CENG 434 Kriptoloji – 6. Ders

Alper UĞUR

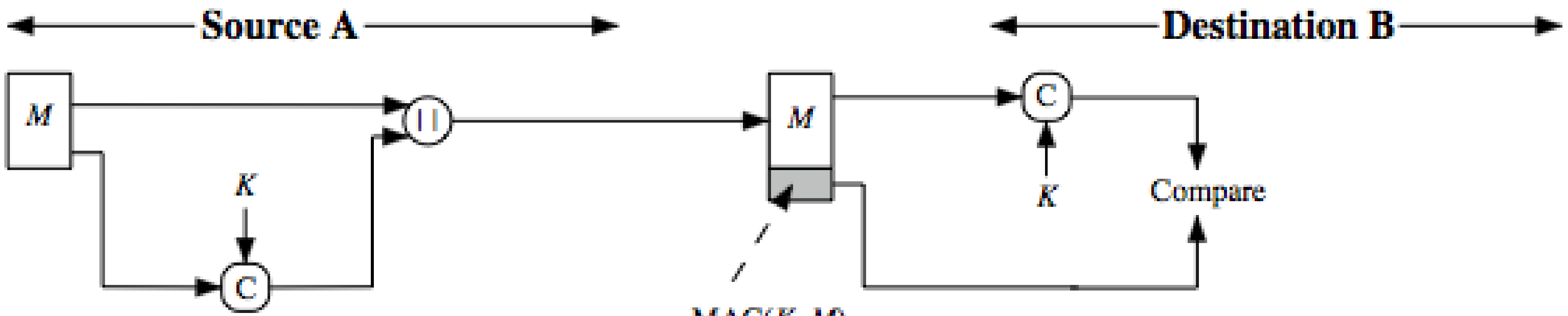
CENG 507 :
KRİPTOGRAFİK ALGORİTMALAR VE SİSTEMLER

CENG 434:
KRİPTOLOJİ

Bütünlük(Integrity)

- MAC (Message Authentication Code)
- MAC = C(K,M)
- Mesaj özeti HASH

a small fixed-sized block of data
generated from message + secret key
MAC = C(K,M)
appended to message when sent



(a) Message authentication

Özetleme Fonksiyonları (Hash Functions)

- Girdinin boyutu sınırlı olmamalı

  (No limitation for the size of input)
- Çıktının boyutu sabit olmalı

  (fixed-length output)
- H(M) fonksiyonu hesaplanması kolay olmalı

  (H(M) easy to calculate, implement)
- **Tek yönlülük:** H(M) =h ise bilinen h de M nin hesaplanması mümkün olmamalı

  One-way: H(M)=h where it is infeasible to computationally find M from h
- **Zayıf çakışma dayanıklılığı (weak collision resistance)**
  - H(M') = H(M) , M' ≠ M
- **Güçlü çakışma dayanıklılığı (strong collision resistance)**
  - (M,M') where H(M)=H(M')

Güvercin yuvası prensibi (Pigeon Hole Principle)

Güvercin Yuvası

- Güvercin sayısı ve yuva sayısı
- # of pigeon and # of holes

- Boş kalma (any unoccupied?)
- 1+ güvercin yerleşmesi
- (more than one pigeon in one hole)

http://www.matematikdunyasi.org/arsiv/PDF/03-I-50-51-GuvercinYuvasi.pdf

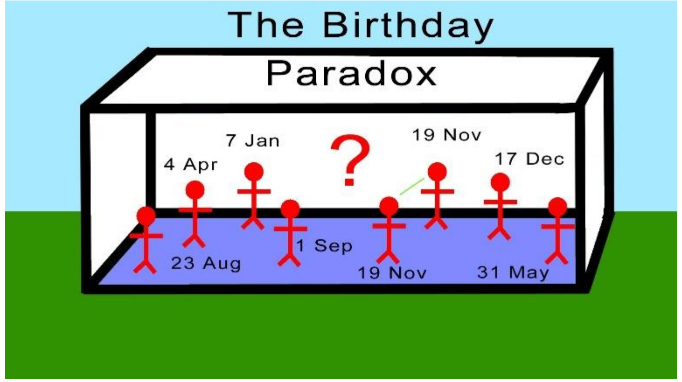
Doğumgünü İkilemi (Birthday Paradox)

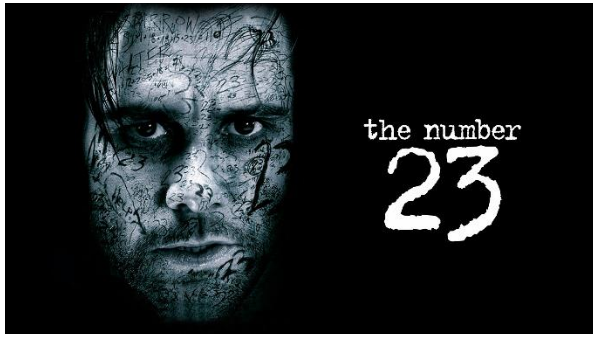
- Bir odada doğumgünü aynı olan iki kişinin olma olasılığı nedir?
(%100 : odadaki kişi sayısı?)
(%50: odadaki kişi sayısı?)

What’s the probability for two person having same birthday?
(%100 : # of person in the room?)
(%50: # of person in the room?)

$$22 + 21 + 20 + \cdots + 1 = 253$$

$$\binom{n}{2}=\binom{23}{2}= 23.22/2 =253$$





Özetleme Fonksiyonların Güvenliği (Security of Hash Functions)

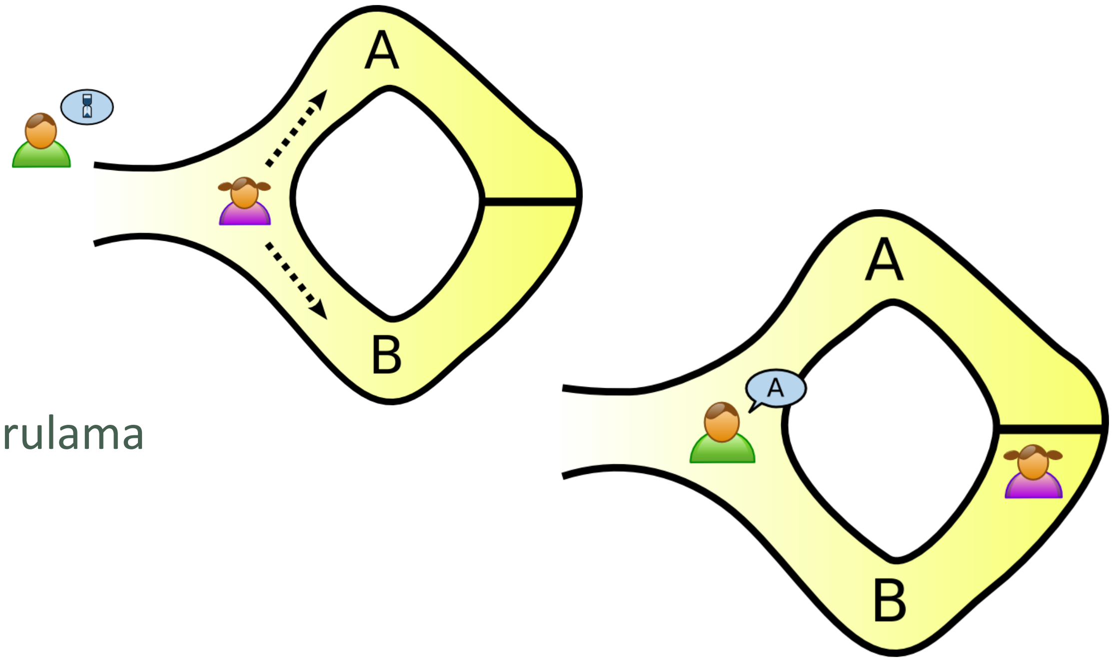
- Özet uzunluğu yeterli mi?
- MD5 sözlük saldırısı (dictionary attack) (16 karakter)
- SHA-1 (128bit)

MD5:5f4dcc3b5aa765d61d8327deb882cf99

http://md5.gromweb.com/

- SHA-3 Yarışma (hamsi : Özgül Küçük, spectral: Çetin Kaya KOÇ)

Zero Knowledge Proof



- Meydan okuma
- Etkileşimli doğrulama

- Amaç: Başka bir bilgi açığa çıkarmadan bir durumu doğrulama

(The goal is to prove a statement without leaking extra information)

- **Bütünlük (Completeness):**
- Eğer sonuç doğru ise doğrulayan yanıltılmayacaktır.
- if the statement is true, the honest verifier (that is, one following the protocol properly) will be convinced of this fact by an honest prover.
- **Geçerlilik(Soundness):**
- Eğer sonuç yanlış ise doğrulayan doğruluğa ikna edilemeyecektir.
  - (Her zaman düşük bir olasılık vardır)
  - if the statement is false, no prover, even if it doesn't follow the protocol, can convince the honest verifier that it is true,
  - except with some small probability

- **Zero-Knowledge:** Sonuç doğru ise doğrulayan bu durumdan ekstra bir bilgi öğrenememelidir.
- If the statement is true, verifier learns anything other than this fact.

Kriptografi ve Matematik

- Gruplar,Halkalar ve Alanlar
- Bölünebilirlik
- Aritmetiğin temel ilkesi
- EBOB
- Öklit
- Modüler aritmetik
- RSA
- Ayrık logaritma
- Diffie-Hellman

Groups, rings and fields
Divisibility
Fundamental principle of Arithmetic
Gcd
Euclid
Modular Arithmetic
RSA
Discrete Logarithm
Diffie-Hellman

Gruplar, Halkalar ve Alanlar

	(A1) Closure under addition:	If a and b belong to S, then $a + b$ is also in S
	(A2) Associativity of addition:	$a + (b + c) = (a + b) + c$ for all a, b, c in S
	(A3) Additive identity:	There is an element 0 in R such that $a + 0 = 0 + a = a$ for all a in S
Group	(A4) Additive inverse:	For each a in S there is an element $-a$ in S such that $a + (-a) = (-a) + a = 0$
Abelian group	(A5) Commutativity of addition:	$a + b = b + a$ for all a, b in S
	(M1) Closure under multiplication:	If a and b belong to S, then ab is also in S
	(M2) Associativity of multiplication:	$a(bc) = (ab)c$ for all a, b, c in S
Ring	(M3) Distributive laws:	$a(b + c) = ab + ac$ for all a, b, c in S $(a + b)c = ac + bc$ for all a, b, c in S
Commutative ring	(M4) Commutativity of multiplication:	$ab = ba$ for all a, b in S
	(M5) Multiplicative identity:	There is an element 1 in S such that $a1 = 1a = a$ for all a in S
Integral domain	(M6) No zero divisors:	If a, b in S and $ab = 0$, then either $a = 0$ or $b = 0$
Field	(M7) Multiplicative inverse:	If a belongs to S and $a \neq 0$, there is an element a^{-1} in S such that $aa^{-1} = a^{-1}a = 1$

Bölünebilirlik

- *a,d,q* birer tamsayı olmak üzere a için *a=dq* şeklide bir *(d,q)* varsa

a, d' ye bölünebilirdir. *d bölen, a bölünen q bölüm*

Eğer *a 2*'ye bölünebilirse *a* çifttir. Böünemezse *a* tektir.
a tamsayısının çift olması için *a=2k* eşitliğini sağlayan bir *k* tamsayısı vardır.

a,b ve c tamsayılar olmak üzere. *a, b* ye *b* de *c* ye bölünebilir ise *a, c* ye bölünebilirdir.
Bölme algoritması : *a=dq+r (a ve d verildiğinde q ve r'yi bulma)*

Aritmetiğin Temel İlkesi

- Her pozitif tamsayı 2 veya daha fazla asal sayının çarpımı ile ifade edilebilir. (Asalsa 1 ile kendisinin çarpımı)

EBOB En büyük ortak bölen (gcd: greatest common divisor)

- (a,b) tamsayı ikilisini bölen en büyük tamsayı, d a ve b d ye bölünebilir.
- $(a_1, a_2, \ldots, a_{n-1}, a_n)$ tamsayıları için a_i nin EBOB'u d
- *$gcd(a,b)=d= \min\{ma+nb>0 : m,n \in Z\}$*

- *Eğer gcd(a,b)=1 ve a, bc yebölünebilirse, a c ye bölünebilirdir.*

Öklit algoritması (Euclidean Algorithm)

- Bölme algoritması : *a=bq+r*
- *a=bq+r ; gcd(a,b) =gcd(b,r) dir.*
- İpucu : *r= a-bq*

- Örnek: gcd(270,192)
  - 270=192*1+78   *a=bq1+r1*
  - 192=78*2+36   b=r1*q2+r2
  - 78=36*2+6   r1=r2*q3+r3
  - 36=6*6+0   r2=r3*q4+r4 , ri=0 qi =gcd(a,b)

Öklit algoritması (Euclidean Algorithm)

- Bölme algoritması : *a=bq+r*
- *a=bq+r ; gcd(a,b) =gcd(b,r) dir.*
- İpucu : *r= a-bq*

```
function Euclid(a,b)
   if b = 0 return(a)
return(Euclid(b,a mod b))
```

```
Extended-Euclid(a, b)
if b = 0 return(a,1,0)
Compute k such that a = bk+(a mod b
(d,x,y) = Extended-Euclid(b,a mod b
return((d,y,x-ky))
end Extended-Euclid
```

- Örnek: gcd(270,192)
  - 270=192*1+78 — *a=bq1+r1*
  - 192=78*2+36 — b=r1*q2+r2
  - 78=36*2+6 — r1=r2*q3+r3
  - 36=6*6+0 — r2=r3*q4+r4 , ri=0 qi =gcd(a,b)

x,y

Modüler Aritmetik

- *a =qn+r   0<=r <n ; q= l_ a/n _l*
- *a= l_ a/n _l .n + (a mod n)*
- *r= a mod n*

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

x	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Çarpmaya göre tersi
5.X =1 mod 67
67= 13.5+2
5=2.2+1
2=2.1+0

1
1=5-2.2
=5-2(67-13.5)
=5(1+2.13) -2.67
=5.27-2.67

```
Extended-Euclid(a, b)
if b = 0 return(a,1,0)
Compute k such that a = bk+(a mod b)
(d,x,y) = Extended-Euclid(b,a mod b)
return((d,y,x-ky))
end Extended-Euclid
```

x,y

- a^{-1} *mod n*
- *(a.*a^{-1} *= 1 mod n)*
- *gcd(a,n) =1 olmalı*

- *Extended Euclid: gcd(a, n) x; y*
- *öyle ki ax+ny= 1 , x=*a^{-1}*mod n*

a^{-1} *mod n (Neden ihtiyaç duyuyoruz?)*

- RSA (Rivest Shamir Adleman)

- e: açık anahtar
- d: gizli anahtar

olmak üzere
e.d =1 mod n bulunabilirse (d =e^{-1} *mod n)*

Şifreleme fonksiyonu
E(M) = M^e mod n

Şifre çözme fonksiyonu
D(E(M)) = (E(M))^d *mod n*

olarak tanımlanabilir.

- a^{-1} *mod n*
- *(a.a^{-1} = 1 mod n)*
- *gcd(a,n) =1 olmalı*

İspat:
(E(M))^d *mod n*
=(M^e)^d mod n

Biliyoruz ki d =e^{-1} *mod n*
=$M^{e.\,e-1}$ mod n
=M mod n

RSA Asimetrik Şifreleme (Açık anahtarlı kriptografi) (Public Key Cryptography)

- RSA (Rivest Shamir Adleman)

- e: açık anahtar
- d: gizli anahtar

olmak üzere
e.d =1 mod n bulunabilirse
(d =e^{-1} *mod n)*

Şifreleme fonksiyonu
E(M) = M^e mod n

Şifre çözme fonksiyonu
D(E(M)) = $(E(M))^d$ *mod n*

olarak tanımlanabilir.

e,d nasıl seçilir?
1-p,q iki büyük asal sayı (yaklaşık aynı büyüklükte)
(Ne kadar büyük? = birkaç yüz basamaklı)
2-n=pq hesaplar
3- Rasgele bir e hesaplar
Öyle ki
e tamsayısı için gcd ((p-1)(q-1),e) =1 şartı sağlanmalıdır.
(aralarında asal)
4- d tamsayısını hesaplar
Öyle ki d =e^{-1} mod (p-1)(q-1) (Nasıl? Öklit ile)

Açık anahtar: (e,n)
Gizli anahtar: (p,q,d)

(p-1) ve (q-1) de gizli tutuluyor ;)

- *Extended Euclid: gcd(a, n) x; y*
- *öyle ki ax+ny= 1 , x=a^{-1}mod n*

RSA ispatı

- RSA (Rivest Shamir Adleman)

- e: açık anahtar
- d: gizli anahtar

olmak üzere
e.d =1 mod n bulunabilirse (d =e^{-1} *mod n)*

Şifreleme fonksiyonu
E(M) = M^e mod n

Şifre çözme fonksiyonu
D(E(M)) = $(E(M))^d$ *mod n*

olarak tanımlanabilir.

Fermat'ın küçük teoremi (Fermat's Little Theorem) ile İspat:

Eğer p asal ve a, 0 dan farklıysa
a^{p-1}= 1 mod p dir. [gcd(a,p) =1]

d =e^{-1} mod (p-1)(q-1) hesaplamıştık

O zaman d.e = 1 mod (p-1)(q-1) olmalı

$(E(M))^d = M^{d.e}$

a^{p-1}= 1 mod p dir.

$= M^{1+k.(p-1)(q-1)}$
= M mod n
mod p ve mod q ya göre doğrula
n= pq
mod n için de doğrudur

RSA ispatı

- RSA (Rivest Shamir Adleman)

- e: açık anahtar
- d: gizli anahtar

olmak üzere
e.d =1 mod n bulunabilirse (d =e^{-1} *mod n)*

Şifreleme fonksiyonu
E(M) = M^e mod n

Şifre çözme fonksiyonu
D(E(M)) = $(E(M))^d$ *mod n*

olarak tanımlanabilir.

$(E(M))^d = M^{d.e}$
$= M^{1+k.(p-1)(q-1)}$
= M mod n

$M^{d.e}$ =? M mod n
Biliyoruz ki
d.e = mod ϕ(n)

$= M^{1+k.(p-1)(q-1)}$
= M mod n

Euler e göre İspat:

Tanım: Euler phi ϕ(n) fonksiyonu : (Euler totient)
n bir tamsayı olmak üzere
ϕ(n): n den küçük ve n ile aralarında asal olan sayıların adedi
n= 9 olsun ϕ(n) = 6 dır 1,2,4,5,7,8

Euler teoremi: *n* ve *a* tamsayı ve gcd(*n,a*)=1 ise
$a^{\phi(n)}$ = 1 mod p dir.

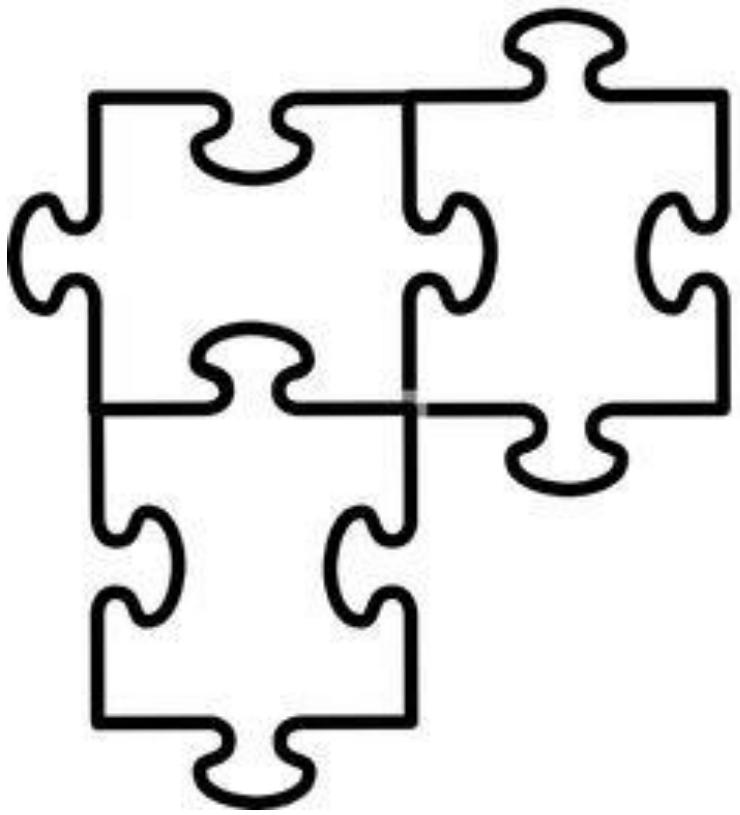
n= 4 a=15 ϕ(n) =2 {1,2}
$a^{\phi(n)}$ = 15^2=225 tir.
*225 = 1 mod 4 (224=56*4)*

Lemma: Eğer n asal sayı ise ϕ(n) =n-1 dir.
Lemma: Eğer p ve q asalsa ϕ(pq) = ϕ(p) ϕ(q) dir.

RSA
n=pq ϕ(n) = ϕ(pq) = ϕ(p) ϕ(q) =(p-1)(q-1)

d =e^{-1} mod (p-1)(q-1) hesaplamıştık (gcd(e, ϕ(pq)) =1)

Ara - 15dk

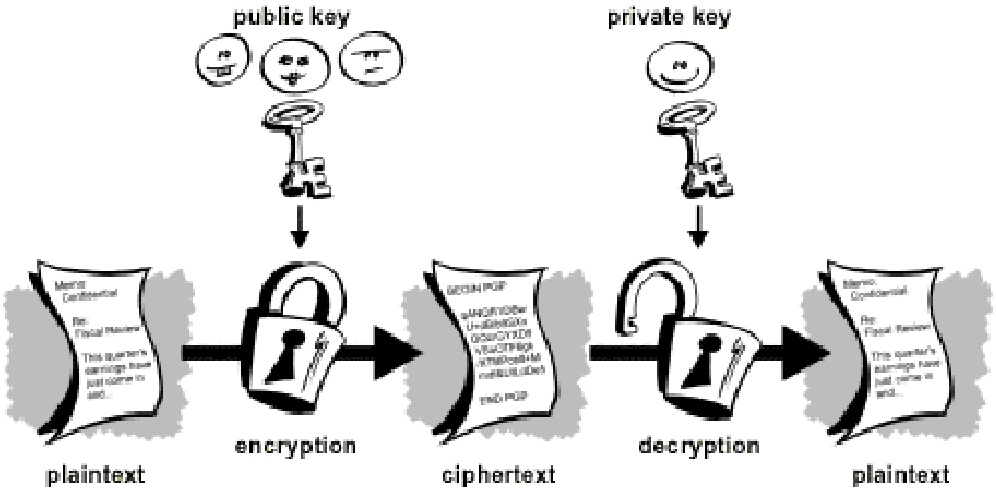


RSA Asimetrik Şifreleme (Açık anahtarlı kriptografi) (Public Key Cryptography)

- RSA (Rivest Shamir Adleman)

- e: açık anahtar (n biliniyor)
- d: gizli anahtar (p ve q gizleniyor)

olmak üzere
e.d =1 mod n bulunabilirse
(d =e^{-1} *mod n)*



Şifreleme fonksiyonu
E(M) = M^e mod n

Şifre çözme fonksiyonu
D(E(M)) = (E(M))^d *mod n*

olarak tanımlanabilir.

RSA Asimetrik Şifreleme (Açık anahtarlı kriptografi) (Public Key Cryptography)

- RSA (Rivest Shamir Adleman)

- e: açık anahtar (n biliniyor)
- d: gizli anahtar (p ve q gizleniyor)

olmak üzere
e.d =1 mod n bulunabilirse
(d =e^{-1} *mod n)*

Şifreleme fonksiyonu
E(M) = M^e mod n

Şifre çözme fonksiyonu
D(E(M)) = $(E(M))^d$ *mod n*

olarak tanımlanabilir.

Neden güvenli?

$M^{e.d}$ hesaplamak kolay

ϕ(n)=(p-1)(q-1) çarpanlara ayırma problemi zor
d =e^{-1} mod ϕ(n)

lnl =155

n = 10941738641570527421809707322040357612003732945449205990913842131476349984288934784717997257891267332497625752899781833797076537244027146743531593354333897

p = 102639592829741105772054196573991675900716567808038066803341933521790711307779,
q = 106603488380168454820927220360012878679207958575989291522270608237193062808643

Ayrık Logaritma Problemi

- G çarpmaya göre dairesel bir grup (multiplicative cyclic group)
- g bu grubun üreteci olsun. (Tüm a ∈ G g^x)
- $g^x = a$ kolay
- $x = \log_g a$ zor

- $g^x = a \bmod q$
- $g^y = a \bmod q$

x	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Diffie-Hellman Anahtar Değişimi

- $g^a \bmod p = A$

(g, p, A)

- $g^b \bmod p = B$

(g, p, B)

- $B^a \bmod p = S_{AB}$

- $A^b \bmod p = S_{AB}$

Diffie-Hellman Anahtar Değişimi

- $g^a \bmod p = A$
- $B^a \bmod p = S_{AB}$
- $(g^b)^a \bmod p = S_{AB}$

(g, p, A)

(g, p, B)

- $g^b \bmod p = B$
- $A^b \bmod p = S_{AB}$
- $(g^a)^b \bmod p = S_{AB}$