

Genel olarak Hill şifre sistemi açık metni n harfli bloklara bölmek bu harfleri nümerik eşitliklerine çevirmek daha sonra da

$$C \equiv AP \pmod{29}$$

bağıntısını kullanarak şifre metnini elde etmek şeklinde ifade edilebilir. Burada $A, n \times n$ tipinde bir matris olup, $(\det A, 29) = 1$ dir. Ayrıca C ve P sırası ile C_1 ve P_1 lerden oluşan $(i = 1, 2, \ldots, n) n \times 1$ tipinde sütun matrisleridir. Şifre metnin'den açık metni elde etmek için de $P \equiv \overline{A}C \pmod{29}$ bağıntısı kullanılır. Buradaki $\overline{A}, A$ matrisinin (mod 29) a göre ters matrisidir.

$$A = \begin{bmatrix} 11 & 2 & 19 \\ 5 & 23 & 25 \\ 20 & 7 & 1 \end{bmatrix}$$

matrisini kullanarak "iyi bayramlar" mesajı şifrelenirse

GTL CKÖ JİH JPI

olarak şifre metni elde edilir.

$$\begin{bmatrix} 4 & 5 \\ 3 & 1 \end{bmatrix}$$

matrisi kullanılarak şifrelenmiş

IV AO IÇ UU

mesajını deşifre etmeyi de okuyucuya bırakıyorum.