

Şifreleme Algoritmaları

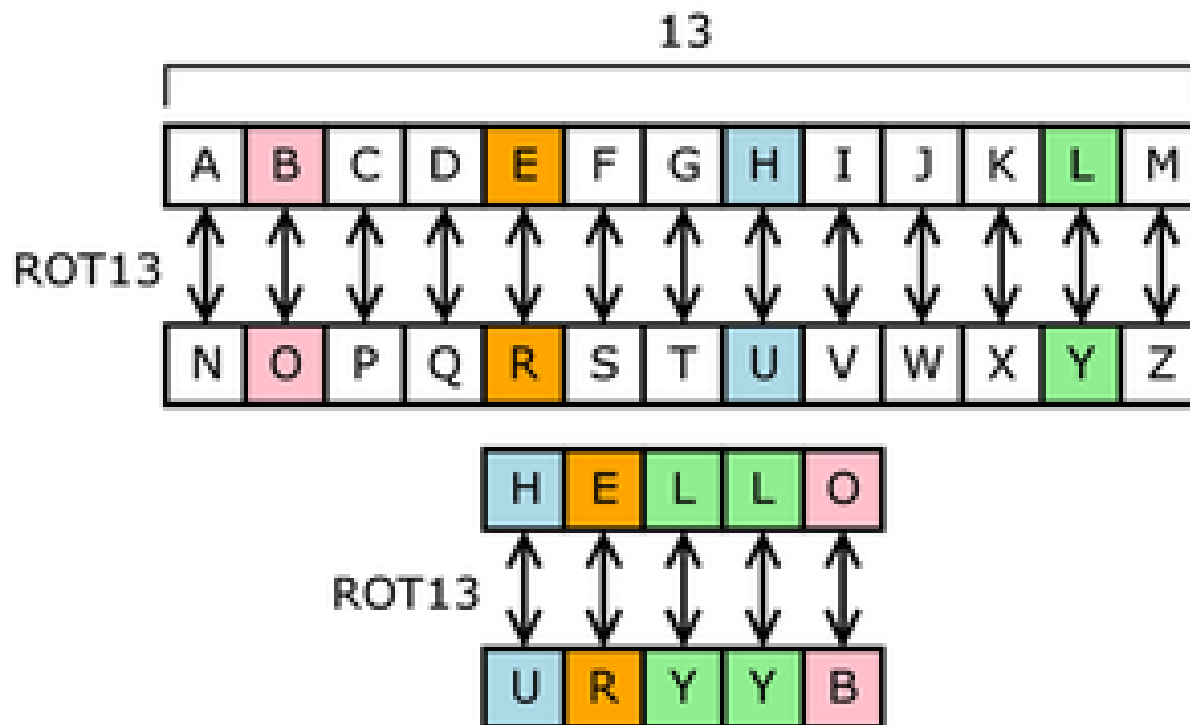


Yerine Koyma Şifresi

Substitution Cipher

Yerine koyma şifreleme metodu, Sezar veya Açık Anahtar Şifreleme metodunun biraz daha zorlaştırılmış şekli olmakla birlikte, **şifre çözmede frekans analiz teknikleriyle kolaylıkla bulunabilecek yöntemler arasındadır.**

Şifreleme Algoritmaları



Şifreleme Algoritmaları



✓ Permutasyonlar

Permutation

✓ Basit şifreleme metotlarından biri de yazılan metnin yeterli büyüklükte $n \times n$ 'lik bir karenin satırlarına sırayla yazılması ve sütunların okunarak şifreli metnin oluşturulmasıdır.

✓ Örneğin; “BU BİR DENEMEDİR.” cümlesini bu yöntemle şifrelemek istediğimizde, 4×4 büyüklükteki kareye metni yazıp boşlukları x ile doldururuz.

Şifreleme Algoritmalarına Örnek



Düz metin

B	U	B	İ
R	D	E	N
E	M	E	D
İ	R	X	X

Şifreli metin

Şifreli metin; sütunların okunmasıyla
“**BREİUDMRBEEEXİNDX**” olacaktır.

Şifreleme Algoritmalarına Örnekler



✓ Permutasyonlar

✓ **Frekans analizi**, bir alfabede harflerin **kullanım sıklığına göre** yapılan değerlendirmedir. Yani şifrelenmiş metinde en çok kullanılmış harf belirlenir ve bu harf kullanılan dilde en çok kullanılan frekansı en yüksek harfle eşleştirilerek, düz metin bulunmaya çalışılır.

✓ Bu şifreli metin frekans analizi ile çözülmeye çalışıldığında dildeki frekans ile örtüşecektir.



Basit Şifreleyiciler

Şifreleyiciler (Cipherlar)

Normal yazılışlı harfleri değiştirme operasyonunu kapsar



- ☐ Metni ters çevirmek (Message Reversal)
- ☐ Geometrik yöntemler (Geometrical Patterns)
- ☐ Yolu değiştirme (Route Transposition)
- ☐ Yol değişiklikleri (Route Variations)
- ☐ Dikey değiştirme (Columnar Transposition)
- ☐ Dikey değiştirme yöntemi (Other Transposition)
- ☐ Çifte dikey değiştirme (Double Columnar Transposition)
- ☐ Çok harfli değiştirme (Poly Literal Transposition)
- ☐ İşaret sözcüğünün değiştirilmesi (Code Word Transposition)

Metni Ters Çevirme (Message Reversal)



- Düz bir metni basit olarak şifrelemek için kullanılır.
- Düz metin tersten yazılır.
- *"Gazi Üniversitesi"* tersi yani *"İsetisrevinü izaG"* şifreli metin elde edilir.
- Tersiyile düz metin elde edilir.

Geometrik Yöntemler (Geometric Patterns)



- Düz metin soldan sağa ve satır satır yazılır.
- Böylece mesajlar dikdörtgen şeklinde oluşturulur.

Örnek: “GAZİ ÜNİVERSİTESİ”

(1) Düz metin dikey iki sütün halinde yazabiliriz:

GE
AR
ZS
İİ
ÜT
NE
İS
Vİ

Düz metin yatay olarak eşit uzunlukta iki satır halinde yazılır:

(2) GEAR ZSİİÜTNEİSVİ

Yol Değiştirme (Route Transposition)



- Yolu değiştirme metodu ek karıştırma sağlar.
- Soldan sağa yazma yolunu kullanırsa

Örneğin: (16 Karakter) (8x2 matris oluşturulur.)

GAZİ ÜNİVERSİTESİ (Düz Metin)

GA

Zİ

ÜN

İV

ER

....

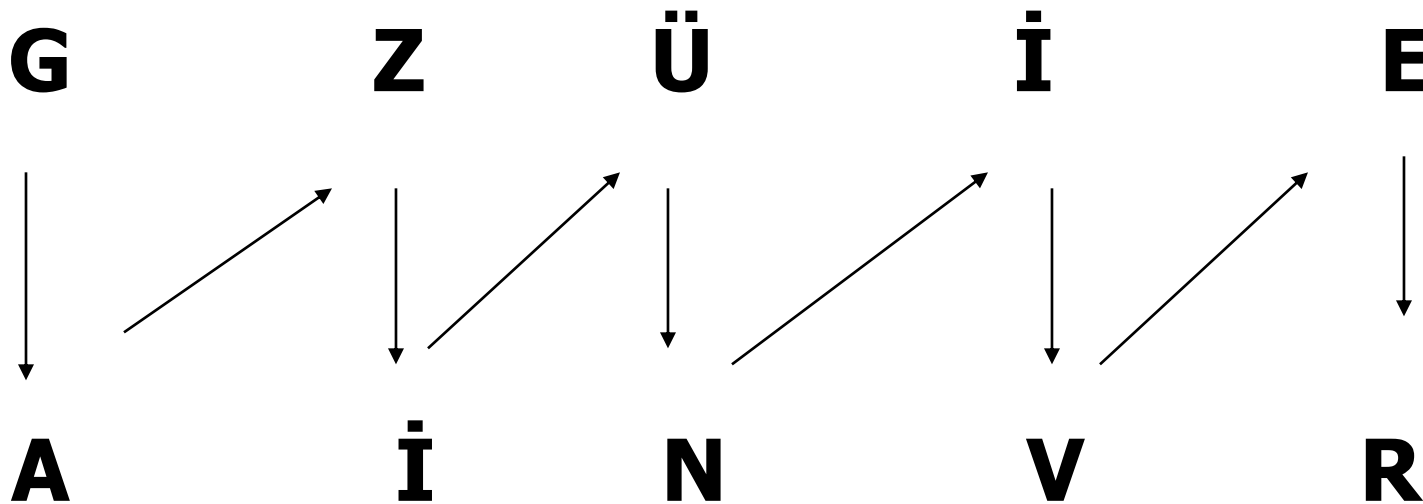
- **GZÜİEG.. AİNVR..** (Şifreli Metin)

Yolu Değiştirme (Route Transposition)



- Eğiri yolu değiştirme, ZIG-ZAG veya Parmaklık metodu

GAZİ ÜNİVERSİTESİ "GZÜİE.. AİNVR..."



Yol Değişimleri (Route Variations)



- Farklı yönler olabilir: yatay, dikey, saat akrebi yönü veya saat akrebinin tersi.

Örneğin, “gel git dur”

Yatay metotları

- 1. gel başlama**
 git
 dur
- 2. leg**
 tig
 rud

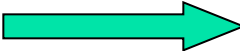
Yol Değişimleri (Route Variations)



- Farklı yönler olabilir: yatay, dikey, saat akrebi yönü veya saat akrebinin tersi.

Örneğin “gel git dur”

Yatay metotları

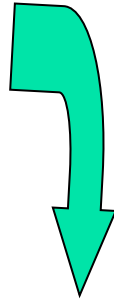
1. gel
git
dur  başlama
2. leg
tig
rud 

Yol Değişimleri (Route Variations)



■ Dikey metotlar (gel git dur)

1. ggd
eiu
ltr
2. dgg
uie
rtl



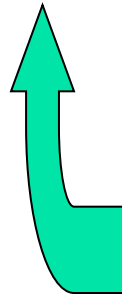
□ Saat akrebi yönü

1. Send
oonh
sple
2. elps
hnoo
dnes



■ Çapraz metotlar (send help soon)

1. sedl
nhpo
eson
2. nose
ophn
ldes



□ Saat akrebi tersi

1. sosp
eonl
ndhe
2. ehdn
lnoe
psos



Dikey Değiştirme (Columnar Transposition)



- Dikey değişiklik yapılır
- Düz metin dikdörtgen şekline getirilir ve dikey metot uygulanır.

“SHIP EQUIPMENT ON THE FOURTH OF JULY”

Sütun numarası

1	2	3	4	5
S	U	T	F	O
H	I	O	O	F
I	P	N	U	J
P	M	T	R	U
E	E	H	T	L
Q	N	E	H	Y

Dikey Değiştirme (Columnar Transposition)



Sütun numarası				
5	4	3	2	1
T	O	F	U	S
O	F	O	I	H
N	J	U	P	I
T	U	R	M	P
H	L	T	E	E
E	Y	H	N	Q

- Parolalı metin (Cipher Text)
- Düz metin ek bir güvenlik sağlayabilmek için değiştirilen metin 5 grup halinde yazılır (yatay ve beşer harf)
- SHIP EQUIPMENT ON THE FOURTH OF JULY Düz metin
- TOFUS OFOIH NJUPI TURMP HLTEE EYHNQ Şifreli metin

Dikey Değiştirme (Columnar Transposition)



Açık metin:

Negotiations stales send instructions today

Düz metin, dört sütun şeklinde:

N	N	E	T
E	S	N	I
G	S	D	O
O	T	I	N
T	A	N	S
I	L	S	T
A	L	T	O
T	E	R	D
I	D	U	A
O	S	C	Y

Çifte Dikey Değiştirme (Double Columnar Transposition)



- Anahtarın birinci numarasını (4213) kullanarak aşağıdaki düz metin değiştirilir.

Sütun yerleri anahtarı

1	2	3	4
4	2	1	3
T	N	N	E
I	S	E	N
O	S	G	D
N	T	O	I
S	A	T	N
T	L	I	S
O	L	A	T
D	E	T	R
A	D	I	U
Y	S	O	C

- Anahtarın ikinci numarasını (5926) kullanarak aşağıdaki sütunların değişmesi sağlanır.

Sütun yerleri anahtarı

5	9	2	6
2	4	1	3
N	E	T	N
S	N	I	E
S	D	O	G
T	I	N	O
A	N	S	T
L	S	T	I
L	T	O	A
E	R	D	T
D	U	A	I
S	C	Y	O

Çifte Dikey Değiştirme (Double Columnar Transposition)

- Double Transposition consists of two applications of columnar transposition to a message. The two applications may use the same key for each of the two steps, or they may use different keys.
- Columnar transposition works like this: First pick a keyword, such as **DESCRIBE**, then write the message under it in rows:

```

D E S C R I B E
-----
Y O U R M O T H
E R W A S A H A
M S T E R A N D
Y O U R F A T H
E R S M E L T O
F E L D E R B E
R R I E S

```

number the
letters in the
keyword in
alphabetical
order.



```

3 4 8 2 7 6 1 5
D E S C R I B E
-----
Y O U R M O T H
E R W A S A H A
M S T E R A N D
Y O U R F A T H
E R S M E L T O
F E L D E R B E
R R I E S

```

read the cipher off by columns, starting with the lowest-numbered column: Column 1 is THNTTB, followed by RAERMDE.. Next, select and number a second keyword, and write this intermediate ciphertext under it in rows:

```

2 7 1 8 9 5 4 6 3
C O A S T L I N E
-----
T H N T T B R A E
R M D E Y E M Y E
F R O R S O R E R
H A D H O E O A A
A L R M S R F E E
S U W T U S L I

```



take it off by columns
again and put it into
five-letter groups for
transmission.

```

NDODR WTRFH ASEER AERM R OFLBE OERSA YEA EI
HMRAL UTERH MTTYS OSU

```

Çok Harfli Değişirme (Poly Literal Transposition)



- İki harften oluşan bir birim kullanarak düz metinden, dört sütundan oluşan bir metot oluşturabiliriz.

“NEGOTIATIONS STALLED SEND INSTRUCTION TODAY”

Aşağıdaki gibi:

1	2	3	4
NE	NS	EN	TI
GO	ST	DI	ON
TI	AL	NS	ST
AT	LE	TR	OD
IO	DS	UC	AY

- Sütunları 4321 düzenine çevirerek veya şifre olarak (LIFE) sözcüğünü kullanarak gerekli değişikliği yaparız.

Çok Harfli Değişirme-tersten (Poly Literal Transposition)



4	3	2	1
TI	EN	NS	NE
ON	DI	ST	GO
ST	NS	AL	TI
OD	TR	LE	AT
AY	UC	DS	IO

- Bilgileri yatay olarak üçer birimler (altı harf) şeklinde alarak parolalı metnin son şekli aşağıdaki gibi olacaktır.

Düz metin :

NEGOTIONS STALLED SEND INSTRUCTIONS TODAY

Şifreli metin:

TIENNSNE ONDISTGO STNSALTI ODTRLEAT AYUCDSIO

Şifre Kelime Değiştirme (Code Word Transposition)



- **Düz metin sözcüklerinin sembolleştirme sözcüklerine sahip olduğunu varsayalım**

Sembolleştirme sistemi

düz metin

JMXY

KEWB

LSRB

MLMA

NMBB

Düz metin

INSTRUCTION

NEGOTIATIONS

SEND

STALLED

TODAY

- **Düz metin ve sembolleştirilmiş mesaj metin aşağıdaki şekilde olacaktır:**

Düz metin : NEGOTIATIONS STALLED SEND INSTRUCTIONS TODAY

Sembolleştirme sistemi metni: KEWB MLMA LSRB JMXY NMBB

Şifre Kelime Değiştirme (Code Word Transposition)



- Beş sütun şeklinde iki harfli birimler oluşturduğumuzda, aşağıdaki diziyi elde ederiz:

1	2	3	4	5
KE	ML	LS	JM	NM
WB	MA	RB	XY	BB

- Sütunların yerini gösteren (31524) sayılı anahtarı kullanarak işlem yapacak olursak sonuç:

3	1	5	2	4
LS	KE	NM	ML	JM
RB	WB	BB	MA	XY

Yerdeğiştirme ile Şifreleme (Substitution Cipher)



- ❑ Parola olarak MORS Sembolleri
(MORSE Code As A cipher)
- ❑ Numaralı Şifreleme (Number Cipher)
- ❑ Ters Şifreleme (Reciprocal Ciphers)
- ❑ CAESAR Ciphers

Mors Alfabeti (Moros Cipher)



- Sembolleştirme bir mors sembolleştirme sistemidir. Bu sistemde hece harfleri yerine başka semboller kullanılır. Sembolleştirme sistemi aşağıdaki şekilde gösterilmektedir:

A	._	J	._ _ _	S	...
B	_...	K	_._	T	_
C	_._.	L	._..	U	.._.
D	.._	M	_ _	V	..._
E	.	N	_..	W	._ _
F	_ _ _ .	O	_ _ _	X	_.._
G	_.	P	._ _.	Y	._ _ _
H		Q	_ _ _.	Z	_ _ ..
I	..	R	._.		

Mors Alfabeti

(MORSE Code As A Cipher)



- Hece harflerinden her birini, nokta ve tirelerden oluşan karşılayıcı karşılamaktadır. MORSE CODE TERİMİ yanlış isim demektir. Gerçek sembolleştirme (code) sisteminde, düz metindeki her kelime sembolleştirme sistemi ile örtüşmesi gerekmektedir. Harflarin yerine Mors sembollerini yerleştirerek düz metin şifrelenir.

Düz metin : CHANGE CIPHER KEY

Şifreli metin : _._. _ _" _' . _._' " _._' _.'
_-' . _-_-

Not: Mors sembollerini kullanırken, boşluklar bırakmak gerekir.

Numaralı Şifreleme (Number Cipher)



- Direk ve basit karşılayıcı şifreleme yöntemi, hece harfleri numara yerini belirlemeyi içermektedir, ancak bir mesaj veya metni şifrelemek için, metindeki her harfi karşılayacak bir numara yerini belirlemeyi içermektedir. Örneğin:

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

Açık metin : T H I N K S E C U R I T Y
PAROLAŞMIŞ METİN : 25 20 9 18 21 3 5 19 11 14 9 8 20

Numaralı Şifreleme (Number Cipher)



- Bu sistemde, sayı değiştirilir ve diğer sistem olarak değerlendirilir.
- Örneğin bu sistemde (A) harfi için (65), (B) harfi için (66)

A	65	J	74	S	83
B	66	K	75	T	84
C	67	L	76	U	85
D	68	M	77	V	86
E	69	N	78	X	87
F	70	O	79	Y	88
G	71	P	80	Z	89
H	72	Q	81		
I	73	R	82		

Açık metin : *S E C R E T C O M M U N I C A T I O N*

Parolalı metin : *83 69 67 82 69 84 67 79 77 77 85 78 73 67 65 84 73 79 78*

Ters Şifreler (Reciprocal Cipher)



- Şifreli metni elde edebilmek, açık metindeki hece harflerini ters çevirmek yolu ile mümkündür. Bu tür karşılıyıcı ters bir karşılıyıcıdır (Reciprocal)

Açık metin ABCDEFGHIJKLMNOPQRSTUVWXYZ
Şifreli metin ZYXWVUTSRQPONMLKJIHGFEDCBA

Bu örnekte

(Z) harfi (A) harfi yerine, (Y) harfi yerine (B) harfi yerine, (S)
yerini (H), (E) yerini (V), (N) yerini (M), (D) yerine (W).....vb.

Açık metin *SEND GUNS SOON*
Parolalı metin *HVMW TFMH HLLM*

Sezar Şifresi (Caesar Cipher)



- Caesar cipher'da, açık metindeki hece harflerini üç mertebe veya istediğimiz kadar kaydırırız.
- $P = D(C) = (C - 3) \text{ MOD } (26)$

Örneğin, aşağıdaki metni üç mertebe kaydırılmış

Açık metin : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Şifreli metin: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Açık metin : SECURE ALL MESSAGES

Parolalı metin : VHFXUH DOO PHVVDJHV

Açık metinde: ALL kelimesi üç harf kaydırılarak (A) harfi (D) harfi ile, (L) harfi (O) harfi ile değiştirilmiştir.

Genel Sezar Şifresi (Caesar Cipher)



- Caesar cipher'da, açık metindeki hece harflerini üç mertebe veya istediğimiz kadar kaydırırız.
- $P = D(C) = (C - K) \text{ MOD } (26)$

Örneğin, aşağıdaki metni üç mertebe kaydırılmış

Açık metin : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Şifreli metin: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Açık metin : SECURE ALL MESSAGES

Parolalı metin : VHFXUH DOO PHVVDJHV

Açık metinde: ALL kelimesi üç harf kaydırılarak (A) harfi (D) harfi ile, (L) harfi (O) harfi ile değiştirilmiştir.