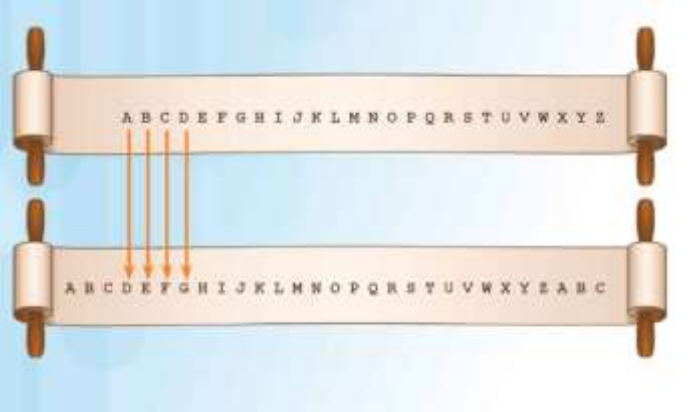
KRİPTOGRAFİ

BURAK KAAN KURT

Kriptografi Nedir ?

Kriptografi ya da '**şifreleme'** okunabilir durumdaki bir verinin içerdiği bilginin istenmeyen taraflarca anlaşılamayacak bir hale dönüştürülmesinde kullanılan yöntemlerin tümüdür.



SİFRELEME = VYIUHOHPH

1 Kriptografi Neden Önemli

Gizlilik bir ihtiyaç

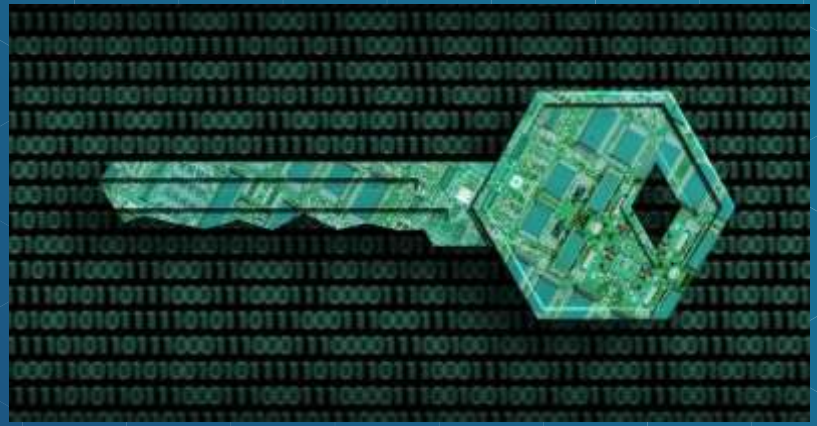
Kerckhoff Prensibi

- *“Bir şifrenin güvenliği, kolayca değiştirilemeyecek hiçbir şeye bağlı olmamalıdır”.*

- *"Rakip hafife alınmamalı. Özellikle rakip şifreleme ve şifre çözme algoritmalarını bilir. Dolayısıyla bir şifre sisteminin gücü, algoritmaya değil, anahtar bilgiyi gizli tutmaya bağlıdır.”*

Auguste Kerckhoff, 1883


1
ERİŞEBİLİRLİK
BİLGİ
GÜVENLİĞİ
2
BÜTÜNLÜK
3
GİZLİLİK



Kriptografik Sistemlerin Esasları

Bir kriptografik sistem, bilgi güvenliğini sağlamak için bir araya getirilmiş birçok küçük yöntemler bütünlüğü olarak görülebilir.

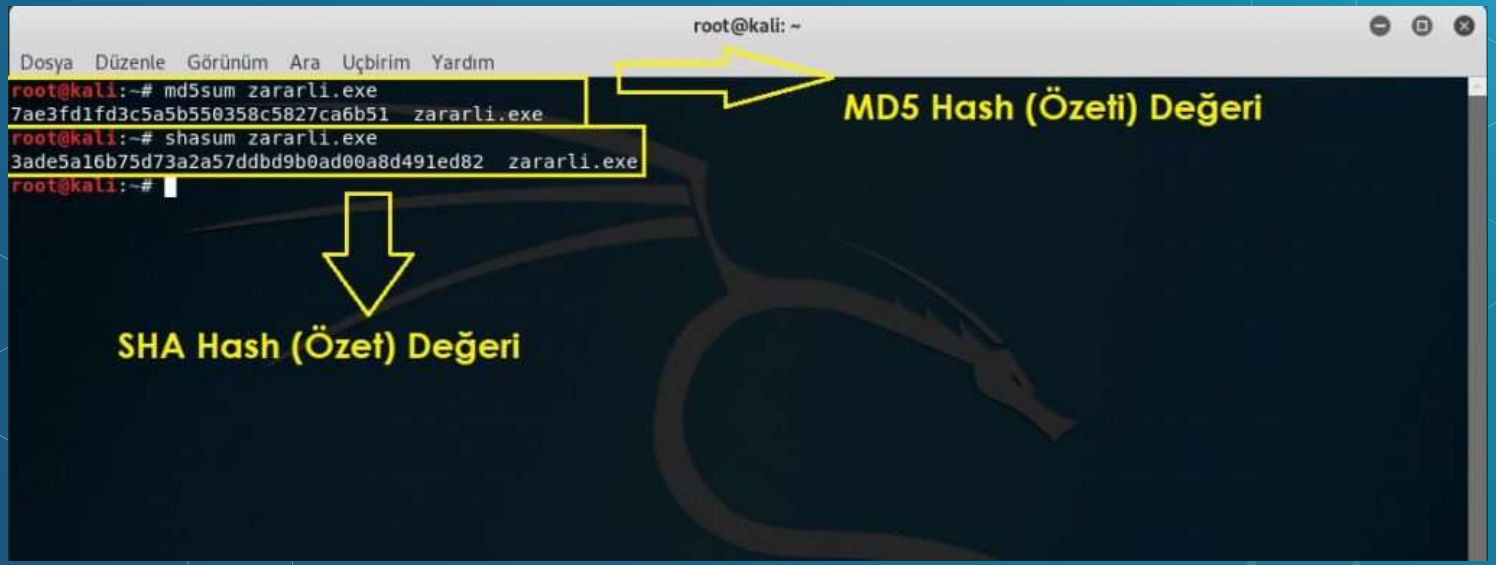
- Anahtarsız şifreleme
- Gizli anahtarlı şifreleme
- Açık anahtarlı şifreleme

Açık Anahtarlı Şifreleme

ŞİFRELEME DEĞİLDİR!!

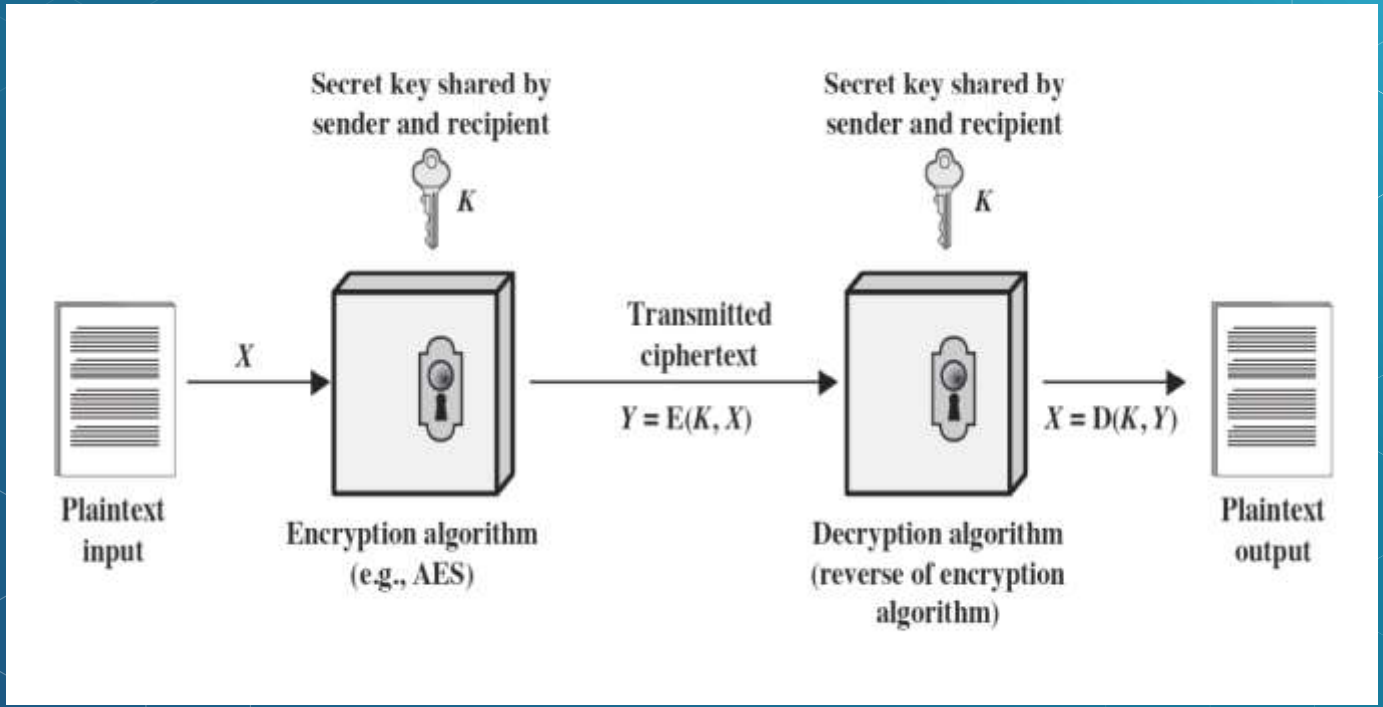
VERİ BÜTÜNLÜĞÜNÜ DOĞRULAMAK AMACIYLA KULLANILIR!

MD5, SHA-1, RIPEMD-160 gibi algoritmalar kullanılarak istenilen verinin özüt (hash) değeri ortaya çıkarılır.



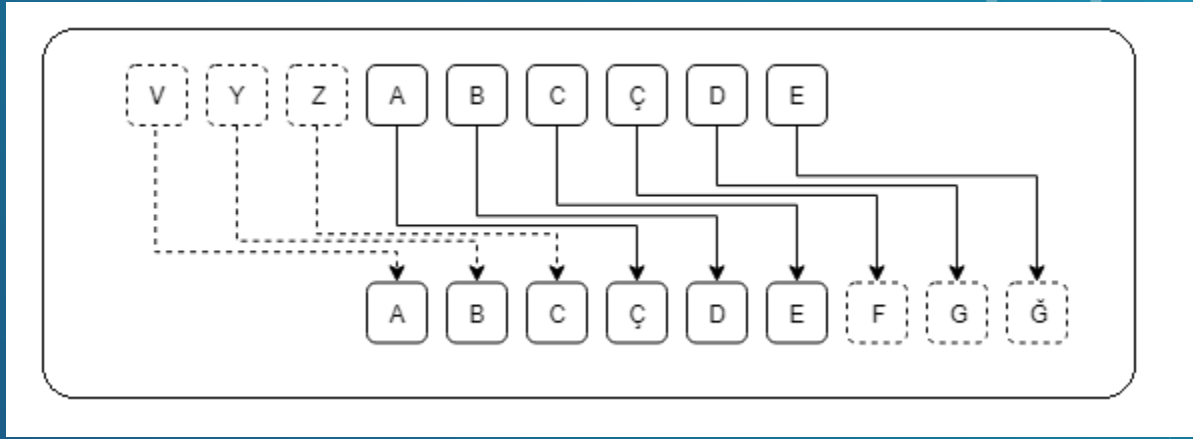
Gizli (simetrik) Anahtarlı Şifreleme

Gizli anahtarlı şifreleme ya da **simetrik şifreleme**, kriptografik yöntemlerden, hem şifreleme hem de deşifreleme işlemi için aynı anahtarı kullanan kripto sistemlere verilen isimdir.


Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D(K, Y)
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

- Sezar, Vigenere, DES, 3DES, RC5, Blowfish, IDEA SAFER, Monoalphabetic

Sezar şifreleme



– Mathematically give each letter a number

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
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

– Algorithm can be expressed as:

$C = E(3, p) = (p + 3) \bmod 26$ //Encryption

$p = D(3, C) = (C - 3) \bmod 26$ //Decryption

Monoalphabetic Şifreleme:

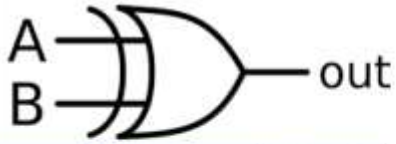
```
Plain:   abcdefghijklmnopqrstuvwxyz
Cipher:  DKVQFIBJWPESCXHTMYAUOLRGZN

Plaintext:   ifwewishtoreplaceletters
Ciphertext:  WIRFRWAJUHYFTSDVFSFUUFYA
```

26! = 4. 10^26 farklı anahtar

Vinegere Tablosu

Key \ Plaintext	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
b	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
c	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	B
d	D	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
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
f	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
g	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
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
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
j	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	I
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
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
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
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
o	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	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	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
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
s	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	R
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
u	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	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	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

```
key:          deceptivedeceptivedeceptive
plaintext:    wearediscoveredsaveyourself
ciphertext:   ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```



One-time Pad: Encryption

Inputs		Output
A	B	X
0	0	0
0	1	1
1	0	1
1	1	0

e=000 h=001 i=010 k=011 l=100 r=101 s=110 t=111

Encryption: Plaintext ⊕ Key = Ciphertext

	h	e	i	l	h	i	t	l	e	r
Plaintext:	001	000	010	100	001	010	111	100	000	101
Key:	111	101	110	101	111	100	000	101	110	000
Ciphertext:	110	101	100	001	110	110	111	001	110	101
	s	r	l	h	s	s	t	h	s	r

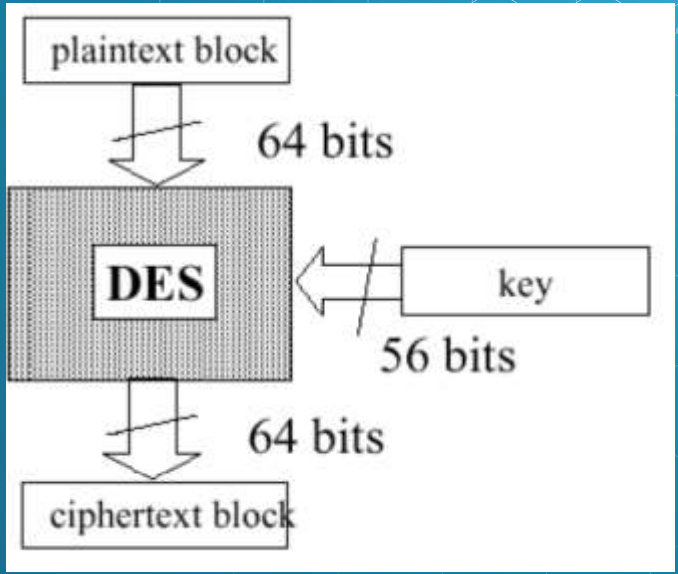
trsrtlerse ← Key:

	s	r	l	h	s	s	t	h	s	r
ciphertext:	110	101	100	001	110	110	111	001	110	101
key:	111	101	110	101	111	100	000	101	110	000
plaintext:	001	000	010	100	001	010	111	100	000	101
	h	e	i	l	h	i	t	l	e	r

trsrtlerse ←

DES/3DES

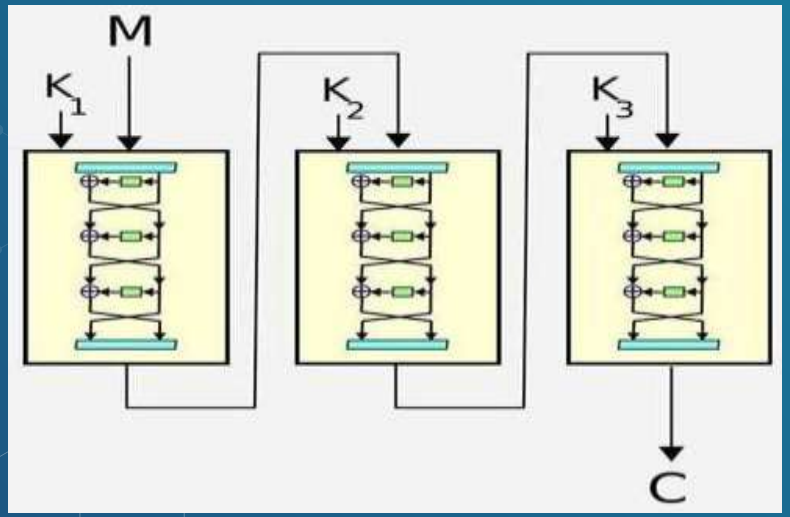
- DES bir blok-şifreleme, yani düz metni belirli büyüklükte bloklara (64 bit) böler ve aynı büyüklükte şifrelenmiş metni geri döndürür.

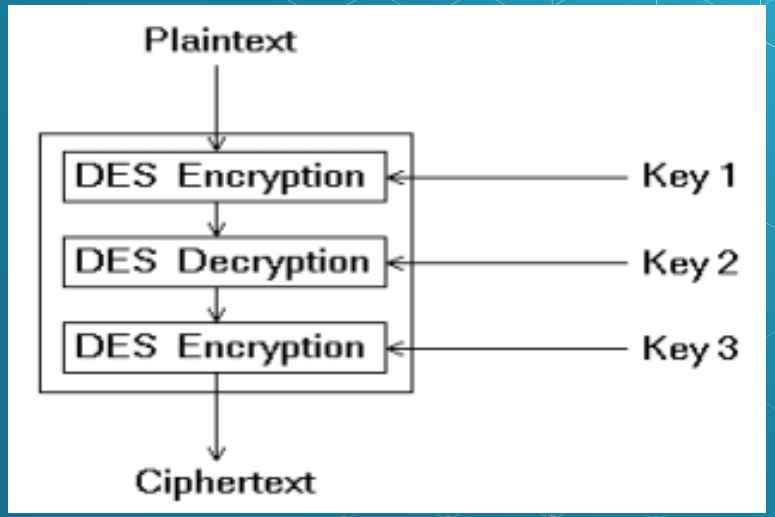


DES (Data Encryption Standard) dünyada en çok kullanılan şifreleme algoritmasıdır. Bir çok sene boyunca insanlar için 'güvenli şifreleme' işlemi DES birlikte anıldı.

Electronic Frontier Foundation'nın 220.000 dolara DES ile şifrelenmiş metinleri kıran bir makine geliştirmelerine rağmen, DES yeni versiyonu TRIPLE-DES ile uzunca süre bankalar ve devlet tarafından kullanılmaya devam edecek.

3DES





KEY= 168 BİT

Key size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 decryptions/s	Time Required at 10^{13} decryptions/s
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	2^{55} ns = 1.125 years	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	2^{127} ns = 5.3×10^{21} years	5.3×10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	2^{167} ns = 5.8×10^{33} years	5.8×10^{29} years
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	2^{191} ns = 9.8×10^{40} years	9.8×10^{36} years
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	2^{255} ns = 1.8×10^{60} years	1.8×10^{56} years
26 characters (permutation)	Monoalphabetic	$26! = 4 \times 10^{26}$	2×10^{26} ns = 6.3×10^{9} years	6.3×10^{6} years

Açık Anahtar (Asimetrik) İle Şifreleme

- **Açık anahtarlı şifreleme**, şifre ve deşifre işlemleri için farklı anahtarların kullanıldığı bir şifreleme sistemidir.

Avantaj ve Dezavantajları

- Simetrik şifreleme sistemleriyle karşılaştırıldığında, asimetrik sistemler çok daha yavaştır. Bu, şifrelemede kullanılan anahtarların uzunluğu ve yapılan işlemlerin karmaşıklığından kaynaklanmaktadır.
- Asimetrik şifreleme yöntemiyle şifrelenmiş bir bilgiyi aynı anda değişik kullanıcılara gönderebilmek için aynı bilginin her alıcı için ayrı ayrı şifrelenmesi gerekmektedir. Bu da şifreleme için ayrı bir yük getirmektedir.

Açık Anahtar Şifreleme Algoritmaları

- Diffie-Hellman
- ElGamal
- Paillier
- Blum–Goldwasser Kriptosistem
- Goldwasser-micali kriptosistemi
- Okamoto-Uchiyama Kriptosistemi

Diffie-Hellman Anahtar Değişimi

Alice				**Bob**		
Gizli	Açık	Hesaplar	Gönderir	Hesaplar	Açık	Gizli
a	p, g		p,g→			b
a	p, g, A	$g^a \bmod p = A$	A→		p, g	b
a	p, g, A		← B	$g^b \bmod p = B$	p, g, A, B	b
a, **s**	p, g, A, B	$B^a \bmod p = s$		$A^b \bmod p = s$	p, g, A, B	b, **s**

Alice ve Bob aralarında asal sayı olarak p=23 ve taban olarak g=5'i seçmeyi anlaşırlar.
Alice gizli bir tam sayı seçer a=6, ve Bob'a $A = g^a \bmod p$ hesaplayıp gönderir.

$A = 5^6 \bmod 23$

$A = 15.625 \bmod 23$

$A = 8$

Bob da gizli bir tam sayı seçer b=15, ve aynı şekilde Alice'e $B = g^b \bmod p$ hesaplayıp gönderir.

$B = 5^{15} \bmod 23$

$B = 30.517.578.125 \bmod 23$

$B = 19$

Alice $s = B^a \bmod p$ yi hesaplar.

$s = 19^6 \bmod 23$

$s = 47.045.881 \bmod 23$

$s = 2$

Bob da $s = A^b \bmod p$ yi hesaplar.

$s = 8^{15} \bmod 23$

$s = 35.184.372.088.832 \bmod 23$

$s = 2$

C Kodu Örneği

```c
#include <stdio.h>

// Function to compute `a^m mod n`
int compute(int a, int m, int n)
{
    int r;
    int y = 1;

    while (m > 0)
    {
        r = m % 2;

        // fast exponention
        if (r == 1) {
            y = (y*a) % n;
        }
        a = a*a % n;
        m = m / 2;
    }

    return y;
}
```

```c
// C program to demonstrate the Diffie-Hellman algorithm
int main()
{
    int p = 23;         // modulus
    int g = 5;         // base

    int a, b;     // `a` - Alice's secret key, `b` - Bob's secret key.
    int A, B;     // `A` - Alice's public key, `B` - Bob's public key

    // choose a secret integer for Alice's private key (only known to Alice)
    a = 6;         // or, use `rand()`

    // Calculate Alice's public key (Alice will send `A` to Bob)
    A = compute(g, a, p);

    // choose a secret integer for Bob's private key (only known to Bob)
    b = 15;         // or, use `rand()`

    // Calculate Bob's public key (Bob will send `B` to Alice)
    B = compute(g, b, p);

    // Alice and Bob Exchange their public key `A` and `B` with each other

    // Find secret key
    int keyA = compute(B, a, p);
    int keyB = compute(A, b, p);

    printf("Alice's secret key is %d\nBob's secret key is %d", keyA, keyB);

    return 0;
}
```

Output:

```
Alice’s secret key is 2
Bob’s secret key is 2
```

AMACA HİZMET ETMEK ÖNEMLİ

DİNLEDİĞİNİZ İÇİN TEŞEKKÜRLER