ŞİFRELİ METİNLER OLUŞTURMA

Şifreleme ya karakteri değiştirerek ya da yerini kaydırarak yapılır, bunun için de bir yöntem ve anahtarı şarttır.
Kriptolojinin temelini oluşturan yöntemler

1. Yerine Koyma (Substitution): Harflerin sabit veya değişken sembollerle değiştirilmesidir.

2. Yer Değiştirme (Transposition): Metindeki karakterlerin sırasının belirli bir düzenle karıştırılmasıdır.

Temel Bileşenler: Herhangi bir şifreleme işlemi için mutlaka bir **algoritma** ve bir **anahtar** gereklidir.

Simetrik Yaklaşım: Görselde belirtilen tek anahtarlı sistem, verinin hem şifrelenmesi hem de çözülmesi için aynı anahtarın kullanıldığı yöntemi temsil eder.

TEK ANAHTARLI ŞİFRELEMEDE

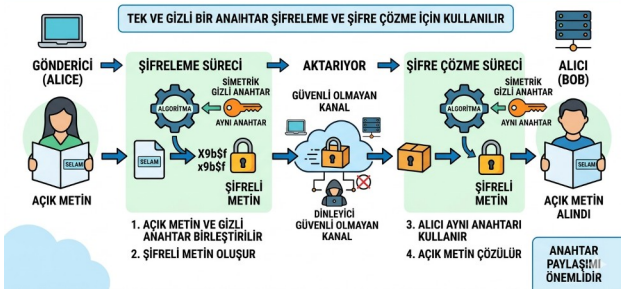
Aynı anahtar hem kapıyı kilitlemek hem de açmak için kullanılır. İşin mantığını üç kısa şu şekilde özetleyebiliriz:

Tek Sır: Hem gönderici hem de alıcı, aynı gizli anahtara (şifreye) sahiptir.

Hız: Bu yöntem çok hızlıdır. Büyük verileri şifrelemek için birebirdir.

Güvenlik Riski: En büyük "olay" anahtarı paylaşmaktır. Anahtarı karşı tarafa gönderirken anahtarı ele geçiren herkes mesajı okuyabilir.

TEK ANAHTARLI (SİMETRİK) ŞİFRELEME: SÜREÇ GÖRSELLEŞTİRMESİ



Bu yöntemin en bilinen modern örneği **AES** (Advanced Encryption Standard) algoritmasıdır; bugün bankacılık işlemlerinden WhatsApp mesajlarına kadar pek çok yerde arka planda bu sistem çalışır.

Yeni şifreler üretilirken kullanılan algoritmalar şifrelerin nasıl deşifre edilebileceğini de belirlemektedir.

Günümüzde şifreleme algoritmalarının güvenliği ve yapısı şu temel nedenlerle kritik öneme sahiptir:

Güvenlik Standartları: Bir şifrenin ne kadar zor çözüleceği ve nasıl deşifre edileceği, kullanılan algoritmanın karmaşıklığına bağlıdır.

Veri Gizliliği: İnternet üzerindeki işlemlerin artmasıyla birlikte, kişisel mahremiyeti korumanın en temel yolu güçlü şifreleme yöntemleridir.

Siber Savunma: Bilgisayar korsanlığı ve siber zorbalık gibi tehditlere karşı en etkili kalkan, teknolojik gelişmelere uyum sağlayan dayanıklı algoritmalardır.

Özetle; dijital dünyada güvenli bir iletişim ve işlem süreci, ancak siber saldırılara dirençli, sağlam matematiksel temellere dayanan algoritmalarla mümkündür.

Örnek...1 :

"BİR ELİN NESİ VAR, İKİ ELİN SESİ VAR." cümlesi, karakter değiştirme yöntemiyle şu şekilde şifrelenmiştir:
"FNUCJQNŞCSJXNCBFYÇCNPNPCJQNŞCXJXNCBFYD"

Noktalama işaretleri ve boşluklar birer karakter kabul edilerek şifrelemeye dahil edilmiştir (Şifreli metin ve gerçek metindeki karakter sayıları, noktalama işaretleri ve boşluklarla birlikte toplandığında 37 karakter olduğuna dikkat ediniz)
Buna göre;

1. Şifreleme anahtarını (eşleşmeleri) bulunuz.
2. "GÜL" kelimesi bu şifreleme mantığına göre nasıl yazılır?

Şifreleme yöntemi olarak her karakter, set içindeki sırasına göre 5 birim sağa kaydırılmaktadır. (Setin sonuna gelindiğinde başa dönülmektedir.) [cebirsel olarak ifade edersek f(x)=x+5 mod 33] İşin içine boşluk, virgül ve noktayı da birer "karakter" olarak dahil ettiğimizde, bu artık sadece bir alfabe kaydırması değil, bir karakter seti (string) kaydırması olur.

İndeks	Karakter	İndeks	Karakter	İndeks	Karakter	İndeks	Karakter
0	A	8	Ğ	16	N	24	T
1	B	9	H	17	O	25	U
2	C	10	I	18	Ö	26	Ü
3	Ç	11	İ	19	P	27	V
4	D	12	J	20	R	28	Y
5	E	13	K	21	S	29	Z
6	F	14	L	22	Ş	30	[Boşluk]
7	G	15	M	23	T	31	,
32	.						

2. "GÜL" Kelimesinin Dönüşümü:

- **G (7)** → 12 **(J)**
- **Ü (26)** → 31 **(,)** *(Vay be, harf virgüle dönüştü!)*
- **L (14)** → 19 **(P)**

Sonuç: "J,P"

Örnek...2 :

Şifreli bir yazışmada kullanılan Latin alfabesindeki harfler alfabetik sıralamaya göre 2'den 30'a kadar numaralandırılır. Daha sonra bu sayısal değerler asal çarpanlarına ayrılır ve kullanılan metin aşağıda açıklanan yöntemle şifrelenir:

- Harflerin sayısal karşılıkları yazılır.
- Yazılan sayılar asal çarpanlarına ayrılır. Asal çarpanları küçükten büyüğe göre soldan sağa doğru çapım biçimde yazılarak sayılar ifade edilir.
- Her bir asal çarpanın kuvveti yanına yazılarak harfin şifreli karşılığı oluşturulur.
- Her iki harf arası bir boşluk bırakılır

Örneğin Pİ kelimesi

P	21	$3^1 7^1$	3171
İ	13	13^1	131

ve bu şekilde Pi kelimesinin şifrelenmiş hali 3171 131 dir. Buna göre "PEYNİR" kelimesini şifreleyiniz

Harfler 2'den başlayarak numaralandırılır ve asal çarpanlarının kuvvetlerine göre kodlanır.
(Not: Latin alfabesi sıralamasına göre A=1 B=2 ile başlayan eşleştirmede P:20, E:6, Y:28, N:17, İ:12, R:21 oluyordu. her değere 1 ekler yeni harf sayı

P:21, E:7, Y:29, N:18, I:13, R:22.

P=3 7 → 3171 E=7 → 71 Y=29 → 291 N=17 → 171 İ=13 → 131 R=22=2 11 → 21111

PEYNIR = 3171 71 291 171 131 21111 olarak şifrelenir

Örnek...3 :

Haldun Öğretmen, öğrencisi Barkut'tan sözel bir metni sayılarla anlamlı bir şekilde şifrelemesini istemiştir.

Barkut öncelikle

A	B	C	...	K	...	Y	Z
1	2	3		14		28	29

olarak sıralı bir şekilde harfleri sayılara dönüştürmüş ardından bu sayıları 3'ün farklı doğal sayı kuvvetlerinin toplamı şeklinde ifade etmiştir. Örnek olarak da kendi adında geçen K harfi için 14 sayısını kullandığını belirtmiş ve $14=0\cdot3^3+1\cdot3^2+1\cdot3^1+2\cdot3^0$ olduğundan için 0112 4 basamaklı saysını oluşturmuştur.

Barkut kelimeleri şifrelerken her harften sonra bir boşluk bıraktığına göre, aynı yöntemle "MATBAZ" kelimesi nasıl şifrelenir.

Soruda verilen formata göre her sayıyı $a\cdot3^3+b\cdot3^2+c\cdot3^1+d\cdot3^0$ şeklinde yazıp katsayıları $(abcd)$ yan yana getireceğiz. $(3^3=27, 3^2=9, 3^1=3, 3^0=1)$

- **M (16):** $0\cdot27+1\cdot9+2\cdot3+1\cdot1 \rightarrow$ **0121**
- **A (1):** $0\cdot27+0\cdot9+0\cdot3+1\cdot1 \rightarrow$ **0001**
- **T (24):** $0\cdot27+2\cdot9+2\cdot3+0\cdot1 \rightarrow$ **0220**
- **B (2):** $0\cdot27+0\cdot9+0\cdot3+2\cdot1 \rightarrow$ **0002**
- **A (1):** (Yine aynı) $\rightarrow$ **0001**
- **Z (29):** $1\cdot27+0\cdot9+0\cdot3+2\cdot1 \rightarrow$ **1002**

Dolayısıyla MATBAZ 0121 0001 0220 0002 0001 1002 olarak sifrelenir

Örnek...4 :

"SICAK ÇORBA" söz öbeğini :

a) metindeki harfler sol baştan sıralandığında, tek sıradaki harfleri alfabede beş ileri, çift sıradaki harfleri alfabede üç geri kaydırarak metni şifreleyiniz. Türk alfabesi ve A=1 B=2 ,...Z=29 ve mod 29 kullanılarak a ve b şıkları yapılmıştır.

b) n, metindeki harflerin sayısal karşılığı olmak üzere, $5\cdot n-3$ ün 29 ile bölümünden kalan şeklindeki örüntüyü kullanarak şifreleyiniz

c) Metnin harfleri 2x5'lik bir tabloya yukarıdan aşağıya, satır tamamlanınca sıradaki sütudan devam ederek yazdıktan sonra tablodaki harfleri satır sırasıyla soldan sağa doğru sıralayıp yazarak metni şifreleyiniz.

a) tabloyu inceleyiniz. Cevap: VGGVÖ AŞOFV

Sıra	Harf	İşlem	Yeni Sıra No	Şifreli Harf
1 (Tek)	S (22)	22 + 5	27	V
2 (Çift)	I (11)	11 - 3	8	G
3 (Tek)	C (3)	3 + 5	8	G
4 (Çift)	A (1)	1 - 3 (Mod 29)	27	V
5 (Tek)	K (14)	14 + 5	19	Ö
6 (Çift)	Ç (4)	4 - 3	1	A
7 (Tek)	O (18)	18 + 5	23	Ş
8 (Çift)	R (21)	21 - 3	18	O
9 (Tek)	B (2)	2 + 5	7	F
10 (Çift)	A (1)	1 - 3 (Mod 29)	27	V

b) tabloyu inceleyiniz. Cevap: PŞİBĞ NZLFB

Kural: Harfin alfabedeki sırası n olmak üzere, şifreli harf şudur:

$$f(n) = (5n - 3) \pmod{29}$$

- **S (22):** $5 \cdot 22 - 3 = 107 \rightarrow 107 = (29 \cdot 3) + 20 \rightarrow$ **P**
- **I (11):** $5 \cdot 11 - 3 = 52 \rightarrow 52 = (29 \cdot 1) + 23 \rightarrow$ **Ş**
- **C (3):** $5 \cdot 3 - 3 = 12 \rightarrow$ **İ**
- **A (1):** $5 \cdot 1 - 3 = 2 \rightarrow$ **B**
- **K (14):** $5 \cdot 14 - 3 = 67 \rightarrow 67 = (29 \cdot 2) + 9 \rightarrow$ **Ğ**
- **Ç (4):** $5 \cdot 4 - 3 = 17 \rightarrow$ **N**
- **O (18):** $5 \cdot 18 - 3 = 87 \rightarrow 87 = (29 \cdot 3) + 0$ (veya 29) $\rightarrow$ **Z**
- **R (21):** $5 \cdot 21 - 3 = 102 \rightarrow 102 = (29 \cdot 3) + 15 \rightarrow$ **L**
- **B (2):** $5 \cdot 2 - 3 = 7 \rightarrow$ **F**
- **A (1):** $5 \cdot 1 - 3 = 2 \rightarrow$ **B**

Şifreli Metin: PŞİBĞ NZLFB

b şıkkında A=0 B=1,.. Z=28 ve mod 29 kullanılırsa elde edilecek şifre MÖGVD JUICV olacaktır.

c) tabloyu inceleyiniz. Cevap: SCKOB IAÇRA

Sütun 1	Sütun 2	Sütun 3	Sütun 4	Sütun 5
S	C	K	O	B
I	A	Ç	R	A

Örnek...5 :

"KISKANMAK" kelimesini "MÜKÜ" anahtarıyla Vigenere tipi şifrelemeyle şifreleyiniz.

Bu bir Vigenere (çok alfabeli) şifrelemedir. Kelimenin altına anahtar tekrar ederek yazılır:

K I S K A N M A K

M Ü K Ü M Ü K Ü M

Her harf çifti (örneğin K+M), alfabedeki sıralarının toplamının 29 ile bölümünden kalan yeni harfe dönüştürülür. A=0, B=1, C=2,....Z=28
tabloya göre cevap ZFEHMJZÜZ olacaktır. Hesaplamaları inceleyiniz.

Açık Metin (M)	Değer	Anahtar (A)	Değer	İşlem (M+A)	(mod29)	Şifreli Harf
K	13	M	15	13+15 = 28	28	Z
I	10	Ü	25	10+25 = 35	6	F
S	21	K	13	21+13 = 34	5	E
K	13	Ü	25	13+25 = 38	9	H
A	0	M	15	0+15 = 15	15	M
N	16	Ü	25	16+25 = 41	12	J
M	15	K	13	15+13 = 28	28	Z
A	0	Ü	25	0+25 = 25	25	Ü
K	13	M	15	13+15 = 28	28	Z

UYARI: hem matematiksel tutarlılık hem anlaşılırlığı açısından şifreleme yaparken Türk alfabesine göre A=0, ...,Z=28 mod 29 hesabı A=1, B=2,....,Z=29 mod 29 hesabından hem daha mantıklı hem daha sağlamdır. A=1 den başlarsak Z=29 olur ama bu mod 29 için aslında 0 demektir. böyle olması listenin A ile mi Z ile mi başladığı konusunda kafa karıştırıcı olabilir.

Anahtar tabanlı ve çok alfabeli şifreleme sistemlerinin temel mantığını özetlersek:

Çoklu Eşleşme: Klasik yöntemlerin aksine, anahtar kullanılan sistemlerde bir harfin tek bir karşılığı yoktur; aynı harf metin içinde farklı karakterlere dönüşebilir.

n-Kadar Çeşitlilik: Anahtarın uzunluğu (n) kaç birimse, bir harf o kadar farklı şekilde şifrelenebilir. Bu da sistemin tek bir alfabe yerine birçok farklı alfabe kullanması demektir.

Anahtar Uzunluğu = Güvenlik: Kullanılan anahtar ne kadar uzun ve karmaşıksa, şifrenin çözülmesi (kırılması) o kadar zorlaşır.

Esnek Algoritma: Şifreleme ve deşifreleme süreci tamamen gönderici ile alıcı arasındaki özel anlaşmaya (algoritmaya) göre şekillenir.

Sabit bir şifre alfabesi yerine, anahtarın uzunluğu ve yapısı sayesinde her harfe dinamik bir kimlik kazandırılır; bu da siber güvenliğin temel taşlarından biridir

SON NOT : Hem matematiksel tutarlılık hem anlaşılırlığı açısından şifreleme yaparken Türk alfabesine göre A=0, ...,Z=28 mod 29 hesabı A=1, B=2,....,Z=29 mod 29 hesabından hem daha mantıklı hem daha sağlamdır. A=1 den başlarsak Z=29 olur ama bu mod 29 için aslında 0 demektir. böyle olması listenin A ile mi Z ile mi başladığı konusunda kafa karıştırıcı olabilir.

Kısaca A=1 ile başlayınca , hesaplama sonucu modül 0 a eşit çıktığında ama A=1 alfabesinde **0 diye bir harf olmaması , duruma "sonuç sıfır çıkarsa Z ye eşitle" diye ekstra kural koymamızı gerektirir.** (Z Problemi) (UYARI CLAUDE AI)

Dolayısıyla alfabetik şifreleme tablosu anahtarının A=0 mı A=1 ile mi başlayacağına sorunun başında dikkat etmek gerekir.

Not: Bu içeriklerin bir kısmının hazırlanmasında Gemini yapay zeka modeli kullanılmıştır. #YapayZekaİşbirliği #PoweredByGemini Bazı soruları beraber çözdük/oluşturduk: matbaz & Gemini