

## ŞİFRELİ METİNLER OLUŞTURMA

Şifreleme ya karakteri değiştirerek ya da yerini kaydırarak yapılır, bunun için de bir yöntem ve anahtar 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 şifrlenmesi 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" anahtarın paylaşılmasıdır. Anahtar karşı tarafa gönderirken anahtar ele geçiren herkes mesajı okuyabilir.

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 algoritmalarla sağlanır.

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 şifrenmiştir:  
"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?

## 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.

**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 çarpım biçiminde yazılarak sayılar ifade edilir.
- Her bir asal çarpanın kuvveti yanına yazılarak harfin şifreli karşılığı oluşturulur.
- Her iki harf arası bir boşluk bırakılır

Örneğin Pi 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

**Örnek...3 :**

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

Barkut öncelikle Türk alfabesine göre hazırlanmış örnek şifreleme anahtarı tablosunu oluşturmuş

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  $13=0 \cdot 3^3+1 \cdot 3^2+1 \cdot 3^1+1 \cdot 3^0$  olduğundan 14 için 0112 4 basamaklı sayısını oluşturmuştur. Barkut kelimeleri şifrelerken her harften sonra bir boşluk bıraktığına göre, aynı yöntemle "MATBAZ" kelimesi nasıl şifrelenir.

**Örnek...4 :**

"SICAK ÇORBA" söz öbeğini :

- metindeki harfler sol baştan sıralandığında, tek sıradaki harfleri alfabede beş ileri, çift sıradaki harfleri alfabede üç geri kaydırarak metni şifreleyiniz.
- n, metindeki harflerin sayısal karşılığı olmak üzere,  $5 \cdot n - 3$  ün 29 ile bölümünden kalan şeklindeki örüntüyü kullanarak şifreleyiniz
- Metnin harfleri  $2 \times 5$ 'lik bir tabloya yukarıdan aşağıya, satır tamamlanınca sıradaki sütundan devam ederek yazdıktan sonra tablodaki harfleri satır sırasıyla soldan sağa doğru sıralayıp yazarak metni şifreleyiniz.

(Türk alfabesi ve A=1 B=2 ,...Z=29 ve mod 29 hesabıyla a ve b şıkları yapılacaktır.)

**Örnek...5 :**

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

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 karmaşıkça, 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 anlaşılabilirliği açısından şifreleme yaparken Türk alfabesine göre  $A=0, \dots, Z=28 \text{ mod } 29$  hesabı  $A=1, B=2, \dots, Z=29 \text{ mod } 29$  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.