ŞİFRELİ METİNLER ÇÖZME

Kriptoloji, en basit tanımıyla verilerin güvenli bir şekilde saklanması ve iletilmesi sanatıdır; ancak bu sanatın kalbi tamamen **matematik** ile atar. Modern dünyada bir mesajın "kilitlenmesi" artık fiziksel kilitlerle değil, çözülmesi binlerce yıl sürecek karmaşık denklemlerle yapılır.

KRİPTOLOJİNİN KULLANIM ALANLARI

Günümüzde dijital ayak izimizin olduğu her yerde kriptoloji devrededir:

İnternet Güvenliği (SSL/TLS): Web sitelerinin başındaki o küçük kilit simgesi, tarayıcınız ile sunucu arasındaki verilerin matematiksel olarak şifrelendiğini gösterir.

Blokzincir (Blockchain) ve Kripto Paralar: Bitcoin ve diğer dijital varlıklar, işlemlerin güvenliğini ve doğruluğunu sağlamak için "Hash" fonksiyonları ve dijital imzalar kullanır.

Uçtan Uca Şifreleme: WhatsApp veya Telegram gibi uygulamalar, mesajların sadece gönderici ve alıcı tarafından okunabilmesini sağlamak için kriptolojik anahtar değişimi yapar.

Askeri ve Diplomatik Haberleşme: Devlet sırlarının ve stratejik hamlelerin düşman unsurlar tarafından ele geçirilmesini önlemek için en üst düzey algoritmalar kullanılır.

Elektronik İmza ve Bankacılık: ATM'den para çekerken veya dijital bir belgeyi imzalarken kimlik doğrulama işlemi kriptolojik protokollerle gerçekleştirilir.

1.SEZAR ŞİFRELEME ALGORİTMASI

Tarihin bilinen en eski ve en basit şifreleme yöntemlerinden biridir. Adını, askeri yazışmalarında bu yöntemi kullanan Roma İmparatoru Jül Sezar'dan alır.
Sezar Şifreleme yöntemi bir yer değiştirme (ikame) şifrelemesidir. Alfabedeki her harf, belirlenen sabit bir sayı kadar ileriye (veya geriye) kaydırılarak yeni bir harf oluşturulur.

Anahtar: Harflerin kaç birim kaydırılacağını belirleyen sayıdır.

Algoritma: Eğer anahtar 3 ise, "A" harfi yerine alfabedeki 3 sonraki harf olan "Ç" yazılır.

Amaç: Bilgiyi değil bilginin anlamını gizlemektir.

Örnek...1 :
Sezar Şifresi oluşturalım. Gizli mesajımız "MERHABA" ve anahtarımız (kaydırma sayımız) 3 olsun.
Alfabemizdeki harflerin sayısal karşılıkları için aşağıdaki tabloyu kullanarak adım adım kaydıralım

Alfabetik şifreleme anahtarı (Bu tablo diğer sorularda da lazım oldukça kullanılacaktır)

Tablo 1

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

- M + 3 → Ö
- E + 3 → Ğ
- R + 3 → T
- H + 3 → J
- A + 3 → Ç
- B + 3 → D
- A + 3 → Ç

Mesaj : MERHABA **Şifreli Mesaj**: ÖĞTJÇDÇ

Not : Şifreleme yapılırken Z harfinden sonra A harfine dönülmektedir yani elimizdeki durumda V+5 olsaydı bu şifrede C ile değiştirilecekti. (27+5=3 mod29, burada mod 29 demek toplama sonucu elde edilen sayının 29 ile kalanına eşitlemektir)

Sezar şifrelemesi günümüzde sadece bir hobi veya temel eğitim aracıdır ve güvenli kabul edilmez.
Çünkü:
1. Sadece 29 (veya İngiliz alfabesinde 26) farklı olasılık vardır; **deneme-yanılma** (Brute Force) ile saniyeler içinde çözülebilir.

2. **Frekans analizi** yapılarak (bir dilde en çok kullanılan harflerin tespitiyle) kolayca kırılabilir.

Örnek...2 :
Haldun Öğretmen, Sezar şifreleme yöntemini kullanarak tahtaya **"ZEKİ"** ismini **"ÇHOM"** olarak şifrelemiştir. Buna göre, Haldun Öğretmen aynı anahtarı (kaydırma sayısını) kullanarak **"METİN"** ismini nasıl şifreler?

Örnek...3 :
Kadir Öğretmen, öğrencilerinden Anıl ve Bora'nın isimlerini Sezar şifreleme yöntemi kullanarak "FŞNR " ve "GTVF" şeklinde şifreli olarak tahtaya yazmıştır.
Buna göre,
a) Şifreli isimlerin hangi isimden elde edildiklerini ve örüntülerini bulunuz.
b) Belirlenen örüntüleri cebirsel olarak genelleyiniz.

Örnek...4 :

Türk alfabesi kullanılarak şifrelenen bir metinde geçen şifreli "EMÖMP " kelimesi asıl kelimenin harflerinin n birim ileri kaydırılmasıyla elde edilmiştir. Şifreleme yapılırken Z harfinden sonra A harfine dönülmekte ve bu işlem döngüsel şekilde tekrarlanmaktadır.
Buna göre aşağıdaki soruları cevaplayınız.
Aşağıdaki tabloda her bir adım, şifreli "EMÖMP " kelimesindeki harflerin 1 birim geriye kaydırılması sonucu oluşan harfleri temsil etmektedir. Buna göre tablodaki boş hücreleri doldurarak şifrelenmiş kelimeyi bulunuz.
harflerin şifre karşılıklarını gösteren alfabe olan şifre alfabesini bulunuz.

	E	M	Ö	M	P
1.Adım					
2.Adım					
3.Adım					
4.Adım					

Örnek...5 :

Aşağıda bir sayı dizisinin ilk 6 terimi verilmiştir.

1.Terim	2.Terim	3.Terim	4.Terim	5.Terim	6.Terim
0	2	6	12	20	30

Buna göre, dizinin genel terimini bulunuz.

2.DOĞRUSAL ŞİFRELEME

Doğrusal şifreleme klasik kriptografide kullanılan, her harfin matematiksel bir fonksiyonla başka bir harfe dönüştürüldüğü bir yer değiştirme şifrelemesidir. Sezar şifrelemesinin biraz daha geliştirilmiş ve matematikselleştirilmiş hali olarak yorumlanabilir. Mantığı Nedir?
Bu sistemde alfabedeki her harfe bir sayı karşılığı verilir (Örn: A=0, B=1, ..., Z=28).
Şifreleme işlemi şu temel matematiksel formül ile yapılır:

E(x) = (ax + b) (mod m)

x: Şifrelenecek harfin sayısal değeri.
a ve b: Anahtarlarımız.
m: Alfabedeki harf sayısı (Türkçede 29).
(mod m): Modül işlemi (bölümden kalan sayı).

Önemli Notlar

1. a sayısının, alfabe boyutu (m) ile aralarında asal olması gerekir. Aksi takdirde farklı harfler aynı harfe dönüşebilir ve şifre çözülemez.

2. Sezar şifrelemesinde anahtar sadece bir "kaydırma" miktarıyken, doğrusal şifrelemede anahtar aslında bir **doğru denklemidir**.

3.Sezar şifrelemesinde a değeri her zaman 1'dir. Yani sadece x+b işlemi yapılır. Doğrusal şifrelemede ise harfler sadece yer değiştirmez, aynı zamanda alfabeye "saçılarak" aralarındaki mesafe de değişir. Örneğin, Sezar'da "A" ve "B" ardışık geliyorsa, şifrelendiklerinde de ardışık kalırlar (Örn: "D" ve "E"). Ancak doğrusal şifrelemede çarpan (a) devreye girdiği için yan yana olan iki harf, şifreli metinde birbirinden çok uzak yerlere düşebilir. Bu da şifrenin basit yöntemlerle (frekans analizi hariç) çözülmesini zorlaştırır.

Örnek...6 :

"CAN" kelimesini doğrusal şifrelemeyle istiyoruz.

- Alfabe: A=0, B=1, C=2, ..., N=16...,Z=25 (Basitleştirmek için İngiliz alfabesini ve m=26 baz alalım).

- Anahtarlarımız: a = 5 ve b = 8 olsun. Yani $a \cdot x+b=5 \cdot x+8$ ve sırasıyla,

1. "C" Harfi İçin (x=2):
$(5 \cdot 2 + 8) = 18 \mod 26$ 18. harf "S" olur.
2. "A" Harfi İçin (x=0):
$(5 \cdot 0 + 8) = 8 \mod 26$ 8. harf "I" olur.
3. "N" Harfi İçin (x=13):
$(5 \cdot 13 + 8) \} = (21 \mod \{26\})$ 21. harf "V" olur.

Sonuç: "CAN" kelimesi "SIV" haline geldi.

Şifre Nasıl Çözülür?

Şifreyi çözmek için formülü tersine çeviririz:
$D(x) = a^{-1}(x - b) \mod m$

- x: Şifreli metindeki harfin sayısal değeri.
- a ve b: Şifreleme sırasında kullanılan anahtarlar.
- m: Kullanılan alfabedeki toplam harf sayısı (Türkçe için 29, İngilizce için 26).
- a-1: a sayısının m moduna göre modüler çarpma tersi.

Yani şifreyi çözmek için sadece anahtarları bilmek yetmez, biraz modüler aritmetik bilgisi de gerekir.

Özetle Doğrusal Şifreleme

- Basittir: Sadece çarpma ve toplama kullanır.
- Zayıftır: Modern bilgisayarlar için saniyeler içinde kırılabilir (çünkü anahtar alanı çok dardır).
- Matematikseldir: Kriptografinin temel mantığını anlamak için harika bir örnektir

Örnek...7 :

Bir kriptoanalist, ele geçirdiği şifreli bir metinde Türkçedeki en sık kullanılan kelimelerin ve harf dizilerinin peşine düşer. Yapılan analizler sonucunda, metinde çok sık tekrar eden üç kelimenin şifreli karşılıkları şu şekilde eşleştirilmiştir:

- "BU" kelimesinin şifreli karşılığı "JC"
- "EN" kelimesinin şifreli karşılığı "HĞ"
- "ÇOK" kelimesinin şifreli karşılığı "ÜAÇ"

Kullanılacak Alfabe: (29 harfli Türk alfabesi cetveli: A=1, B=2, ..., Z=29)

Buna göre

a) Şifreli kelimeler ile gerçek kelimeler arasındaki sayısal ilişkiyi (harflerin alfabedeki sıralarını kullanarak) inceleyiniz. Her harfin kendi şifreli karşılığına nasıl bir değişimle ulaştığını belirleyiniz.

b) Bu şifreleme sisteminde kullanılan şifre alfabesini (yani her harfin karşılığını gösteren yeni cetveli) oluşturunuz.

c) Bu şifreleme yöntemini $f(x) = ax + b \mod\{29\}$ biçiminde cebirsel olarak genelleyiniz. (örüntüyü cebirsel olarak genelleyiniz ya da kısaca a ve b değerlerini bulunuz.

Örnek...8 :

Bir istihbaratçı, şifrelenmiş bir metni incelerken Türkçede çok sık kullanılan "AD" ve "SU" kelimelerinin şifreli metinde sırasıyla "Fİ" ve "ÜG" olarak geçtiğini tespit etmiştir.

Kullanılacak Alfabe Dizisi (m=29):

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

Buna göre

a) Verilen kelime eşleşmelerinden yola çıkarak şifreleme fonksiyonundaki a (çarpan) ve b (kaydırma) değerlerini bulunuz.

b) Bu örüntüyü kullanarak "FEN" kelimesinin şifreli karşılığını bulunuz.

c) Bu şifreleme sisteminin genel cebirsel formülünü yazınız.

Örnek...9 :

A	B	D	K	R
1	2	3	4	0

Üstteki tabloda gerçek bir metinde geçen harflerin sayısal karşılıkları verilmiştir. Bu metinde geçen harflerin değerlerinin 3 katının 2 eksiği alınmakta ve çıkan değerler 5'ye bölünerek elde edilen kalan değerlerle şifreli metin oluşturulmaktadır.

Buna göre bu şifreleme yöntemiyle şifrelenerek "KADBAR" olarak elde edilen kelimesinin gerçek karşılığını bulunuz.

Örnek...10 :

Şifreli bir şekilde haberleşen Aden ve Barkut, kurdukları cümlelerde harflerin yerlerini değiştirerek iletişim sağlamaktadırlar. Şifreledikleri cümleyi çözerken cümleleri tam ortadan ikiye bölüp, alt alta yazarak gerçek cümleye ulaşmaktadırlar. Aden, Barkut ile yaptığı bir yazışmasında "YRNÖÜEİAIGRŞLM" cümlesini kurmuştur. Buna göre, SAAT DÖRTTE cümlesini aynı yöntemle şifreleyiniz

Yer değiştirme (transpozisyon) yöntemine dayalı şifrelemenin mantığını şu üç ana maddede özetleyebiliriz:

Harf Sayısı ve Karmaşıklık: Metindeki harf sayısı arttıkça olasılıklar katlanarak büyür. Gelişigüzel karıştırılmış uzun metinleri çözmek hem üçüncü kişiler hem de alıcı için imkansız hale gelebilir.

Önceden Belirlenmiş Yöntem: Şifrenin çözülebilmesi için gönderici ve alıcının karıştırma yönteminde (anahtar) önceden anlaşması şarttır.

Sistemli Gruplandırma: Karmaşıklığı yönetilebilir kılmak için metinler ya "n"li bloklara ayrılarak blok içinde karıştırılır ya da "ortadan ikiye bölüp çapraz okuma" gibi belirli geometrik kurallarla şifrelenir.

Steganografi, gizli bir mesajın varlığını tamamen gizleme sanatıdır. Yunanca steganós (gizlenmiş) ve gráphein (yazmak) kelimelerinin birleşiminden oluşur.

Kriptografi (şifreleme) ile sıkça karıştırılır ancak temel bir farkları vardır: Kriptografide mesajın içeriğini okunmaz hale getirirsiniz (mesaj oradadır ama ne olduğu anlaşılmaz); steganografide ise mesajın orada olduğu bile belli değildir.

Steganografi Nasıl Çalışır?
Gizlemek istediğiniz veri (metin, resim veya ses), şüphe uyandırmayacak başka bir dosyanın (genellikle bir görsel veya müzik dosyası) içine gömülür.
En Yaygın Yöntem: LSB (En Önemsiz Bit) Değiştirme Dijital bir fotoğraftaki her pikselin renk değerleri bitlerle (0 ve 1) ifade edilir. Steganografi, bu piksellerin en sağındaki (değeri en düşük) bitleri gizli mesajın bitleriyle değiştirir. Bu değişim o kadar küçüktür ki, insan gözü orijinal resim ile mesaj yüklü resim arasındaki farkı ayırt edemez.

Kullanım Alanları ve Örnekler

1. Dijital Filigranlama: Bir resmin veya videonun içine telif hakkı bilgilerini görünmez bir şekilde gömmek.
2. Güvenli Haberleşme: Şifreli mesajların dikkat çekmemesi için masum görünen bir kedi fotoğrafının içine saklanması.
3. Tarihsel Örnekler: Eski Yunan'da kölelerin saçları kazınır, mesaj kafalarına dövme yapılır ve saçları uzayınca karşı tarafa gönderilirdi. Karşı taraf saçları tekrar kazıyarak mesajı okurdu.

İpucu: Güvenliği artırmak için genellikle önce mesaj kriptografi ile şifrelenir, ardından steganografi ile bir resmin içine gizlenir. Böylece mesaj fark edilse bile içeriği okunamaz.

VİGENERE ŞİFRELEMESİ

Vigenère şifrelemesi, metindeki harfleri belirli bir anahtar kelimeye göre kaydırarak şifreleyen bir polialfabetik (çok alfabeli) şifreleme yöntemidir. Tek bir kaydırma miktarı kullanan Sezar şifrelemesinin aksine, Vigenère yönteminde her harf farklı miktarlarda kaydırılır.
Çalışma Mantığı
Şifreleme işlemi genellikle Vigenère Tablosu (veya Tabula Recta) adı verilen 26x26'lık bir matris kullanılarak yapılır. Bu tablo, alfabenin her satırda birer kez sola kaydırılmasıyla oluşur.

Anahtar Kelime: Bir anahtar seçilir (örneğin: "ELMA").
Tekrar: Anahtar kelime, şifrelenecek metnin boyuna ulaşana kadar tekrar edilir.
Kesişim: Metnin ilk harfi ile anahtarın ilk harfi tabloda bulunur; bu iki harfin kesiştiği noktadaki harf, şifreli metni oluşturur.

Örnek...11 :

"MERHABA" kelimesini Vigenère şifrelemesi kullanarak "SU" anahtarıyla şifrelemek istiyoruz:

1. Metin: M E R H A B A
2. Anahtar: S U S U S U S (Anahtar kelime yetmediği için başa döndü)
3. Metindeki harf ve harfe karşılıkgelen anahtar harflerin sayısal değerlerini (A=0, B=1, ..., Z=28) toplayarak ilerliyoruz.
4. Son olarak elde edilen toplamın 29 ile toplamından kalanı bulup şifreli harfi oluşturuyoruz.

Metin Harfi	Değeri	Anahtar Harfi	Değeri	Toplam	Mod 29	Şifreli Harf
M	15	S	21	36	7	G
E	5	U	24	29	0	A
R	20	S	21	41	12	J
H	9	U	24	33	4	D
A	0	S	21	21	21	S
B	1	U	24	25	25	Ü
A	0	S	21	21	21	S

Dolayısıyla "MERHABA" kelimesini Vigenère şifrelemesi kullanarak şifrelenmiş hali "GAJDSÜS" olarak elde edilir.

Neden Önemli?
Vigenère, 16. yüzyılda geliştirildiğinde uzun süre kırılamadığı için "le chiffre indéchiffrable" (kırılamayan şifre) olarak anılmıştır. Sezar şifrelemesi gibi yöntemlerin aksine, harf frekans analiziyle kolayca çözülemez çünkü aynı harf (örneğin "A") anahtarın durumuna göre metnin farklı yerlerinde farklı harflere dönüşebilir. Ancak 19. yüzyılda Kasiski ve Friedman gibi kriptograflar, anahtar uzunluğunu tespit ederek bu şifreyi kırmanın yollarını bulmuşlardır.

Çok alfabeli (Vigenere tipi) şifreleme ve anahtar kullanımıyla ilgili temel çıkarımlar şu şekilde özetlenebilir:

Anahtar Belirtileri: Şifreli metinde aynı harfin farklı karakterlerle eşleştiği görülüyorsa, değişken bir anahtarın kullanıldığı anlaşılır.

Çözüm Yöntemi: Anahtar ve algoritma bir kez deşifre edildiğinde, metnin tamamı kolayca okunabilir hale gelir.

Örüntü ve Algoritma: Anahtar bulunduğunda, harf sıralamaları üzerinden yapılan genellemeler şifreleme mantığını (algoritmayı) ortaya çıkarır.

Matematiksel Mantık: Vigenere şifrelemede, orijinal metindeki harf ile anahtardaki harfin sayısal değerleri (A=0, B=1... düzeninde) toplanarak şifreli karakter elde edilir.

Örnek...12 :

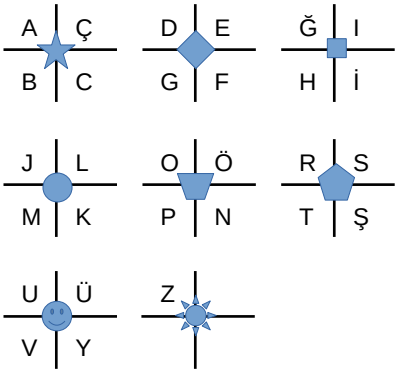
"EĞİTİM" kelimesini "**DERS**" anahtarıyla, Türk alfabesi standart sayısal değerlerini (A=0, B=1, ..., Z=28) kullanarak şifreleyiniz.

Örnek...13 :

"KARADENİZ" kelimesini "ÇAY" anahtarıyla, Türk alfabesi standart sayısal değerlerini (A=0, B=1, ..., Z=28) kullanarak şifreleyiniz.

Örnek...14 :

Yanda Türk alfabesi, sembollerle isimlendirilmiş sekiz ayrı tabloya bölünmüştür. Şifreleme sırasında harfi çevreleyen grafiksel çerçeve (kenarlıklar) kullanılmaktadır. Çerçevenin merkezine, harfin ait olduğu tabloyu temsil eden özel sembol yerleştirilerek görsel kod tamamlanır.



Örneğin bu yöntemle KALEM kelimesi

 biçiminde şifrelenmiştir.

Buna göre "ZONGULDAK" kelimesini aynı yönergeye uygun şekilde şifreleyiniz.

ÖZET

Anahtar tabanlı çok alfabeli şifreleme yöntemlerinin temel özelliklerini şu şekilde özetleyebiliriz:

- Değişken Karşılıklar: Aynı harfin metin içerisinde farklı harflerle şifrelenmesi, bir anahtar kullanıldığının en temel göstergesidir.
- Çözüm Anahtarı: Anahtarın tespit edilmesi, şifreleme algoritmasıyla birlikte tüm metnin deşifre edilmesini sağlar.
- Örüntü ve Algoritma: Anahtar belirlendiğinde harf sıralamaları üzerinden elde edilen örüntüler, kullanılan genel şifreleme algoritmasını ortaya çıkarır.
- Vigenere Şifrelemesi: Bu özel yöntemde, gerçek metin ile anahtar harflerinin sayısal değerleri (A=0, B=1...) toplanarak şifreli metin oluşturulur.

Mors alfabesi, harfleri, rakamları ve bazı sembolleri kısa ve uzun sinyallerle (nokta "." ve çizgi "-") ifade eden bir iletişim sistemidir. 19. yüzyılda telgraf haberleşmesinde kullanılmıştır.

Şifreleme ile ilişkisi:
Mors alfabesi aslında bir **şifreleme yöntemi değil, bir kodlama sistemidir.** Yani harflerin yerini tamamen farklı semboller alır (örneğin A = .-), ancak bu dönüşüm herkes tarafından bilinir.
Bu yüzden gizlilik sağlamaz; sadece iletimi kolaylaştırır. Gerçek şifrelemede ise mesajın anlamı gizlenir.
Ancak Mors alfabesi, bir metni farklı bir biçime dönüştürdüğü için basit düzeyde "şifreye benzer" bir yapı oluşturur.
Eğer Mors alfabesi üzerine ek olarak bir anahtar ya da farklı kurallar uygulanırsa, o zaman gerçek bir şifreleme sistemine dönüştürülebilir.
Kısacası, Mors alfabesi tek başına bir şifreleme yöntemi değil, fakat şifreleme işlemlerinde kullanılabilecek bir **ara kodlama aracı**dır.

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