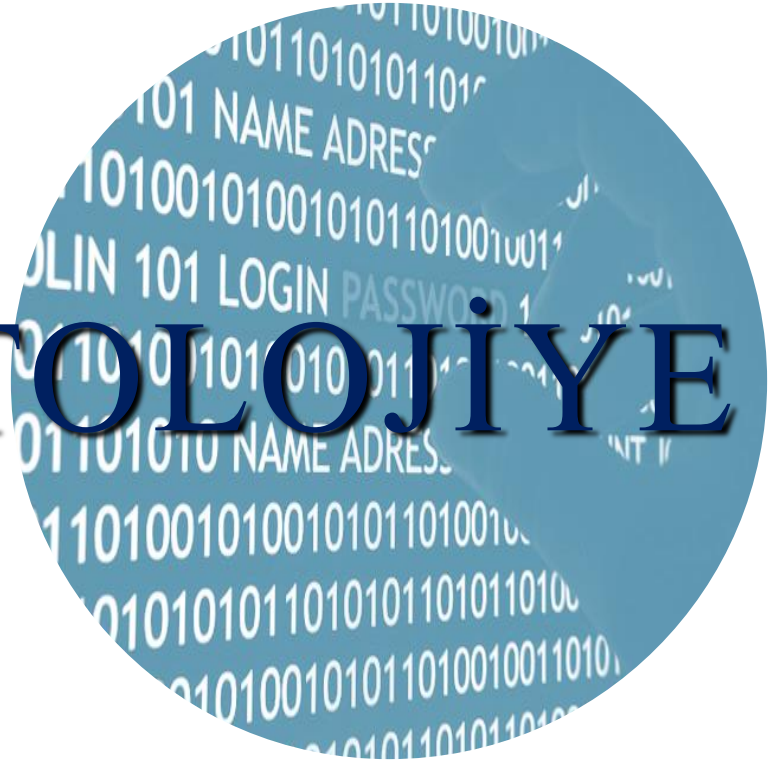
KRİPTOLOJİYE GİRİŞ



DR. GÜNAY TEMÜR

KRİPTOLOJİ

Kriptoloji en basit tanımı ile şifreleme bilimidir; bilgilerin gizlenmesi ve ortaya çıkarılmasıyla ilgilenir. Kriptoloji bilimi, kriptografi ve kriptanaliz olmak üzere iki alt sistemden oluşur.

KRİPTO

- Kökeni Yunanca’dan gelmektedir:
  - kryptos = gizli
  - -graphia = yazmak
  - -logia = -alanındaki çalışmalar
  - analyse = temel parçalarına ayırıp incelemek
- Kodlama teorisi?

KRİPTOLOJİ

- Haberleşmede veri güvenliğini sağlayan şifreleme cihazlarını, bu cihazlarda kullanılan algoritmaların tasarımını ve bu algoritmaların güvenilirliğini araştırır.
- Matematik bazlı olup elektrik ve elektronik mühendisliği, bilgisayar mühendisliği, istatistik ve fizik bölümlerini ilgilendiren disiplinlerarası bir alandır.

KRİPTOGRAFİ

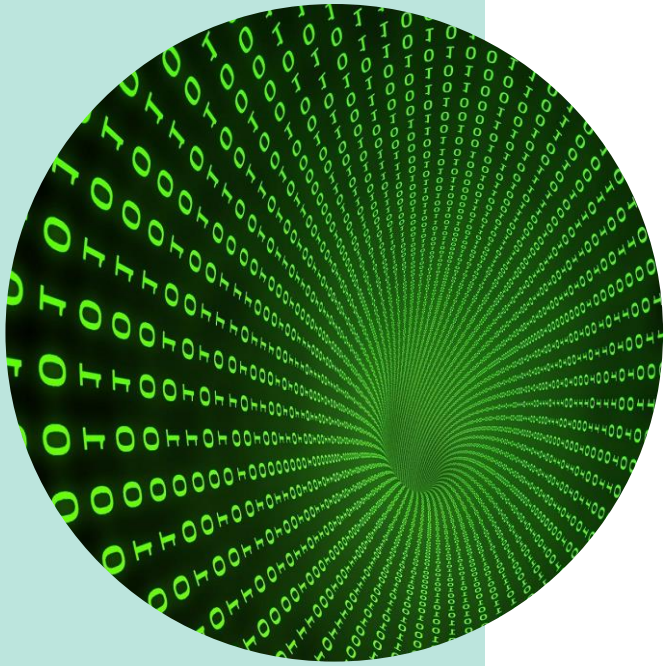
- Kriptografi, iletilen bilginin istenmeyen şahıslar tarafından anlaşılmayacak bir biçime dönüştürülmesinde kullanılan tekniklerin bütünüdür. Bilgi güvenliği ve bütünlüğünü sağlamayı amaçlayan tekniklerin geliştirilmesini hedefler.
- Kriptografi gizlilik, bütünlük, kimlik denetimi ve inkar edememe gibi bilgi güvenliğinin temel amaçlarını sağlamaya çalışan matematiksel yöntemleri içermektedir.

KRİPTOANALİZ

- Kriptolojinin, kriptografik sistemlerin şifrelenmiş metinlerini çözebilmek için bu sistemlerin güvenliklerini inceleyen - zayıf yanlarını bulmaya çalışan dalıdır.
- Anahtara sahip olmadan bir gizli (şifreli) yazının açık halini bulma bilimi olarak da nitelendirilebilir.

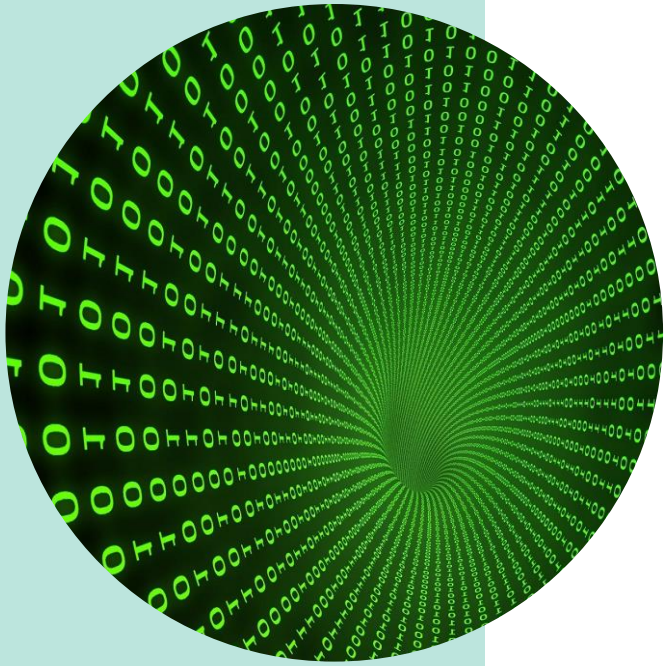
ŞİFRELEMENİN EVRİMİ VE ÖNEMİ

- Tüm modern şifreleme teknolojilerinin temeli kriptografiye dayanır.
- Özetle kriptografi; bir kod oluşturma ve çözmeye çalışma eylemidir. Elektronik şifrelemenin tarihi nispeten yeni olsa da, kriptografi Antik Yunan’a kadar uzanan bir bilim dalıdır.
- Antik Yunanlılar, yazılı hassas verileri hem düşmanlarından hem de kendi halkından saklamak için kriptografiyi kullanan ilk toplumdu.



ŞİFRELEMENİN EVRİMİ VE ÖNEMİ

- İlkel kriptografi yöntemleri geliştirmede Romalılar da o dönemlerde, “Sezar’ın şifresi” olarak bilinen ve bir harfi alfabedeki başka bir harf yerine değiştirmeyi içeren bir ikame şifre yöntemi ile aynı şeyi yaptılar. Örneğin bu yöntemi Türkçemize uyarladığımızda, anahtar üç sağa kaydırma içeriyorsa, A harfi Ç olur, B harfi D olur vb.



ŞİFRELEMENİN EVRİMİ VE ÖNEMİ

- Veri şifreleme önemlidir, çünkü insanların gizliliğini korumaya yardımcı olur ve verileri saldırganlardan ve diğer siber güvenlik tehditlerinden korur. Şifreleme, sağlık, eğitim, finans ve bankacılık ve perakende gibi kuruluşlar için günümüzde zorunludur.

ŞİFRELEMENİN EVRİMİ VE ÖNEMİ

- Bir web sitesinin adresinin “https://” ile başladığını fark ettiyseniz buradaki “s” “secure-güvenli” anlamına gelir ve bu web sitesinin aktarım şifrelemesi kullandığını gösterir. Sanal özel ağlar (VPN’ler), bir cihazdan gelen ve giden verileri meraklı gözlerden gizli tutmak için şifreleme kullanır.

ŞİFRELEMENİN EVRİMİ VE ÖNEMİ

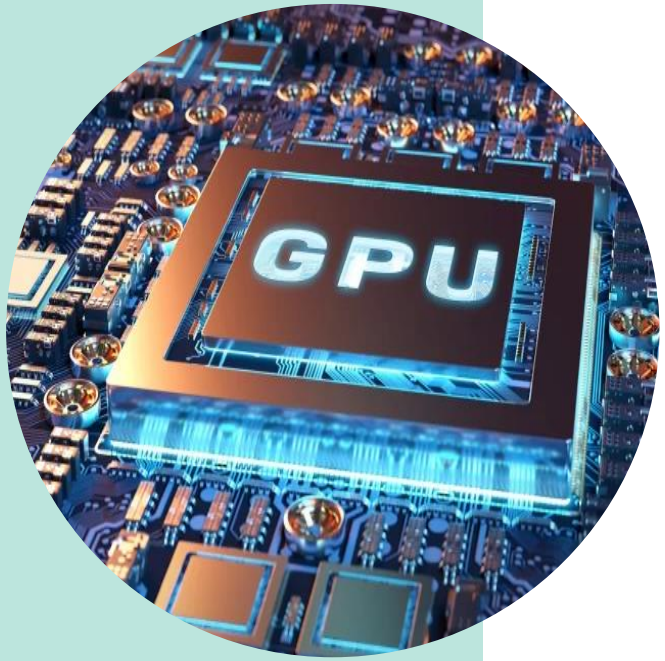
- Şifreleme dört önemli işlevi yerine getirir:
- **Gizlilik :** Verilerin içeriğini gizli tutar.
- **Bütünlük :** Mesajın veya verilerin kaynağını doğrular.
- **Kimlik doğrulama :** Gönderildiğinden beri mesajın veya verilerin içeriğinin değiştirilmediğini doğrular.
- **Reddetmeme :** Veriyi veya mesajı gönderenin kaynak olduğunu inkar etmesini engeller.

MODERN ŞİFRELEME TEKNOLOJİSİNDEN BAZI ÖRNEKLER

- Modern şifreleme teknolojisi, şifrelenmiş verileri daha iyi gizlemek için daha gelişmiş algoritmalar ve daha büyük anahtar boyutları kullanır. Anahtar boyutu ne kadar büyük olursa, bir siber saldırının şifreli metnin şifresini başarıyla çözmek için çalıştırması gereken kombinasyonlar o kadar fazla olur.
- Anahtar boyutu gelişmeye devam ettikçe, siber saldırı ile şifrelemeyi kırmak için gereken süre o kadar hızla artar.

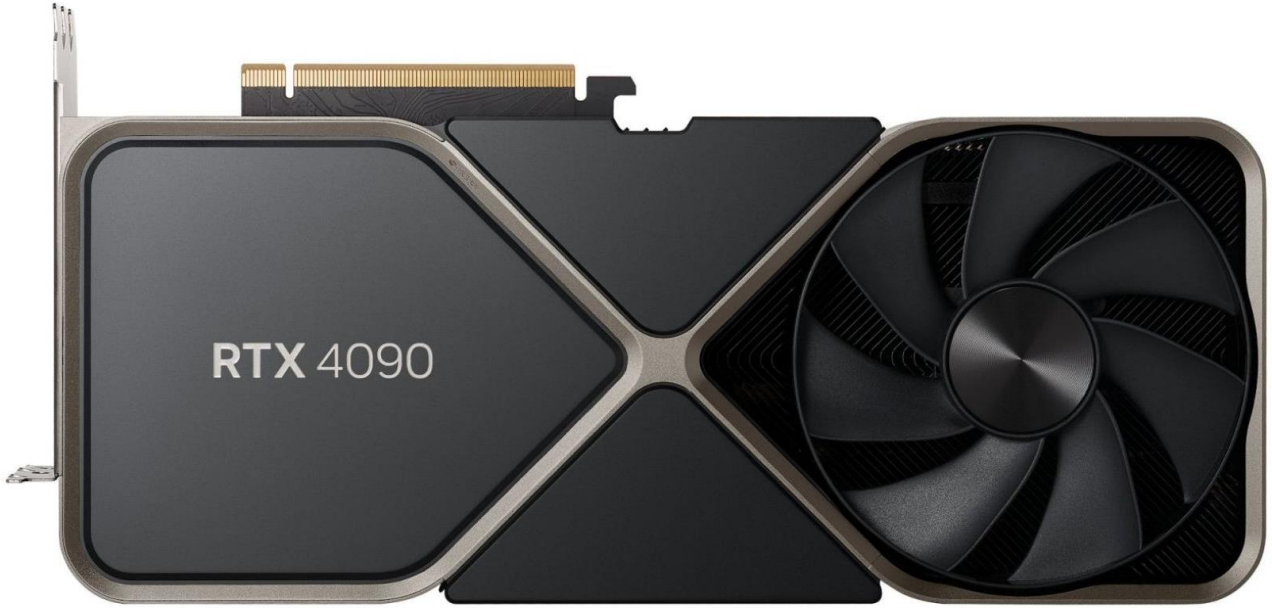
MODERN ŞİFRELEME TEKNOLOJİSİNDEN BAZI ÖRNEKLER

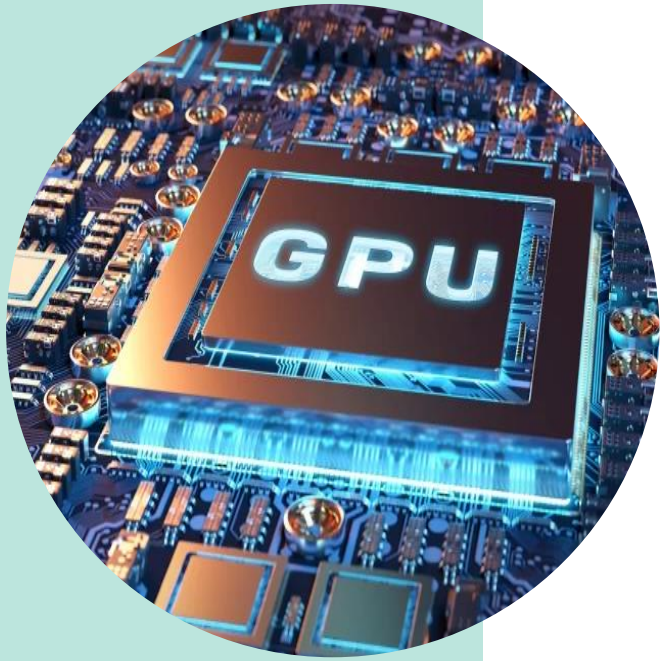
- Örneğin, 56 bitlik bir anahtar ile 64 bitlik bir anahtarın değeri rakamsal olarak yakın görünse de, 64 bitlik anahtarın kırılması 56 bitlik anahtara göre 256 kat daha zordur.
- Günümüz modern şifrelemelerin çoğu en az 128 bitlik bir anahtar kullanır, 256 bitlik veya daha büyük anahtarlar kullanılan alanlar da vardır. Bunu rakamlarla anlatmak gerekirse, 128 bitlik bir anahtarı kırmak, 339.000.000.000.000.000.000.000.000.000.000.000 (339 Desilyon) ‘dan fazla olası anahtar kombinasyonunu denemeyi gerektirir.



MODERN ŞİFRELEME TEKNOLOJİSİNDEN BAZI ÖRNEKLER

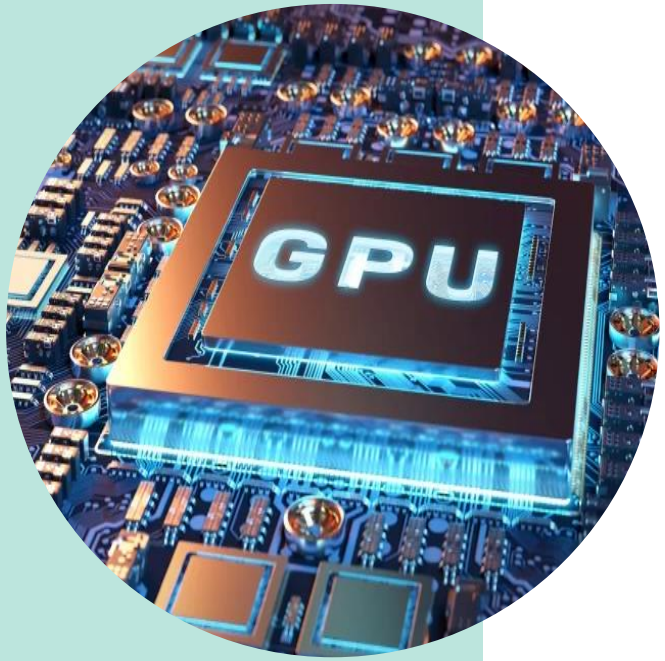
Yapılan testlere göre GeForce RTX 4090 şifreleri kırma konusunda inanılmaz derecede başarılı. Bu model 8 grafik kartının, 18 karakter uzunluğunda bir şifreyi 48 dakikada kırabileceği belirtiliyor.





MODERN ŞİFRELEME TEKNOLOJİSİNDEN BAZI ÖRNEKLER

- Nvidia GeForce RTX 4090 grafik kartı sadece oyun konusunda değil, aynı zamanda yüksek bilgi işlem gücü gerektiren işlemlerin yapılmasında da son derece yetenekli. Grafik kartının bu üstün yetenekleri olumlu işlerde kullanılacağı gibi bir şeyi hacklemek için de kullanılabilir. Örneğin, bazı parola korumalı veriler.
- Hashcat'in (en hızlı şifre kırma aracı olarak tanınıyor) baş geliştiricisi ve yarı zamanlı güvenlik analisti Sam Croley, uygulamasını GeForce RTX 4090 3D kartıyla test etti ve şifre kırmada GeForce RTX 3090'dan iki kat daha hızlı olduğu ortaya çıktı.



MODERN ŞİFRELEME TEKNOLOJİSİNDEN BAZI ÖRNEKLER

- Elcomsoft, gerçekleştirdiği “ekran kartlarını kullanarak şifre kırma” testinde aşağıda yer verdiğimiz beş farklı NVIDIA ekran kartını kullandı:
  - NVIDIA GTX 1650
  - NVIDIA RTX 3050
  - NVIDIA RTX 3060
  - NVIDIA RTX 2070
  - NVIDIA RTX 3060 Ti

ŞİFRELEME VE ŞİFRE ÇÖZME

- En temel düzeyde elektronik şifreleme, bilgileri veya anlam kazandırılmış bilgilerden oluşan verileri, yalnızca şifreyi çözme anahtarına sahip olan tarafların erişebileceği şekilde karıştırmak için matematiksel modeller yardımıyla saklamasına yarayan bir kriptografi biçimidir.

ŞİFRELEME NEDİR

- Şifreleme, düz metin olarak bilinen normal verileri, şifresini çözmek için özel bir anahtara sahip olmayanlar tarafından okunamayan, görünüşte rastgele karakterler gibi görünen şifreli bir metine dönüştürmek için “şifre” adı verilen oldukça karmaşık bir algoritma kullanır.

ŞİFRELEME NEDİR

- Öyle ki, şifrelenmiş bir metni okuyan bir yazılım, anahtarı olmadan buradan anlamlı bir sonuç türetemez. Yalnızca anahtara sahip olanlar, rastgele dizilmiş anlamsız karakterler gibi görünen bu metnin şifresini çözerek, onun gerçek halini görüntüleyebilir.

ŞİFRE ÇÖZME

- Şifreleme işleminin tersidir. Şifreli metin yine anahtar kullanılarak açık metne dönüştürülme işlemidir.

ŞİFRELEMENİN TEMEL ELEMANLARI

- Bir kriptosistemin 5 elemanı vardır.
- P=Plaintext: Şifrelenecek olan düz metin
- K=Key(Anahtar): Şifrelemede kullanıcak olan anahtar
- E=Encryption: Şifreleme
- C=Ciphertext: Düz metinin şifrelenmiş hali.
- D=Decryption: Şifre çözümü.
- **NOT: Güvenlik anahtarın gizliliğine bağlıdır, algoritmanın gizliliğine değil.**

KLASİK KRİPTOGRAFİK SİSTEMLER

- **Sezar Şifresi (M.Ö. 100-44)**
  - Harflerin alfabede K =3 konum sonrasındaki karşılığı ile değiştirir
  - C = P+ K (mod 26)
  - MERHABA → PHUKDED
  - Kriptanalizi istatistiksel analizle kolayca yapılmaktadır

0	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
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
D	E	F	G	H	İ	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

KLASİK KRİPTOGRAFİK SİSTEMLER

- Sezar Şifresi

0	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
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

- f(x) = i + 7
  - Gölyaka ?

KLASİK KRİPTOGRAFİK SİSTEMLER

- Sezar Şifresi

0	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
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
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

- f(x) = i + 7
  - Golyaka ?

G	O	L	Y	A	K	A
Z	H	E	R	T	D	T

KLASİK KRİPTOGRAFİK SİSTEMLER

- Sezar Şifresi

0	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
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

- f(x) = i - 5
  - Kripto ?

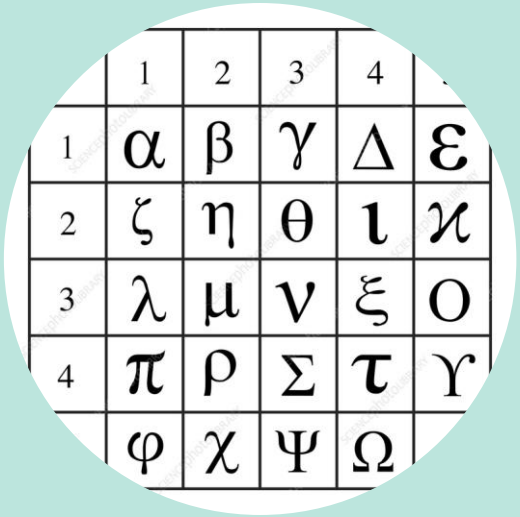
KLASİK KRİPTOGRAFİK SİSTEMLER

- Sezar Şifresi

0	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
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
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	e

- f(x) = i - 5
  - Kripto ?

K	R	İ	P	T	O
P	W	N	U	Y	T

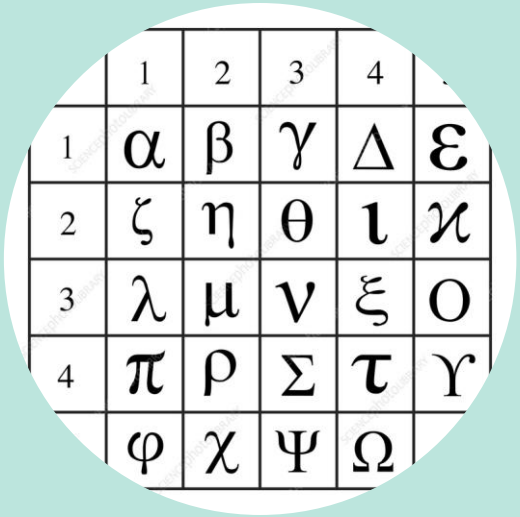


	1	2	3	4	
1	α	β	γ	Δ	ε
2	ζ	η	θ	ι	κ
3	λ	μ	ν	ξ	ο
4	π	ρ	σ	τ	υ
	φ	χ	ψ	ω	

POLYBİUS ŞİFRELEME SİSTEMİ

Polybius adında bir kişi tarafından bulunan iki boyutlu bir tahtaya harflerin ve rakamların dizilmesine esasına dayalı bir şifreleme sistemidir.

	1	2	3	4	5	6
1	A	B	C	Ç	D	E
2	F	G	Ğ	H	I	İ
3	J	K	L	M	N	O
4	Ö	P	R	S	Ş	T
5	U	Ü	V	Y	Z	

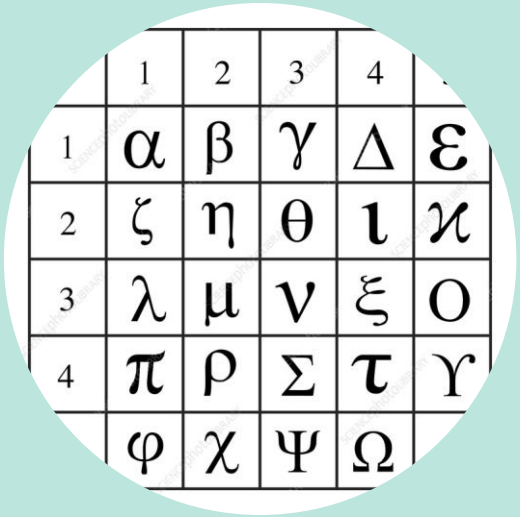


	1	2	3	4	
1	α	β	γ	Δ	ε
2	ζ	η	θ	ι	κ
3	λ	μ	ν	ξ	ο
4	π	ρ	σ	τ	υ
	φ	χ	ψ	ω	

POLYBİUS ŞİFRELEME SİSTEMİ

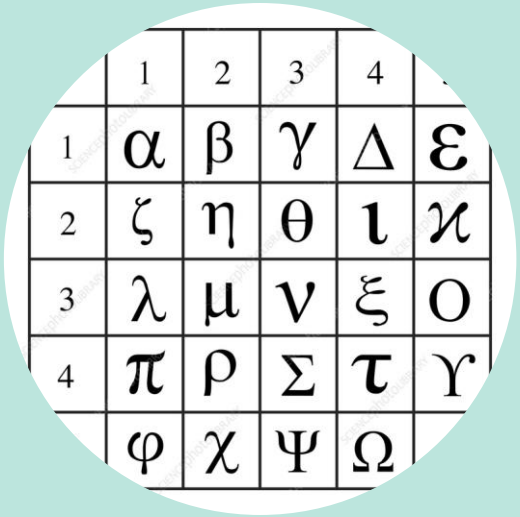
Bu sistemde harfler, yatay ve dikey rakamların kesişmesiyle gösterilir. Örneğin "YARIŞ" sözcüğü bu şifreleme sisteminde şu şekilde gösterilir: 54 - 11 - 43 – 25 - 45

	1	2	3	4	5	6
1	A	B	C	Ç	D	E
2	F	G	Ğ	H	I	İ
3	J	K	L	M	N	O
4	Ö	P	R	S	Ş	T
5	U	Ü	V	Y	Z	



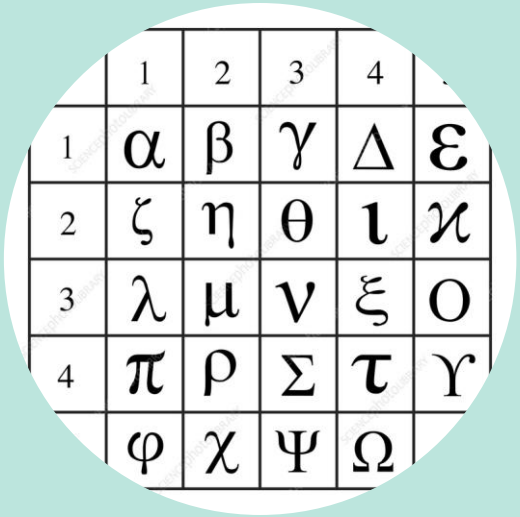
AFFİNE ŞİFRELEME SİSTEMİ

Bu şifreleme yöntemindeki amaç geometride doğrunun denklemi olarak bilinen y=ax+b doğrusal fonksiyonunu şifreleme işleminde kullanmaktır. Buna göre x, şifrelenecek mesajı (plain text), y şifrelenmiş mesajı (cipher text) ifade etmekte olup a ve b ikilisi anahtarı oluşturmaktadır.



AFFİNE ŞİFRELEME SİSTEMİ

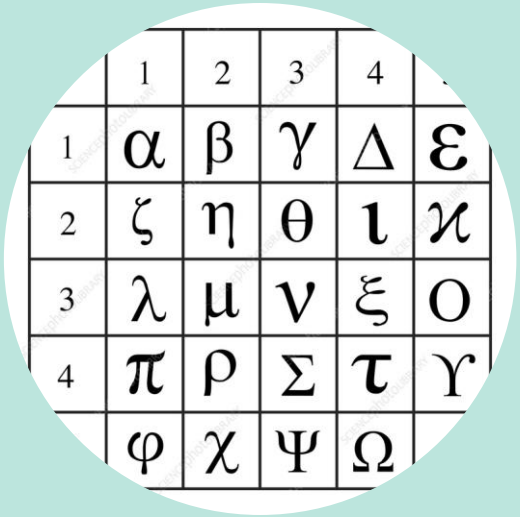
Harf Sayı Karşılıkları							
a	0	b	1	c	2	ç	3
d	4	e	5	f	6	g	7
ğ	8	h	9	ı	10	i	11
j	12	k	13	l	14	m	15
n	16	o	17	ö	18	p	19
q	20	r	21	s	22	ş	23
t	24	u	25	ü	26	v	27
w	28	x	29	y	30	z	31



AFFİNE ŞİFRELEME SİSTEMİ

Şifrelenmek istenen açık mesajın her karakterleri için, o karaktere karşılık gelen sayı değeri basit bir matematiksel fonksiyona girdi olarak gönderilir. Fonksiyon sonuç olarak farklı bir sayı değeri çıktısı üretir. Fonksiyondan çıkış olarak üretilen bu sayı değeri, tabloda hangi karakteri temsil ediyorsa o karakter, şifreli mesajın yapısını oluşturur.

Affine şifrelemede doğrunun denklemi olan $y=ax + b$ doğrusal fonksiyonu kullanılır. Bu denklemde x açık mesajı, a ve b ikili anahtarı, y ise şifreli mesajı ifade eder.



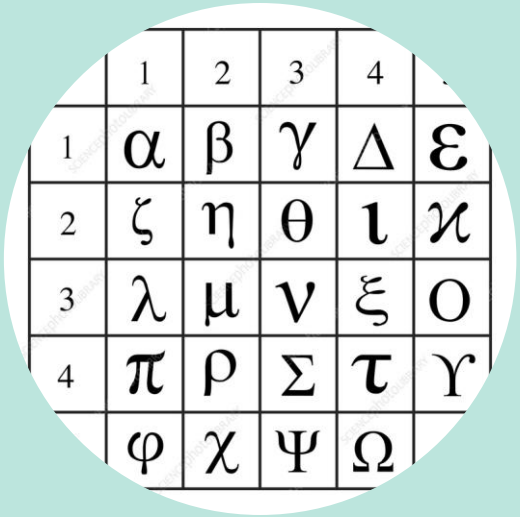
AFFİNE ŞİFRELEME SİSTEMİ

Harf Sayı Karşılıkları							
a	0	b	1	c	2	ç	3
d	4	e	5	f	6	g	7
ğ	8	h	9	ı	10	i	11
j	12	k	13	l	14	m	15
n	16	o	17	ö	18	p	19
q	20	r	21	s	22	ş	23
t	24	u	25	ü	26	v	27
w	28	x	29	y	30	z	31

ÖRNEK:

Açık mesaj: affine

a	0
f	6
f	6
i	11
n	16
e	5



AFFİNE ŞİFRELEME SİSTEMİ

ÖRNEK:

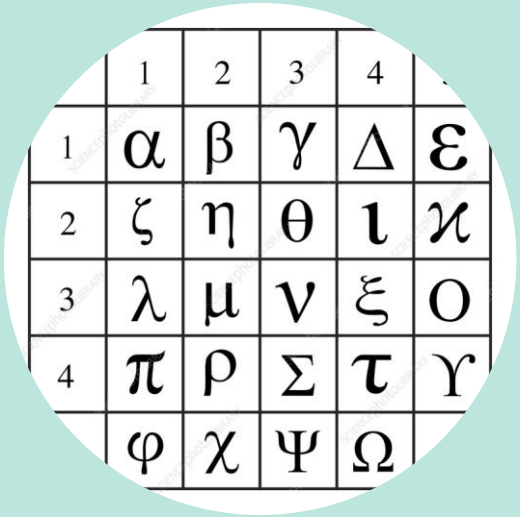
Açık mesaj: affine

Anahtar : (a,b) (7,3)

a	0
f	6
f	6
i	11
n	16
e	5

E(x) = y = ax + b mod c
*a için y = 7*0 + 3 mod 32 = 3*
*f için y = 7*6 + 3 mod 32 = 13*
*i için y = 7*11 + 3 mod 32 = 16*
*n için y = 7*16 + 3 mod 32 = 19*
*e için y = 7*5 + 3 mod 32 = 6*

3	Ç
13	K
13	K
16	N
19	P
6	F



AFFİNE DEŞİFRELEME SİSTEMİ

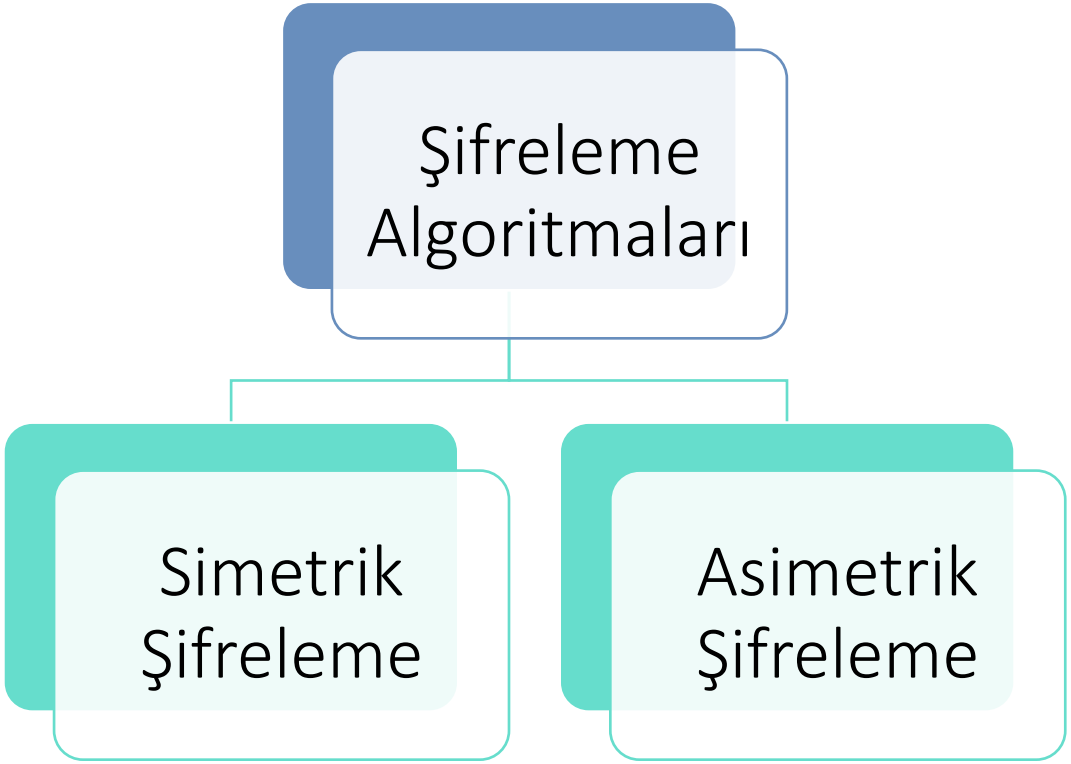
ÖRNEK:

Şifreli mesaj: çkknpf Anahtar : (a,b) (7,3)

3	Ç
13	K
13	K
16	N
19	P
6	F

D(x) = x = a(y – b) mod c
ç için x = 23(3 – 3) mod 32 = 0*
k için x = 23(13 - 3) mod 32 = 6*
n için x = 23(16 - 3) mod 32 = 11*
p için x = 23(19 - 3) mod 32 = 16*
f için x = 23(6 - 3) mod 32 = 5*

ALGORİTMALAR



SİMETRİK ŞİFRELEME

Simetrik şifreleme, elektronik veriyi şifrelemek ve çözmek için sadece tek bir anahtar kullanan şifreleme tipidir. Simetrik şifreleme algoritmaları da kendi içerisinde ikiye ayrılır.

Blok algoritmalar: Blok şeklinde olan elektronik verileri özel anahtarı kullanarak bitlerin uzunluğunu belirler. Veri şifrelendiği esnada sistem veriyi bloklar tamamlanana kadar kendi belleğinde tutar.

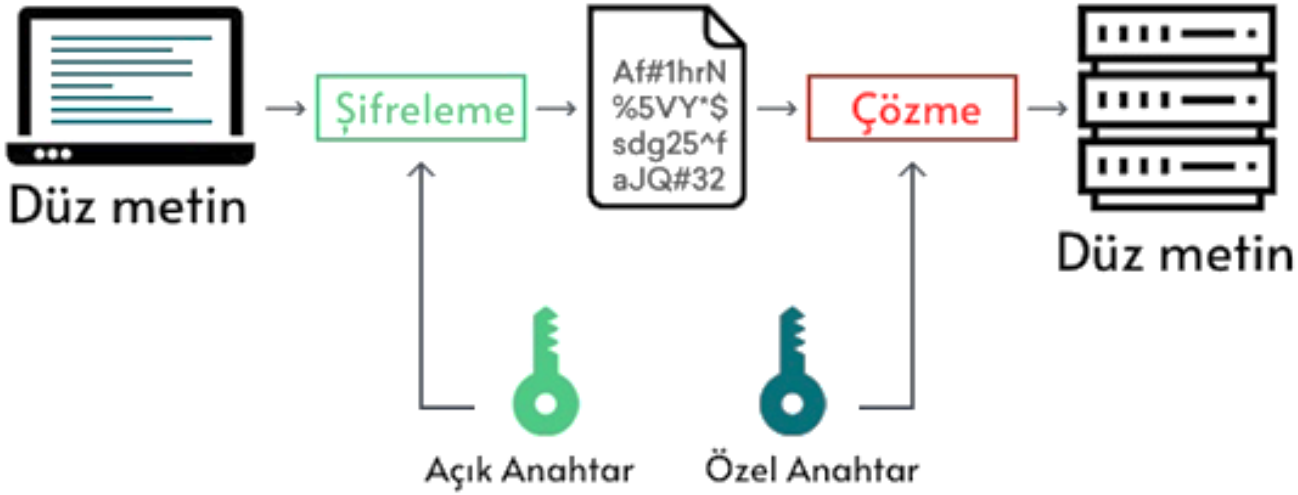
Akış algoritmaları: Veri, sistemin belleğinde durmak yerine akışlar ile şifrelenir.

SİMETRİK ŞİFRELEME

Bazı simetrik şifrelemelere örnek vermek gerekirse;

- RC4, RC5, RC6 (Rivest Cipher 4-5-6)
- IDEA (International Data Encryption Algorithm)
- DES (Data Encryption Standard)
- AES (Advanced Encryption Standard)
- 3DES (Triple DES)

ASİMETRİK ŞİFRELEME



Simetrik şifreleme, asimetrik şifrelemeye göre eski bir şifreleme algoritma olsa da asimetrik şifrelemeye göre daha etkin ve hızlı bir metottur. Bu yapısı sayesinde veri boyutunun artmasına ve ağır bir işlemci kullanımına yol açmamaktadır.

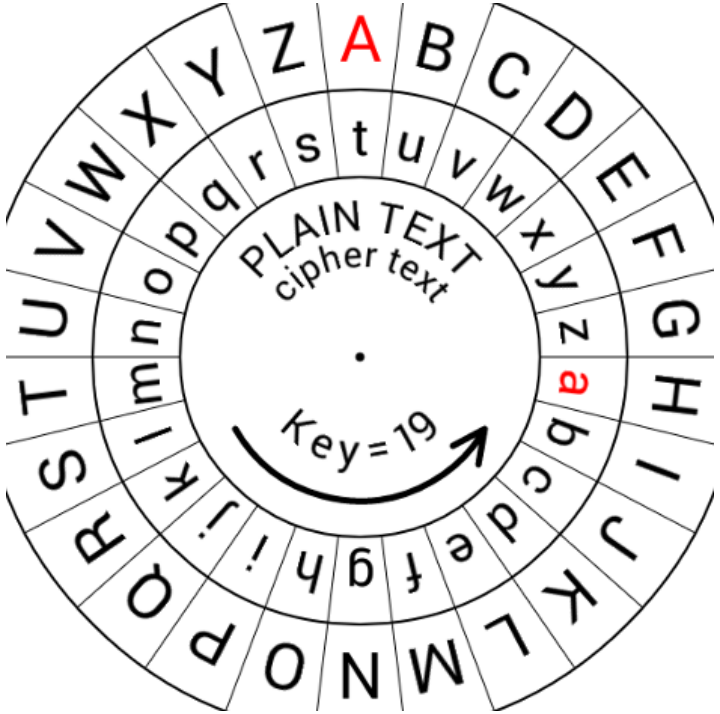
Asimetrik şifreleme, içerisinde bir özel ve bir açık anahtar bulunduran bir şifreleme algoritmasıdır. Açık anahtar güvenilir veya güvenilir olmayan herkese verilebilirken özel anahtarın güvenilir bir kişiye veya kişilere verilmesi gerekmektedir.

ASİMETRİK ŞİFRELEME

Asimetrik şifrelemenin iki ana kullanım amacı vardır. Bunlar doğrulama ve gizliliktir. Asimetrik şifreleme kullanılarak mesajların özel anahtar ile imzalanabildiğini ve mesajı alan kişi kendi özel anahtarı ile mesajı doğrulayarak mesajın doğru olduğunu teyit edebilmektedir.
Günümüzde en çok kullanılan asimetrik şifreleme algoritmaları ise aşağıdaki gibidir;

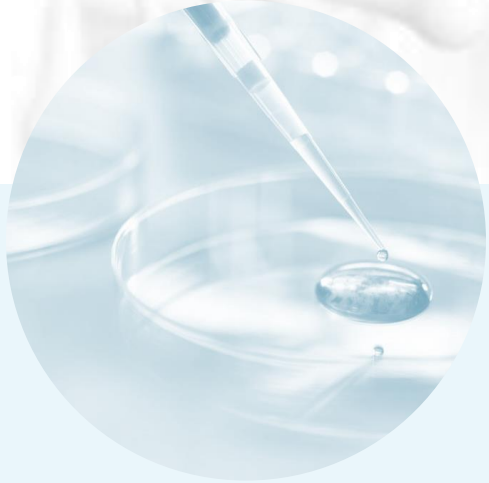
- RSA (Rivest-Shamir-Adleman)
- DSA (Digital Signature Algorithm)
- DH (Diffie-Hellman)

GÜNÜMÜZDE KRİPTOGRAFİK SİSTEMLER



Bugün, kriptografi çok geniş uygulama alanlarına dahil olarak günlük hayatın önemli bir parçası olmuştur:

- sim kartlar,
- cep telefonları,
- uzaktan kumandalar,
- online bankacılık,
- online alışveriş,
- uydu alıcıları,



TEŞEKKÜRLER

GÜNAY TEMÜR