

Temel Şifreleme Yöntemleri

Kriptoloji

Geleneksel Şifreleme Yöntemleri

- **Vigenere Cipher**

- Temelde mantık aynı ama bu sefer elimizde Vigenere tablomuz var. Buna ek olarak birde rastgele oluşturduğumuz bir anahtar kelime sayesinde güvenliği artırmış olacağız

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

Vigenere Cipher

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

Açık Metin=teknoloji

Şifreli Metin=trkuhlfjv

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

Açık Metin: GOLYAKA

Şifreli metin: qswgmok

Geleneksel Şifreleme Yöntemleri

- **Vigenere Cipher Other**

- Mono alfabetik yerine koymalı şifreleme yöntemlerindedir. Şifrelemede öncelikle kullanılacak alfabenin her harfine karşılık gelecek sayısal değerler atanır.

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

Şifreleme

Harf	Index
t	18
e	4
k	9
n	12
o	13
l	10
o	13
j	9
i	8

Anahtar

Harf	Index
G	6
U	19
N	12
A	0
Y	23

Açık Mesaj

Index	Mod	Şifreli Index	Harf
$18+6=24$		24	Z
$4+19=23$		23	Y
$9+12=21$		21	W
$12+0=12$		12	N
$13+23=36$	$36 \bmod 25 = 11$	11	M
$10+6=16$		16	R
$13+19=32$	$32 \bmod 25 = 7$	7	h
$9+12=21$		21	W
$8+0=8$		8	i

Şifreli metin=zywnmrhwi

Deşifreleme

Harf	Index
z	24
y	23
w	21
n	12
m	11
r	16
h	7
w	21
i	8

Anahtar

Harf	Index
G	6
U	19
N	12
A	0
Y	23

Şifreli Mesaj

Index	Mod	Şifreli Index	Harf
$24-6=18$		18	t
$23-19=4$		4	e
$21-12=9$		9	k
$12-0=12$		12	n
$11-23=-12$	$-12+25=13$	13	o
$16-6=10$		10	l
$7-19=-12$	$-12+25=13$	13	o
$21-12=9$		9	j
$8-0=8$		8	i

Açık metin=teknoloji

BITTİ