KRİPTOLOJİ BİLİMİ

DANIŞMAN: Doç. Dr. Onur ŞAHİN

Sıla KARAŞAHİN

GİRİŞ

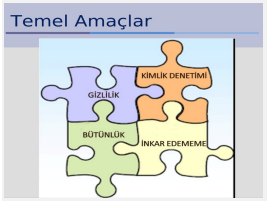
Kriptoloji, bilginin yetkisiz kişiler tarafından erişilmesini, değiştirilmesini veya taklit edilmesini önlemek amacıyla geliştirilen yöntem ve teknikleri inceleyen bilim dalıdır. Kriptografi ve kriptoanaliz olmak üzere iki ana alt disiplinden oluşan kriptoloji, güvenli iletişimin sağlanmasında temel bir rol üstlenmektedir. Matematik, bilgisayar bilimi, bilgi teorisi ve cebirsel yapılar gibi farklı disiplinlerden yararlanan bu alan, gizlilik, bütünlük, kimlik doğrulama ve inkâr edilemezlik gibi bilgi güvenliğinin temel ilkelerinin gerçekleştirilmesini hedefler. Kriptolojinin uzun ve eskilere dayanan bir tarihi vardır. İlk kriptografik belge yaklaşık olarak M.Ö. 1900 yılında yazıldığı tahmin edilen Rosetta tabletidir.

İnsanlığın bildiği en eski şifreleme yöntemlerinden biri Ortadoğu'da kullanılan Atbash Şifreleme yöntemidir.

Bir diğer şifreleme yöntemi ise, 2500 yıldan uzun bir süre öncesinde Yunanlılar tarafından veri güvenilirliğini sağlamak amacıyla kullanılan askeri şifreleme yöntemi olan Seytale Şifreleme yöntemidir

GÜNÜMÜZDE KULLANILAN ALANLAR

Sim Kartlar
Cep Telefonları
Online Bankacılık
Online Alışveriş
Uydu Alıcıları
Uzaktan Kumandalar



SEZAR ŞİFRELEME YÖNTEMİ

Roma İmparatoru Jül Sezar tarafından kullanılmıştır. Her harf, alfabede kendisinde sonra gelen üçüncü harf ile değiştirilir. Örneğin ''MATEMATİK'' kelimesi;

1) ''MATEMATİK ''kelimesi anahtar $k = 3$ alınarak şifrelenir.
2) Tablodan yararlanarak, $k = 3$ olduğundan $A + 3\,(mod29)$ fonksiyonu oluşturulur. $(mod29)$ a göre işlem yapıldıktan sonra ''MATEMATİK'' $k = 3$ ile ''ÖÇVĞÖÇVLN'' şeklinde şifrelenir.

Türkçe Harfler ve Sayı Karşılıkları

A	B	C	Ç	D	E	F	G	Ğ	H
0	1	2	3	4	5	6	7	8	9
I	İ	J	K	L	M	N	O	Ö	P
10	11	12	13	14	15	16	17	18	19
R	S	Ş	T	U	Ü	V	Y	Z	0
20	21	22	23	24	25	26	27	28	29

İngilizce Harfler Ve Sayı Karşılıkları

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9
K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19
U	V	W	X	Y	Z	0			
20	21	22	23	24	25	26			

YERİNE KOYMA ALGORİTMASI

Bu algoritmada P (muhtemel olan sonlu tüm açık metinler kümesi), C (tüm şifreli metinler kümesi) olmak üzere $P = C = Z_{29}$ şeklinde olup ve $\boldsymbol{K}$, 29 tane harfin (0,1,…,28) tüm olası permütasyonlarını içermektedir. Gönderilmek istenen metin $\forall \boldsymbol{\pi} \in \boldsymbol{K}$ için $\boldsymbol{e_\pi(x) = \pi(x)}$ fonksiyonu kullanılarak şifrelenir. Karşı tarafa iletilen şifrelenmiş metin $\boldsymbol{d_\pi(y) = \pi^{-1}(y)}$ fonksiyonu ile çözülür.

"HER PENCERE BÜYÜKLÜĞÜNE GÖRE IŞIK ALIR" Cümlesi tablo yardımıyla aşağıdaki gibi şifrelenir:
''NYŞ ÇYDZYŞY HBIBEUBVBDY GKŞY FCFE PUFŞ''
ve ikinci tablodan yerine koyarak okunur.

a	b	c	ç	d	e	f	g	ğ	h
P	H	Z	Ö	Ğ	Y	O	G	V	N
ı	i	j	k	l	m	n	o	ö	p
F	Ü	M	E	U	L	D	T	K	Ç
r	s	ş	t	u	ü	v	y	z	
Ş	C	S	İ	B	R	I	A		

A	B	C	Ç	D	E	F	G	Ğ	H
Z	ü	ş	p	n	k	ı	g	d	b
I	İ	J	K	L	M	N	O	Ö	P
Y	u	s	ö	m	j	h	f	ç	a
R	S	Ş	T	U	Ü	V	Y	Z	
v	t	r	o	ı	i	ğ	e	c	

FİBONACCİ SAYILARI İLE ALGORİTMA

İlk olarak şifrelenecek olan metin 2mx2m tipinde bir kare matrise dönüştürülür. Bu matris içine eksik kalan matris elemanları yerine sıfır alınarak yerleştirilir. Bundan sonra bu matris soldan başlayarak 2x2 tipinde alt matrislere ayrılır.

Örneğin, Aşağıda verilmiş şifrelenen matrisin metnini bulalım

$$\mathbf{K}=\begin{bmatrix} 8 & 16 & 16 & 5 \\ 28 & 14 & 16 & 19 \\ 15 & 10 & 15 & 8 \\ 28 & 28 & 28 & 28 \end{bmatrix}$$

K matrisi soldan sağa doğru 2x2 matrislere ayrılır.

$$\boldsymbol{A_1} = \begin{bmatrix} 8 & 16 \\ 28 & 14 \end{bmatrix} \qquad \boldsymbol{A_2} = \begin{bmatrix} 16 & 5 \\ 16 & 19 \end{bmatrix}$$

$$\boldsymbol{A_3} = \begin{bmatrix} 15 & 10 \\ 28 & 28 \end{bmatrix} \qquad \boldsymbol{A_4} = \begin{bmatrix} 15 & 8 \\ 28 & 28 \end{bmatrix}$$

Alt matris sayısı **n=4>3** olduğundan $\left[\left|\frac{4}{2}\right|\right] = \mathbf{2}$, **k=2** olur.

Fibonacci Q matrisi kullanılarak

$$\boldsymbol{Q} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

$k = 2$ için

$$\boldsymbol{Q^2} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}, \qquad \boldsymbol{(Q^2)^{-1}} = \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix}$$

Şifre çözme işlemi her alt matris için

$$\boldsymbol{B_i = \left(Q^2\right)^{-1} * A_i\ (mod29)}$$

şeklinde uygulanır. Örneğin A_1 için

$$\boldsymbol{B_1} = \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} \begin{bmatrix} 8 & 16 \\ 28 & 14 \end{bmatrix} = \begin{bmatrix} -20 & 2 \\ 48 & 12 \end{bmatrix}$$

olur.

Mod 29 alınırsa

$$\boldsymbol{B_1} = \begin{bmatrix} 9 & 2 \\ 19 & 12 \end{bmatrix} \boldsymbol{(mod29)}$$

olur. Aynı işlemler diğer alt matrisler için de uygulanır. Elde edilen sayılar tablo kullanılarak harfe çevrilir.

G	O	O	D	0	M	O	R	N	I	N	G
8	16	16	5	28	14	16	19	15	10	15	8

Bunun sonucunda alt matrislerden elde edilen harfler birleştirildiğinde açık metin '' GOOD MORNING'' olarak bulunur.

AFİN ŞİFRELEME ALGORİTMASI

Afin şifreleme algoritmasında $\boldsymbol{P = C = Z_{29}, A, B \in Z_{29}}$ için $\boldsymbol{\mathcal{K} = \{(a,b) \in Z_{29} * Z_{29}: (a,29) = 1\}, K = (a,b) \in \mathcal{K}}$ şeklinde tanımlanır. Şifrelenmek istenen metin $\boldsymbol{x, y \in Z_{29}}$ olmak üzere $\boldsymbol{e_k(x) \equiv ax + b(mod29)}$ dönüşümü ile karşı tarafa iletilir. Şifre çözümü için ise

$$\boldsymbol{d_k(y) \equiv a^{-1}(y - b)(mod29)}$$

fonksiyonu kullanılır.

''ON'' kelimesine uygulanacak olursa $\boldsymbol{O = 17}$ ve $\boldsymbol{N = 16}$'dır. $\boldsymbol{K = (7,3)}$ şeklinde keyfi bir anahtar seçilecek olursa tanımdan yararlanarak $a = 7, b = 3$ olur. $(7,29) = 1$ olduğundan şifreleme fonksiyonu

$$\boldsymbol{e_k(x) \equiv 7x + 3(mod29)}$$

olur.

Buna göre;

$$\boldsymbol{7.17 + 3 \equiv 6(mod29)} \text{ ve } \boldsymbol{7.16 + 3 \equiv 28(mod29)}$$

bulunur.

Tablodan yararlanılarak ''ON'' kelimesinin şifrelenmiş hali ''FZ'' olarak elde edilir . Şifrelenmiş metin $\boldsymbol{K}$ anahtarı yardımıyla açık metne dönüştürülür.

$\boldsymbol{a.a^{-1} \equiv 1(mod29)}$ olduğundan $\boldsymbol{a.a^{-1} - 29y \equiv 1(mod29)}$ elde edilip $\boldsymbol{K = (7,3)}$ anahtarı yardımıyla $\boldsymbol{7a^{-1} - 29y \equiv 1(mod29)}$ fonksiyonu bulunur. Öklid algoritması yardımıyla $\boldsymbol{a^{-1}}$ aşağıdaki şekilde ifade edilir:

$$\boldsymbol{29 = 4.7 + 1}$$
$$\boldsymbol{7 = 7.1 + 0}$$

O halde,

$$\boldsymbol{1 = 29 - 4.7}$$
$$\boldsymbol{1 = 7.(-4) - 29.(-1)}$$

olup

$$\boldsymbol{a^{-1} \equiv -4 \equiv -4 + 29 \equiv 25(mod29)}$$

yazılır. Dolayısıyla

$$\boldsymbol{25(y - 3) \equiv (25.7)x \equiv x(mod29)}$$

denkliği ile

$$\boldsymbol{d_k(y) \equiv 25(y - 3) \equiv 25y - 75 \equiv 25y - 17(mod29)}$$

fonksiyonu bulunur.

$\boldsymbol{y = 6}$ alınırsa, $\boldsymbol{d_k(y) \equiv 25(6 - 3) \equiv 17(mod29)}$ $\mathbf{x = 17}$ elde edilir. Bu ise tablodan ''O'' harfine karşılık gelir.

$\boldsymbol{y = 28}$ alınırsa $\boldsymbol{d_k(y) \equiv 25(28 - 3) \equiv 16(mod29)}$ $\mathbf{x = 16}$ elde edilir. Bu ise tablodan ''N'' harfine karşılık gelir. Böylece **''ON''** metnine ulaşılır.

KAYNAKÇA

1. gcris.pau.edu.tr
2. Özyılmaz, Ç., "Kriptolojiye giriş", Yüksek Lisans Tezi, Karabük Üniversitesi Fen Bilimler Enstitüsü, Matematik Ana Bilim Dalı, Karabük, (2014).
3. Yeşilbaş, E., "Cebirsel kriptoloji yöntemleri ve bazı uygulamalar", Yüksek Lisans Tezi, Recep Tayyip Erdoğan Üniversitesi Fen Bilimleri Enstitüsü, Matematik Ana Bilim Dalı, Rize, (2016).
4. https://ebs.pusula.pau.edu.tr.