



Açık Anahtarlı Şifreleme ve Mesaj Kimlik Doğrulaması

Dr. Fatih KALEMKUŞ
Kafkas Üniversitesi

Asimetrik (Açık Anahtar) Şifreleme Algoritmaları

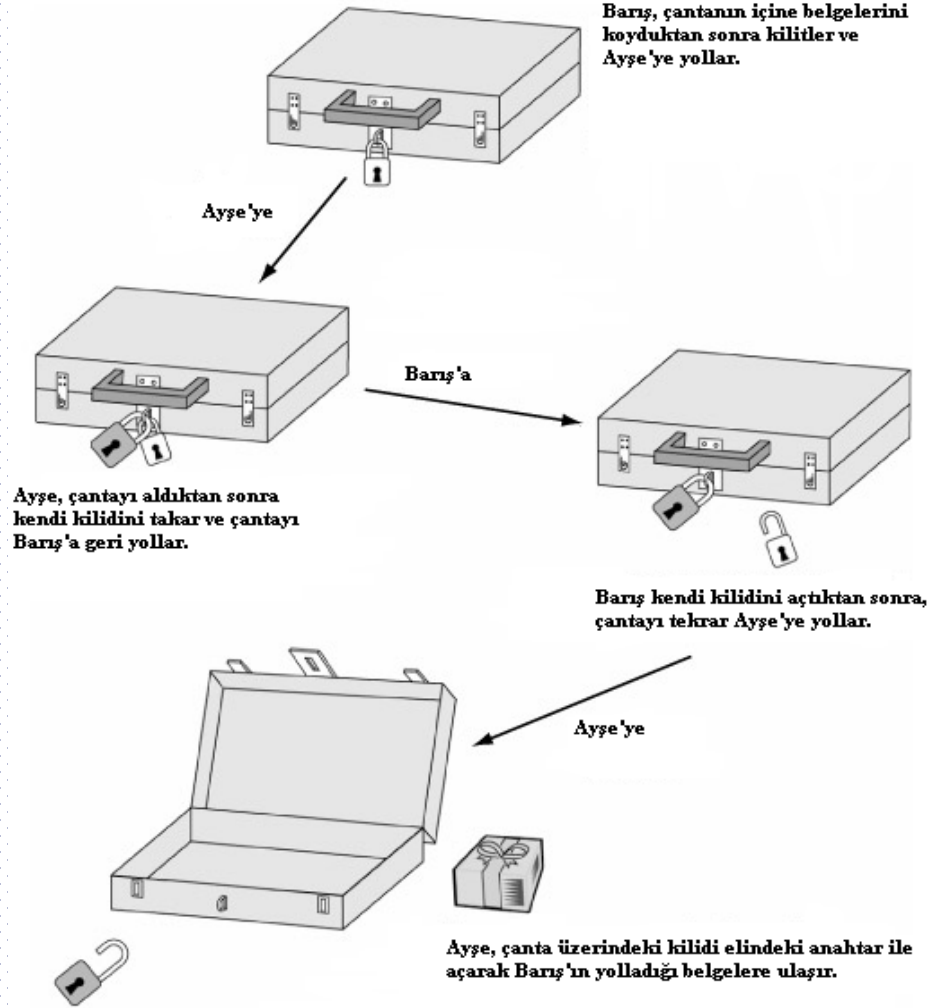
- RSA
- Diffie-Hellman
- DSA
- Eliptik Eğriler

Asimetrik Kriptografi (Açık Anahtar Kriptografisi)

- 1976 yılında Diffie ve Hellman
- Gizliliğin yanı sıra, kimlik doğrulama ve inkar edememe
- Simetrik Kriptografi'deki anahtar dağıtımı sorununa çözüm
- Gizli ve açık, iki çeşit anahtar mevcut
 - Açık anahtarlar herkes tarafından bilinir.
 - Gizli anahtarlar kişiye özeldir.

Diffie-Hellman Anahtar Değişimi

- Gizli anahtarlı sistemlerde şifreleme ve şifre çözme için ortak bir anahtar gerekmektedir.
- Diffie-Hellman anahtar değişimi bu anahtarı oluşturmak için kullanılmaktadır.
- Sonlu cisimler üzerinde veya eliptik eğri aritmetiğinde bu anahtar değişiminin uygulaması yapılabilmektedir.



Ayrık Logaritma Problemi

➤ $Z_p^* = \{1, 2, \dots, p-1\}$

Z_p^* 'de g ve y verilmiş ve $g^x = y \pmod{p}$
ise x kaçtır?

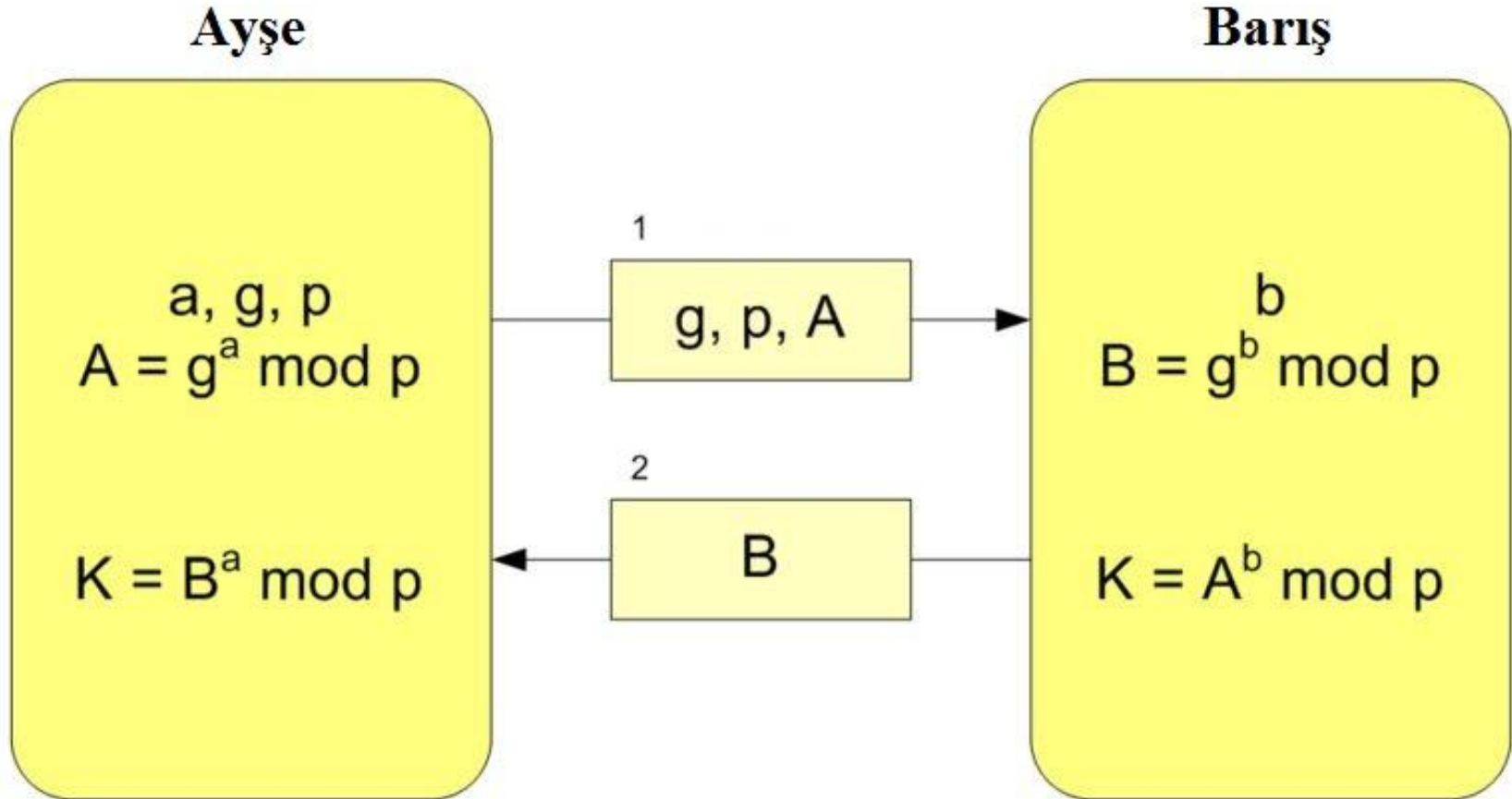
$x = \log_g y$ bulunması zor bir problemdir.

Örnek: Z_{17} 'de $g=3$ ve $y=11$,

$$3^x = 11 \pmod{17} \Rightarrow x = ?$$

$3^1 \pmod{17}$	$= 3$
$3^2 \pmod{17}$	$= 9$
$3^3 \pmod{17}$	$= 10$
$3^4 \pmod{17}$	$= 13$
$3^5 \pmod{17}$	$= 5$
$3^6 \pmod{17}$	$= 15$
$3^7 \pmod{17}$	$= 11$
$3^8 \pmod{17}$	$= 16$
$3^9 \pmod{17}$	$= 14$
$3^{10} \pmod{17}$	$= 8$
$3^{11} \pmod{17}$	$= 7$
$3^{12} \pmod{17}$	$= 4$
$3^{13} \pmod{17}$	$= 12$
$3^{14} \pmod{17}$	$= 2$
$3^{15} \pmod{17}$	$= 6$
$3^{16} \pmod{17}$	$= 1$
$3^{17} \pmod{17}$	$= 3$

Diffie-Hellman Anahtar Değişimi



$$K = A^b \text{ mod } p = (g^a \text{ mod } p)^b \text{ mod } p = g^{ab} \text{ mod } p = (g^b \text{ mod } p)^a \text{ mod } p = B^a \text{ mod } p$$

Asimetrik Kriptografi



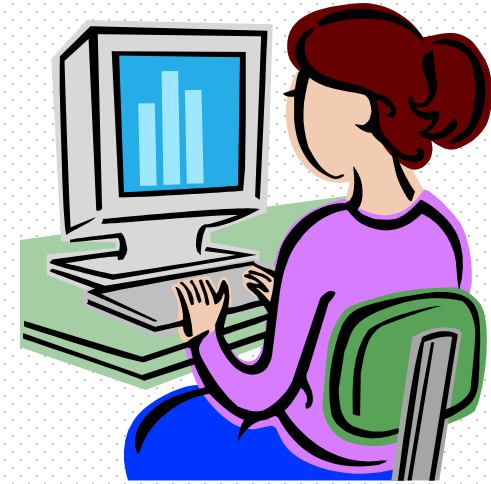
BARIŞ



AÇIK



GİZLİ



AYŞE

Açık Anahtar Şifreleme Uygulamaları

Şifreleme /Şifre Çözme (Encryption/Decryption)

– mesaj alıcınının açık anahtarı ile şifrelenir.

Dijital İmza (Digital signature)

– gönderici, mesajını (genelde mesaj özetini) kapalı anahtarı ile şifreler.

Anahtar Değişimi (Key Exchange)

– Simetrik şifreleme algoritmasınının gizli anahtarını, iki taraf paylaşması gerekiyor.

Basitçe, taraflardan biri bu anahtarı belirler ve alıcınının açık anahtarı ile şifreler ve alıcıya iletir.

Açık Anahtarlı Şifreleme için Gereksinimler

Kullanıcı B kolayca, açık anahtarlı şifreleme için anahtar ikilisini yaratabilir: açık anahtar (public key) PU_b ;
gizli anahtar (private key) PR_b

Kullanıcı A da benzer şekilde açık anahtar ikilisini yaratır:
açık anahtar(public key) PU_a ;
gizli anahtar (private key) PR_a

Kullanıcı A, izleyen mesaj M için açık anahtar şifrelemeyi, **Kullanıcı B** nin açık anahtarı ile yapar:

$C = E_{PU_b}(M)$ 'yi **Kullanıcı B** ye gönderir.

Kullanıcı B ise gizli anahtarını ve şifre çözme algoritmasını kullanarak C den, **Kullanıcı A**, nın gönderdiği M mesajını elde eder: $D_{PR_b}(C) = D_{PR_b}[E_{PU_b}(M)] = M$

Açık Anahtarlı Şifreleme Gereksinimleri

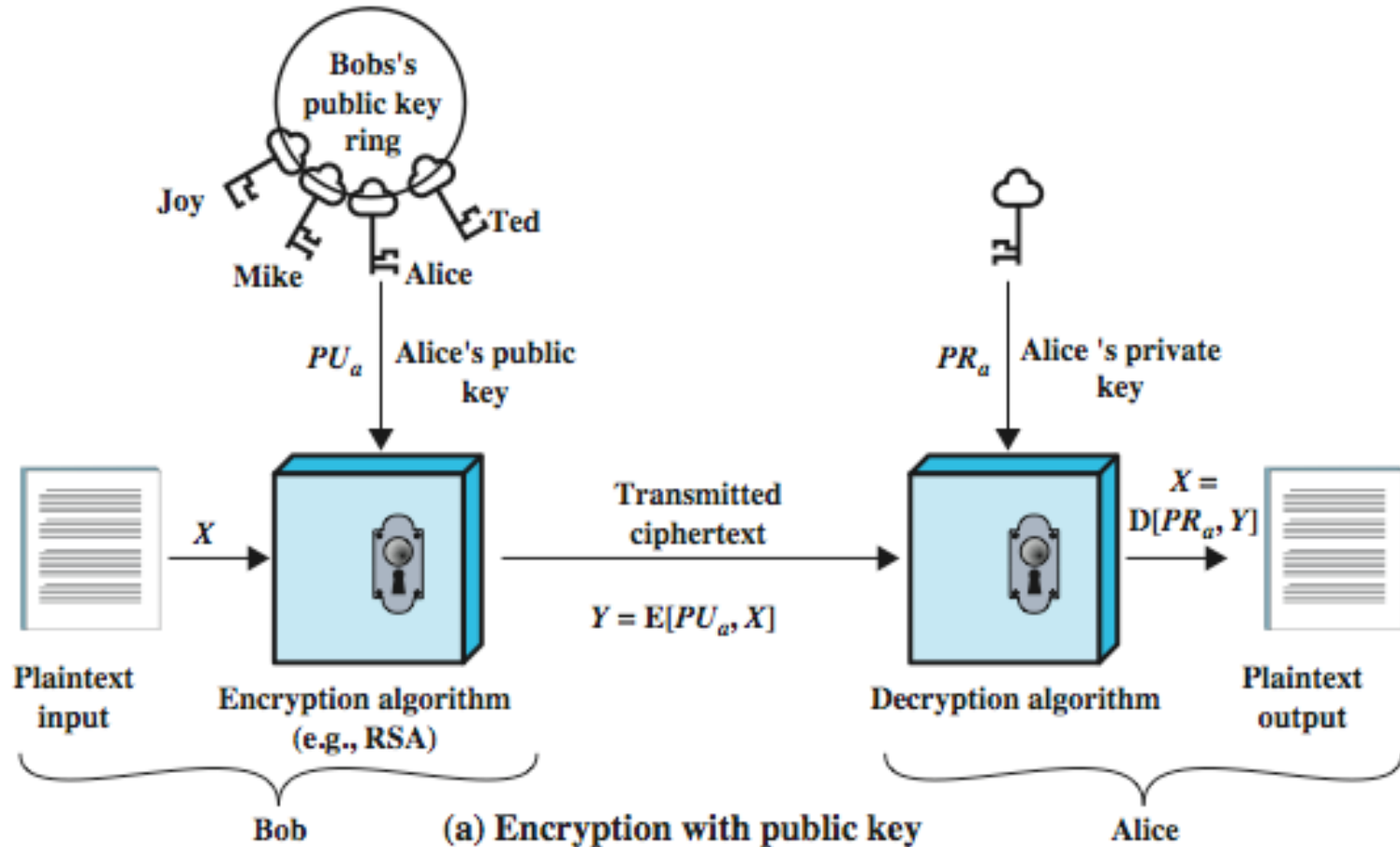
$$C = E_{PU_b}(M)$$

Kötü niyetli veya erişim yetkisi olmayan için:

- PU_b dan PR_b elde etmesi hesaplama açısından mümkün olmamalı.
- PU_b ve C yi kullanarak M elde etmek hesaplama açısından mümkün olmamalı.
- PU_b ve PR_b arasında matematiksel bir bağ mevcuttur. (trap-door)

$$M = D_{PR_b}[E_{PU_b}(M)] = D_{PU_b}[E_{PR_b}(M)]$$

Pratik bir açık anahtar sistemi için uygun bir trap-door fonksiyonuna ihtiyaç vardır.



SİMETRİK (GELENEKSEL) VE ASİMETRİK (AÇIK ANAHTARLI) ŞİFRELEME KARŞILAŞTIRMASI

Geleneksel Şifreleme (Conventional Encryption)

Çalışması İçin Gerekenler:

1. Şifreleme ve şifre çözme için aynı anahtarla aynı algoritma kullanılır.
2. Gönderici ve alıcı algoritmayı ve anahtarı paylaşmak zorundadır.

Güvenlik İçin Gerekenler:

1. Anahtar gizli tutulmalıdır.
2. Başka bilgi yoksa, mesajın çözülmesi imkansız veya en azından pratik olmamalıdır.
3. Algoritmanın bilinmesi ve şifreli örneklerin elde edilmesi, anahtarı belirlemek için yeterli olmamalıdır.

Açık Anahtarlı Şifreleme (Public-Key Encryption)

Çalışması İçin Gerekenler:

1. Şifreleme ve şifre çözme için bir çift anahtar kullanılır: biri şifreleme, diğeri şifre çözme için.
2. Gönderici ve alıcı eşleşmiş anahtar çiftinden birine (aynı olmayan) sahip olmalıdır.

Güvenlik İçin Gerekenler:

1. İki anahtardan biri gizli tutulmalıdır.
2. Başka bilgi yoksa, mesajın çözülmesi imkansız veya en azından pratik olmamalıdır.
3. Algoritmanın, anahtarlardan birinin ve şifreli örneklerin bilinmesi, diğer anahtarın belirlenmesi için yeterli olmamalıdır.

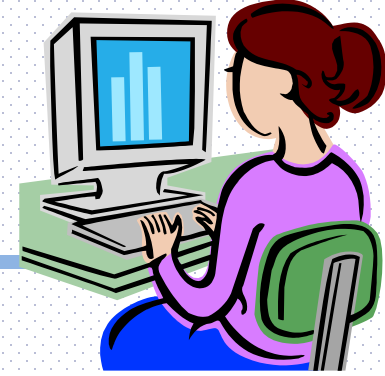
RSA Algoritması

- 1977 - Ron Rivest, Adi Shamir ve Leonard Adleman
- Çarpanlara ayırmanın zorluğunu temel alır
- Şifreleme ve elektronik imza uygulamalarında kullanılmaktadır.

RSA Algoritması

- Çarpanlara ayırma problemi nedir ?
- Verilen N sayısını bölen asal sayıları bulmak.
- 187'in asal çarpanları nelerdir?
- 12524224246730422698081804002962677144908939996961633338
1049941622953718673240322529328207020354780888067722576207
2069660129919434461376409226606711070377545994535659859425
8251300949290798217344667521645463459276100019171025163859
0123948630732326307922952494464857505415177402322499891218
582307842351942219477?

Dr. Fatih KALEMKUŞ



RSA'da Anahtar Oluşturma

➤ Ayşe iki asal sayı p ve q 'yu seçer.

Örnek $p=17$ ve $q=11$

➤ $N = p \times q$ 'yu elde eder.

$$N = 17 \times 11 = 187$$

➤ $\phi(N) = (q-1) \times (p-1)$ 'i hesaplar.

$$\phi(N) = 16 * 10 = 160$$

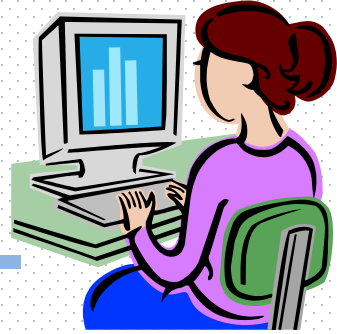
➤ $1 < e < \phi(N)$ ve $\text{obeb}(e, \phi(N))=1$ olan bir e seçer.

$e = 7$ diyelim;

✓ $1 < e=7 < 160$ ve $\text{obeb}(7,160)=1$

$$p = 17 \quad q = 11$$

$$N = 187 \quad e = 7$$



RSA'da Anahtar Oluşturma

➤ $1 < d < \varphi(N)$ ve $e \times d = 1 \pmod{\varphi(N)}$ olan d 'yi bulur

$$7 \times d = 1 \pmod{160} \Rightarrow d = 23$$

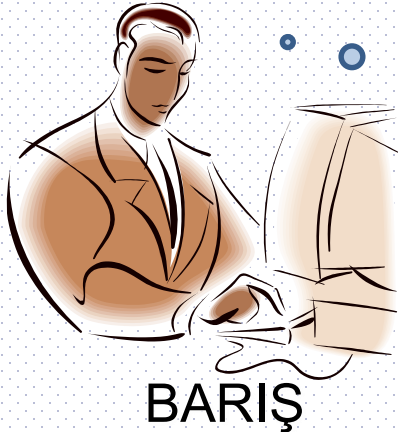
➤ Böylece Ayşe gizli p , q ve d anahtarlarını, açık N ve e anahtarlarını oluşturmuş olur.

➤ $e=65537 = (2^{16}-1)$ hızlı şifreleme

Gizli Anahtarlar: $p = 17$ $q = 11$ $d = 23$

Açık Anahtarlar: $N = 187$ $e = 7$

RSA – Şifreleme

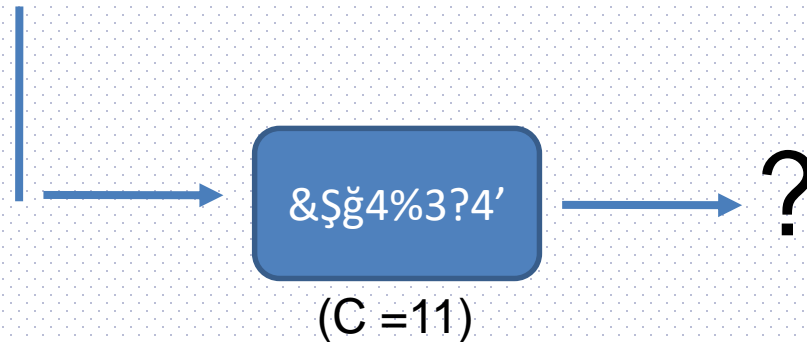


- m =Merhaba ($m = 88$)
- $C = m^e \pmod{N}$
- $C = 88^7 = 11 \pmod{187}$



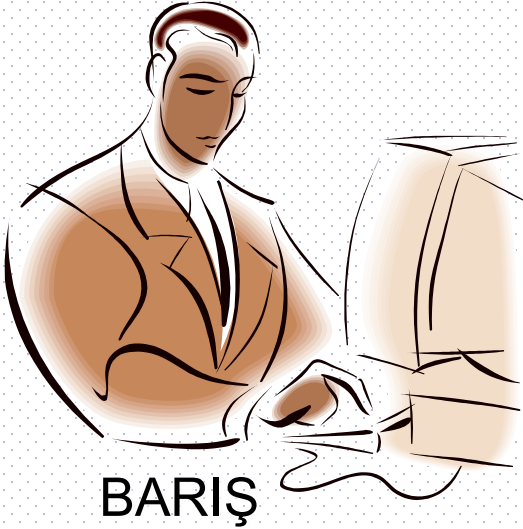
Gizli: $p=17, q=11, d=23$

Açık: $N=187, e=7$



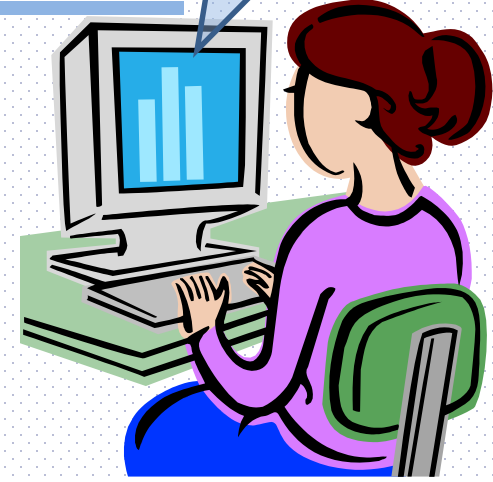
AYŞE

RSA – Şifre Çözme



&Şğ4%3?4'
(C = 11)

Bariş:
Merhaba



Anahtarlar

Açık: $N=187$, $e=7$

Gizli: $p=17$, $q=11$, $d=23$

- $C = 11$

- $m = C^d \pmod{N}$

-> $m = 11^{23} = 88 \pmod{187}$

-> $m = \text{Merhaba}$

***CRT kullan, mod p & q
ayrı ayrı hesapla.

Doğrudan yapmaya
göre 4 kat daha hızlı

RSA nasıl çalışır? Matematiksel teori?

Euler's Theorem:

$$a^{\varphi(n)} \bmod n = 1 \text{ where } \gcd(a, n) = 1$$

RSA:

$$n = p \cdot q$$

$$\varphi(n) = (p-1)(q-1)$$

e & d sayıları $\bmod \varphi(n)$ 'ye göre birbirlerinin tersi

Yani $e \cdot d = 1 + k \cdot \varphi(n)$ bir tamsayı k için

dolayısıyla :

$$\begin{aligned} C^d &= M^{e \cdot d} = M^{1+k \cdot \varphi(n)} = M^1 \cdot (M^{\varphi(n)})^k \\ &= M^1 \cdot (1)^k = M^1 = M \bmod n \end{aligned}$$

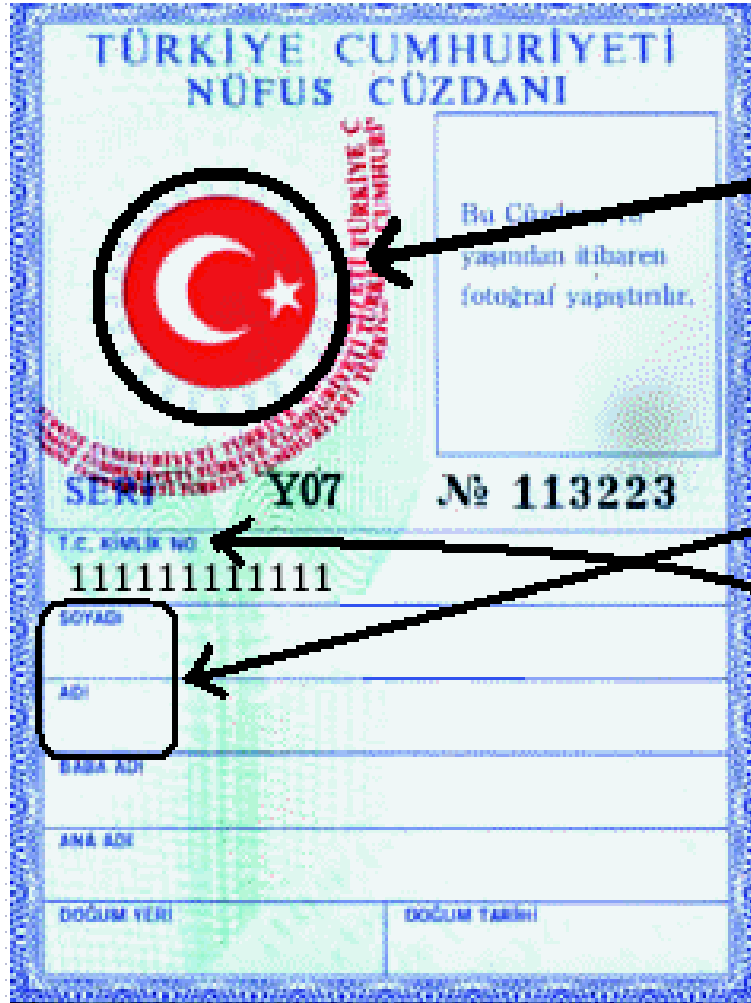
RSA Güvenilirliği

- **Deneme-yanılma saldırısını (Brute force attack):** Tüm olası anahtarları deneyerek bulmaya dayanıklılık için büyük e ve d seçilebilir.
- Nekadar büyük anahtar kullanılır ise açık şifreleme algoritması o kadar yavaşlayacak.
- Çok büyük n için büyük iki asal sayı çarpanını bulmak zor bir problemdir.
- 1994 yılında 428 bit RSA n çarpanlarına ayrıldı. Ödül: **\$100**
- 2010 yılı başlarında 768 bit uzunluğunda n tam sayısı (232 ondalık basamaklı), “**Number Field Sieve**” algoritması ile çarpanlarına ayrılmıştır (<http://eprint.iacr.org/2010/006.pdf>).
- Standartlar, RSA için n nin en az 2048 bit olmasını tavsiye ediyor.

Elektronik İmza

- Gönderilmek istenen belgeye eklenen kimlik doğrulama amacıyla kullanılan elektronik veriye elektronik imza adı verilir.
- E-imza sanal ortamda ıslak imzanın yerine geçmekte ve kullanıcı kimliğini içermektedir.
- E-imza bireylerin kimlik bilgilerinden oluşturulmakta olup herkesin e-imzası birbirinden farklıdır.
- Kullanıcı tarafından gönderilen mesajın kesinlikle o kişi tarafından yollandığı, gönderilen mesajın iletim esnasında değiştirilmediği, göndericinin gönderdiği mesajı inkar edememesi e-imza ile sağlanır.

Elektronik İmza



Sertifika Otoritesi

Açık Anahtar

Mesaj Özeti

Elektronik İmza Algoritmaları

- RSA
- Digital Signature Algorithm (DSA)
- Elliptic Curve Digital Signature Algorithm (ECDSA)

RSA ile İmzalama



AYŞE

Açık: $N=187$, $e=7$

Gizli: $p=17$, $q=11$, $d=23$



BARIŞ

Sevgili Barış,
.....
.....
.....
.....
.....
.....
Ayşe

m



Özet:
e10f1ss8fb3

$H(m)$



Elektronik İmza
Ayşe

$H(m)^d \pmod{N} = s$



RSA – İmza doğrulama



AYŞE

Sevgili Barış,
.....
.....
.....
.....
.....

Elektronik İmza
AYŞE Ayşe



BARIŞ

Benimle bir daha
asla.....
.....
.....
.....
.....

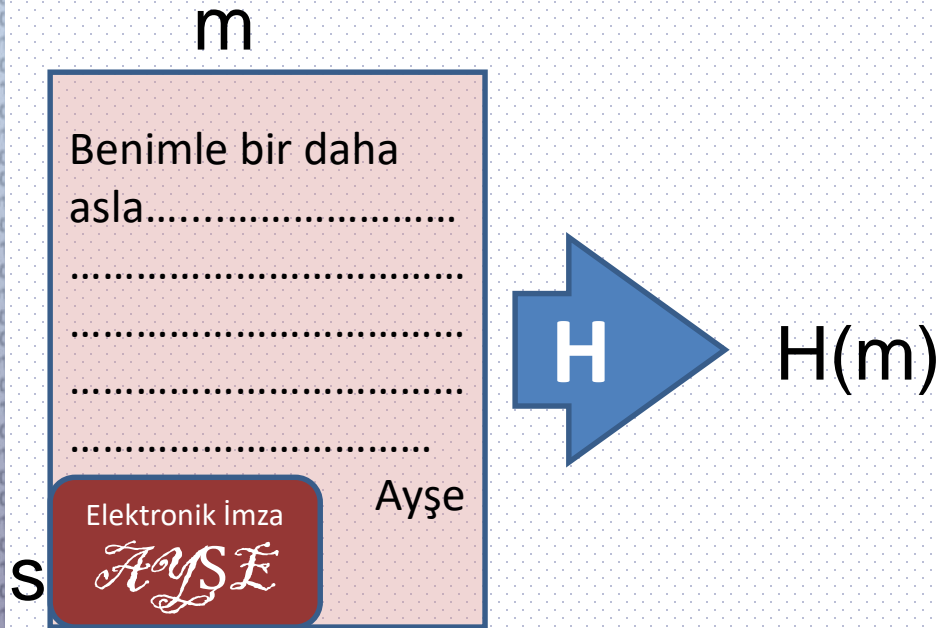
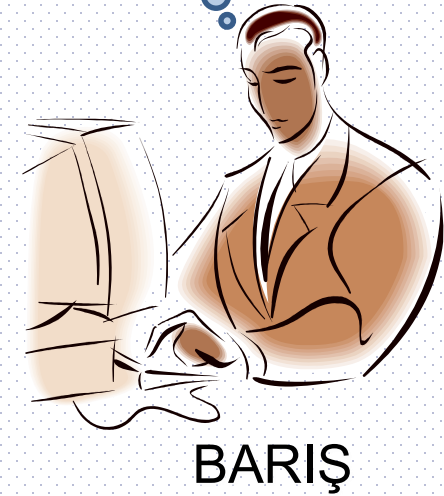
Elektronik İmza
AYŞE Ayşe



Kötü Adam



RSA – İmza Doğrulama



$$s^e \pmod{N} = H'(m) \neq$$

Ayşe'nin Açık Anahtarları: $N=187$, $e=7$

Çarpanlara Ayırma Yöntemleri

- Quadratic Sieve (QS), $O\left(\exp\left(\sqrt{\log n \log \log n}\right)\right)$
- Number Field Sieve (NFS), $O\left(\exp\left(\left(64/9 \log n\right)^{1/3} (\log \log n)^{2/3}\right)\right)$
- Elliptic Curve Factorization $O\left(\exp\left(\sqrt{\log p \log \log p}\right)\right)$

RSA Sayılarının Çözülmesiyle İlgili Tarihsel Veriler

Ondalık Basamak Sayısı	Yaklaşık Bit Sayısı	Başarı Tarihi	MIPS-yılı	Kullanılan Algoritma
100	332	Nisan 1991	7	Karekök Eleme (Quadratic Sieve)
110	365	Nisan 1992	75	Karekök Eleme
120	398	Haziran 1993	830	Karekök Eleme
129	428	Nisan 1994	5000	Karekök Eleme
130	431	Nisan 1996	1000	Genelleştirilmiş Sayı Alanı Elemesi (GNFS)
140	465	Şubat 1999	2000	Genelleştirilmiş Sayı Alanı Elemesi
155	512	Ağustos 1999	8000	Genelleştirilmiş Sayı Alanı Elemesi
160	530	Nisan 2003	—	Örgü Elemesi (Lattice Sieve)
174	576	Aralık 2003	—	Örgü Elemesi
200	663	Mayıs 2005	—	Örgü Elemesi

Notlar:

- **MIPS-yılı**, bir işlemin yaklaşık olarak kaç MIPS (Million Instructions Per Second) gücündeki bir işlemciyle 1 yılda yapılabileceğini belirtir.

Dr. Fatih KALEMKUŞ

Number Field Sieve

- 1024 bitlik RSA sayısı 2.2 GHz AMD 64 işlemcili, 2GB bellekli yaklaşık 12 milyon bilgisayar kullanılarak 1 sene de

$$O(\exp((c+O(1))(\log n)^{1/3}(\log\log n)^{2/3}))$$

Örnek

- RSA-512(=RSA-155)
 - NFS yöntemi ile çarpanlarına ayırmak için yaklaşık $2,6 \times 10^6$ büyüklüğünde bir faktör bulmak gerekmektedir.
 - Ayrıca
 - $6,7 \times 10^6$ tane satır
 - $2,6 \times 10^6$ tane sütun
 - $4,2 \times 10^8$ ağırlıklı dan oluşan matrisini çözmek gerekmektedir.
 - Bu sistemi toplamda yukarıda bahsedilen olanakları ile çözmek Sieving için 73 gün
 - Matris çözümü ve diğer işlemler için yaklaşık 30 gün, toplamda 103 gün sürecektir.

RSA Parametre Güvenlik Değerleri

Güvenlik Seviyesi (=secstr)	RSA(=nlen)
80	1024
128	3072
192	7680
256	15360

DSA (Digital Signature Algorithm)

- Sayısal İmza Algoritması
- 1991, NIST (National Institute of Standards and Technology)
- 1993 FIPS 186 (Federal Information Processing Standard)
- El-Gamal şifreleme sisteminin bir türevidir.
- Ayrık logaritma problemine dayanır.

Ayrık Logaritma Problemi

➤ $Z_p^* = \{1, 2, \dots, p-1\}$

➤ Z_p^* 'de g ve y verilmiş ve $g^x = y \pmod{p}$ ise x kaçtır?

➤ $x = \log_g y$ bulunması zor bir problemdir.

➤ Örnek: Z_{17} 'de $g=3$ ve $y=11$,

$$3^x = 11 \pmod{17} \Rightarrow x = ?$$

Üst alma square and multiply yöntemi ile basittir:

$$3^{129} = 3^{128} \cdot 3^1 = 5 \cdot 3 = 4 \pmod{11}$$

Dr. Fatih KALEMKUŞ

$3^1 \pmod{17} = 3$
$3^2 \pmod{17} = 9$
$3^3 \pmod{17} = 10$
$3^4 \pmod{17} = 13$
$3^5 \pmod{17} = 5$
$3^6 \pmod{17} = 15$
$3^7 \pmod{17} = 11$
$3^8 \pmod{17} = 16$
$3^9 \pmod{17} = 14$
$3^{10} \pmod{17} = 8$
$3^{11} \pmod{17} = 7$
$3^{12} \pmod{17} = 4$
$3^{13} \pmod{17} = 12$
$3^{14} \pmod{17} = 2$
$3^{15} \pmod{17} = 6$
$3^{16} \pmod{17} = 1$
$3^{17} \pmod{17} = 3$

DSA'da Anahtar Oluşturma



- Ayşe $q \mid (p-1)$ olacak şekilde iki asal sayı p ve q 'yu seçer.

Örnek $p=23$ ve $q=11$

- $(Z_p - \{0\})$ 'in q elemanlı alt grubunun üreteci g 'yi hesaplar.

$$g = 2 \quad [2^{11} = 1 \pmod{23}]$$

- $1 < x < (q-1)$ olan x seçer.

$$x = 7 \text{ diyelim. } (1 < x = 7 < 10)$$

- $y = g^x \pmod{p}$ 'yi hesaplar

$$y = 2^7 \pmod{23} = 13$$

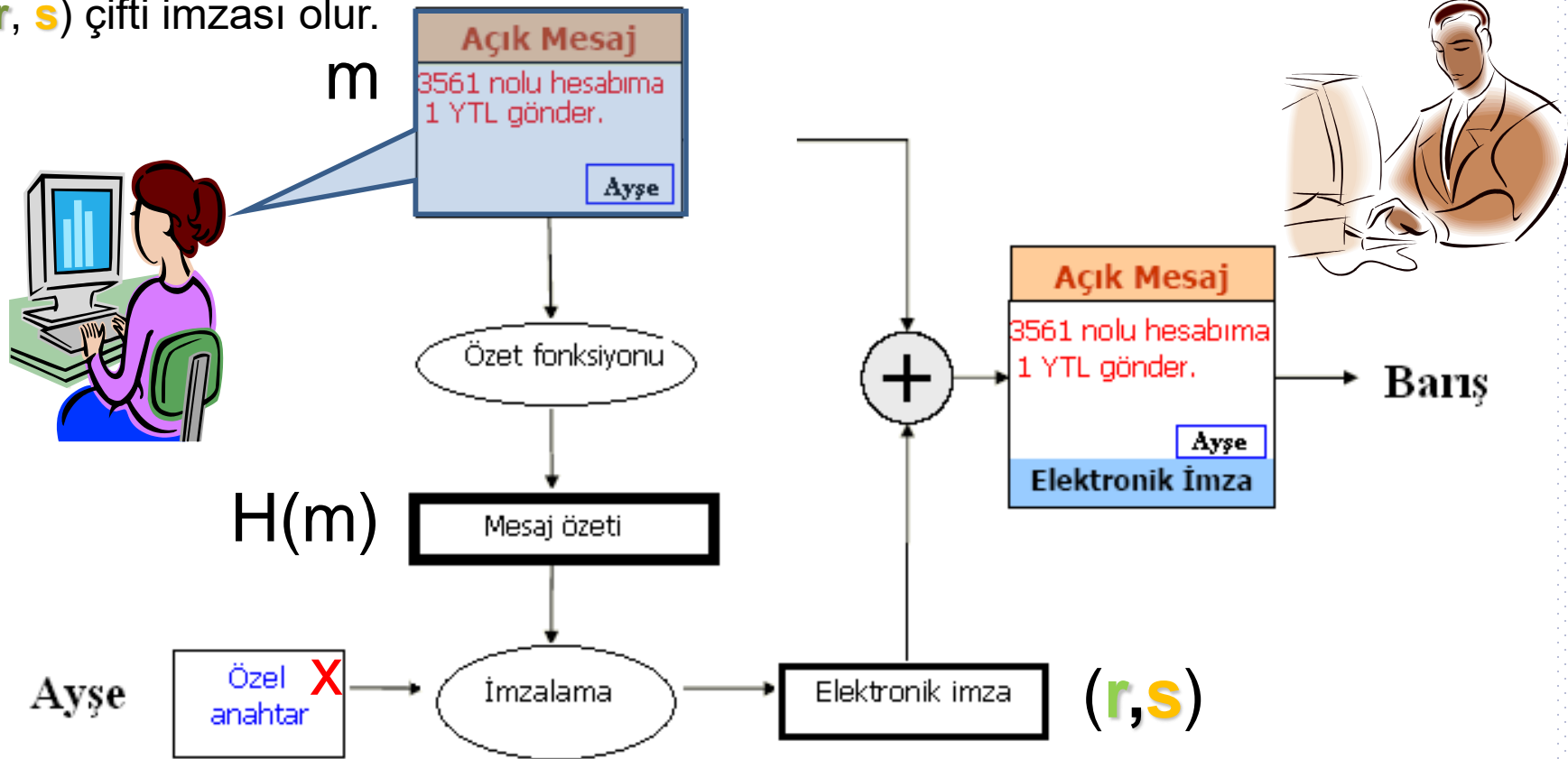
Açık Anahtarlar: $p = 23$ $q = 11$ $g = 2$ $y = 13$

Gizli Anahtar: $x = 7$

DSA - İmzalama

Ayşe,

- $1 < k < q-1$ olan bir k seçer ve $k^{-1} \pmod q$ 'yu bulur.
- $r = (g^k \pmod p) \pmod q$ hesaplar.
- $s = k^{-1} (H(m) + xr) \pmod q$ 'yu elde eder.
- (r, s) çifti imzası olur.



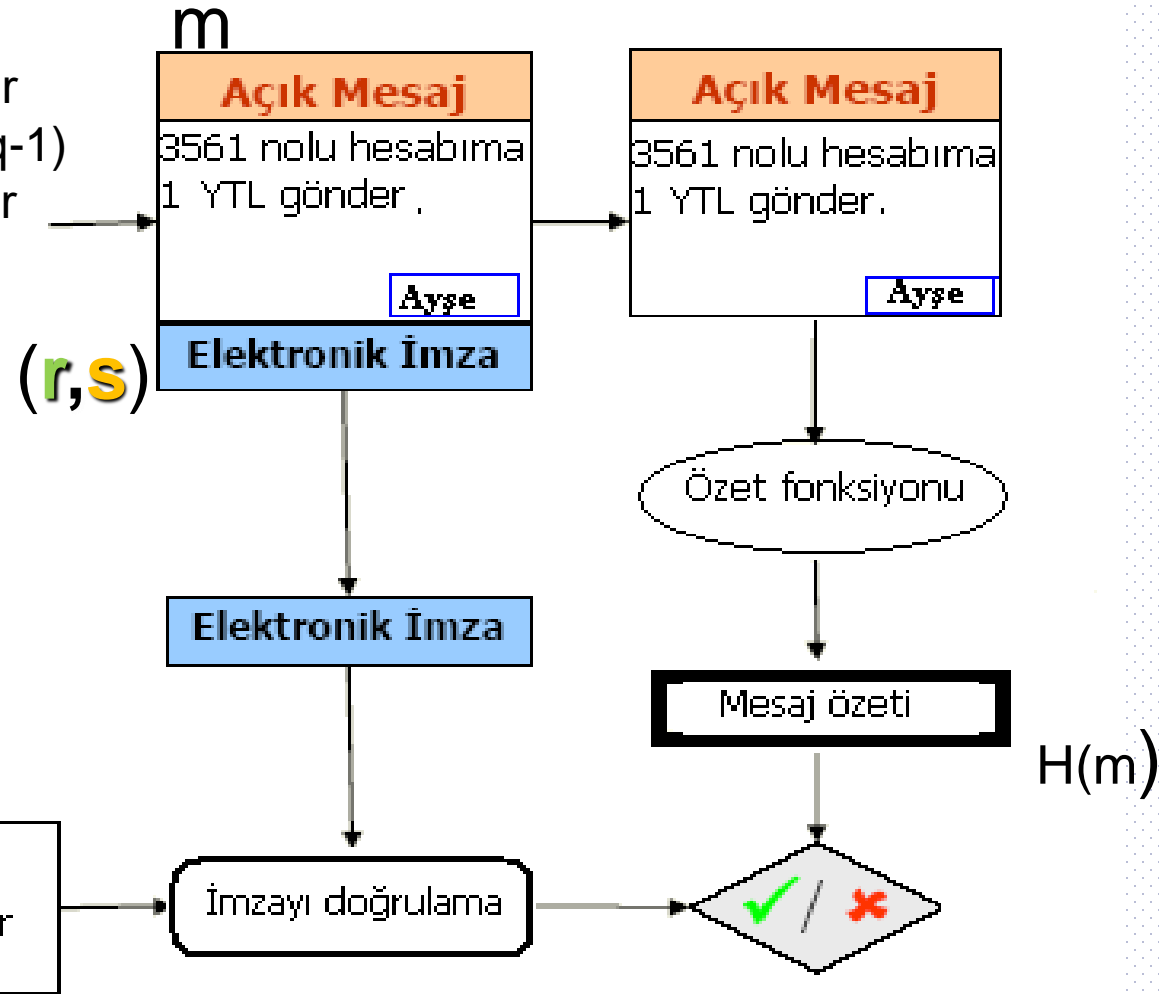
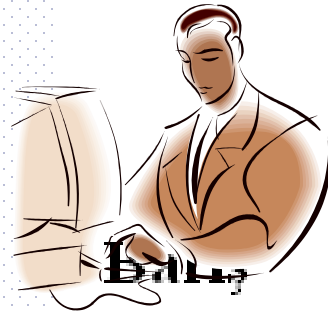
Açık: p, q, g, y Gizli: x

Dr. Fatih KALEMKUŞ

DSA - İmza doğrulama

Bariş,

- Ayşe'nin açık anahtarlarını alır
 - r ve s 'yi kontrol eder. ($1 < r, s < q-1$)
 - $H(m)$ ve $w = s^{-1} \text{ mod } q$ 'yu bulur
 - $u_1 = H(m) * w \text{ mod } q$
 - $u_2 = r * w \text{ mod } q$
- Son olarak;
- $v = (g^{u_1} y^{u_2} \text{ mod } p) \text{ mod } q$
 - $r = v$ ise imza doğrulanır.





DSA Parametre Değerleri

p	q
1024	160
2048	224
2048	256
3072	256

Dr. Fatih KALEMKUŞ

ECDSA (Elliptic Curve DSA)

- 1985 – Victor Miller ve Neal Koblitz
- Eliptik eğrilerdeki ayrık logaritma problemine dayanır.
- DSA'da kullanılan çarpımsal $(\mathbb{Z}_p/\{0\}, *)$ grubunun yerine toplamsal eliptik eğri grubu $(E(\mathbb{F}_p), +)$ kullanılır.

Eliptik Eğri Kriptografi

- Eliptik Eğri Kriptografi (Elliptic Curve Cryptography (ECC)) tabanlı şifreleme algoritmaları, RSA yerine tercih edilmeye başlandı.
- [Dr. Scott Vanstone](#) (Matematik ve Bilgisayar Bilimleri Profesörü ve Certicom şirketi kurucularından), ECC için açık anahtarlı kriptografinin gelecek nesli (özellikle kablosuz iletişim) olarak bahsediyor. Certicom firmasının ECC üzerine algoritmalar konusunda birçok patenti mevcuttur.

Kaynak:

http://www.compseconline.com/hottopics/hottopic20_8/Next.pdf

Eliptik Eğri Kriptografi

-Kullanım Yararları-

Eliptik Eğri tabanlı şifreleme algoritmaları, DSA ve RSA parametrelerine nazaran daha küçük parametreler kullanırlar ve eşdeğer güvenlik seviyesini sağlarlar (Bakınız: “On the Security of 1024-bit RSA and 160-bit Elliptic Curve Cryptography”).

- İşlemci Gücü
- Veri depolama alanı
- Band genişliği
- Güç Tüketimi

sınırlı ise Eliptik Eğri Kriptografi kullanımın faydası olacaktır.

Eliptik Eğri Kriptografi, sınırlı çevre birimlerine sahip akıllı kart, mobil cihazlar, el bilgisayarları ve diğer benzeri sistemler için tercih edilebilir.

Eliptik Eğri Kriptografi

- **Standartlar:** ANS X9F1 | CRYPTREC | IEEE P1363 | NESSIE | NSA Suite
- Netscape Security Services (NSS), yazılım kütüphanesi kümesi olup, birçok platform bağımsız işlemci-server uygulamalarını desteklemektedir.
- NSS içinde desteği bulunanlar: SSL v2 and v3, TLS, PKCS #5, PKCS #7, PKCS #11, PKCS #12, S/MIME, X.509 v3 sertifikaları ve diğer güvenlik ile ilgili standartlar.

Eliptik Eğri Kriptografi

- Open SSL and NSS (sürüm 3.8) Eliptik Eğri Kriptografi algoritmalarını desteklemektedir.
- Mozilla web tarayıcı Eliptik Eğri Kriptografi algoritmalarını SSL sayesinde desteklemektedir.
- E-posta imzalama/doğrulama için ECDSA kullanılabilir (Digital Signature Algorithm (DSA), **Eliptik Eğri Kriptografi** sürümü)

Eliptik Eğriler

- $p > 3$ bir asal sayı olmak üzere
- F_p 'de bir eliptik eğri $E(F_p)$ şöyle tanımlanır:



$a, b \in F_p = \{0, 1, 2, \dots, p-1\}$ ve $4a^3 + 27b^2 \neq 0 \pmod{p}$

$$y^2 = x^3 + ax + b$$

$x, y \in F_p = \{0, 1, 2, \dots, p-1\}$ olan tüm (x, y) çözümleri ve $\infty = (0, 1, 0)$

Eliptik Eğriler - Örnek

- F_{23} 'te tanımlı $y^2=x^3+x+1$ bir eliptik eğridir $E(F_{23})$
($4+27=8 \pmod{23}$)

$E(F_{23})$ 'e ait (x,y) noktaları:

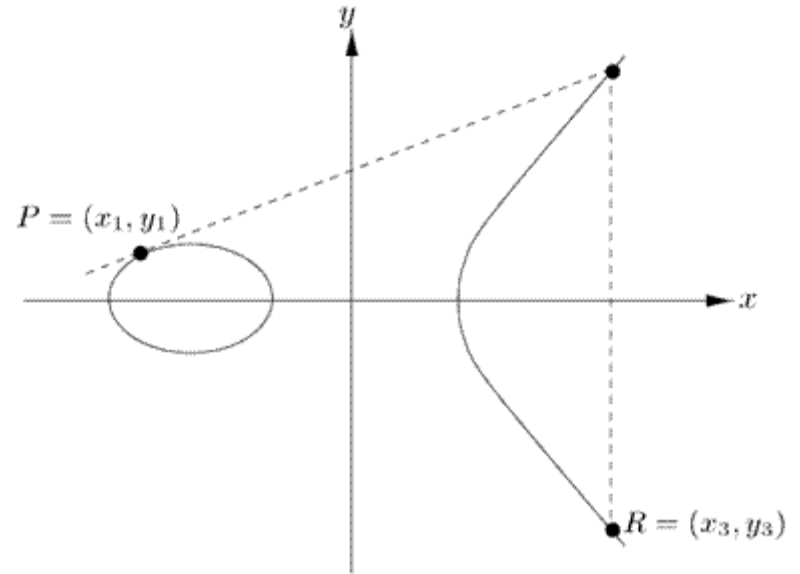
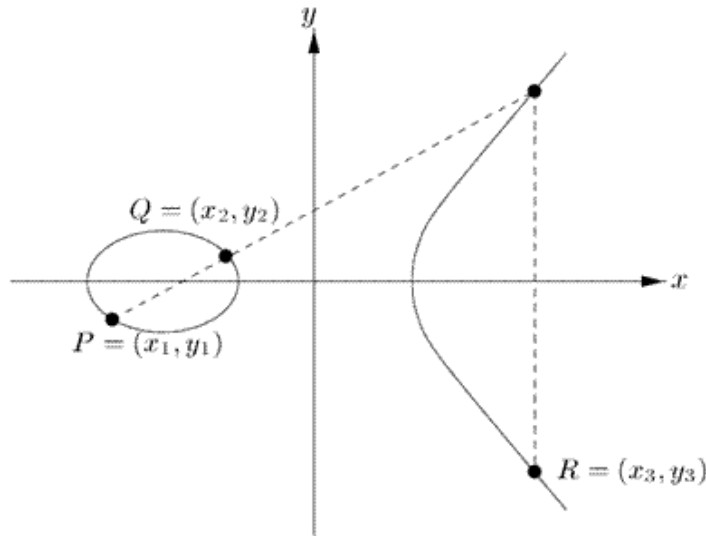
(0, 1)	(0, 22)	(1, 7)	(1, 16)	(3, 10)	(3, 13)	(4, 0)	(5, 4)	(5, 19)
(6, 4)	(6, 19)	(7, 11)	(7, 12)	(9, 7)	(9, 16)	(11, 3)	(11, 20)	(12, 4)
(12, 19)	(13, 7)	(13, 16)	(17, 3)	(17, 20)	(18, 3)	(18, 20)	(19, 5)	(19, 18)

Eliptik Eğriler

- $E(\mathbb{F}_p)$ 'ye ait tüm bu noktalar toplamsal grup oluşturur.
- Bu grubun aritmetiğinde iki temel işlem tanımlanır:

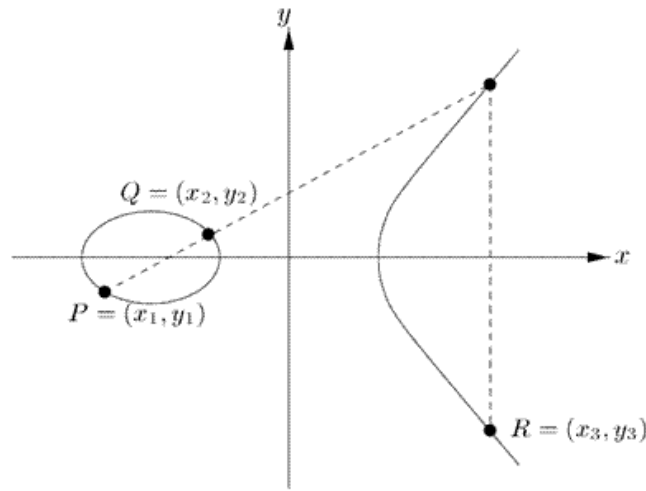
Toplama : $P \neq Q \Rightarrow P + Q = R$

İki kat alma : $2P = R$

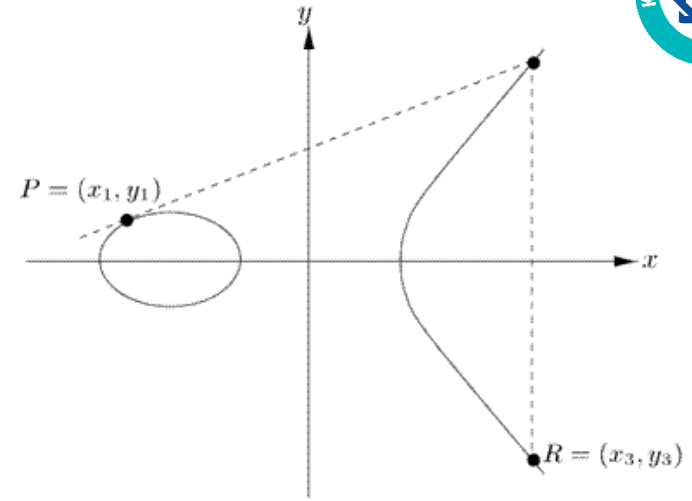


Dr. Fatih KALEMKUŞ

Toplama



İki kat alma



$$P + Q = R$$

$$P + P = R$$

$$x_1 \neq x_2$$

$$y_1 = 0 \rightarrow P = -P \rightarrow 2P = 0$$

$$P + Q = (x_3, y_3)$$

$$2P = (x_3, y_3)$$

$$x_3 = (\lambda^2 - x_1 - x_2) \bmod p$$

$$x_3 = (\lambda^2 - 2x_1) \bmod p$$

$$y_3 = (\lambda(x_1 - x_3) - y_1) \bmod p$$

$$y_3 = (\lambda(x_1 - x_3) - y_1) \bmod p$$

$$\lambda = \left(\frac{y_2 - y_1}{x_2 - x_1} \right) \bmod p$$

$$\lambda = \left(\frac{3x_1^2 + a}{2y_1} \right) \bmod p$$

Eliptik Eğriler – Örnek Toplama

$$E(\mathbb{F}_{23}) \quad y^2 = x^3 + x + 1$$

$P = (3, 10)$ ve $Q = (9, 7)$ olsun. $P + Q = (x_3, y_3)$:

$$\frac{7031}{9862}$$

$2 \cdot 12 \equiv 1 \pmod{23}$ olduğundan $2^{-1} = 12$ 'dir. Son olarak;

$$x_3 = 11^2 - 3 - 9 = 6 - 3 - 9 = -6 \equiv 17 \pmod{23} \quad \text{ve}$$

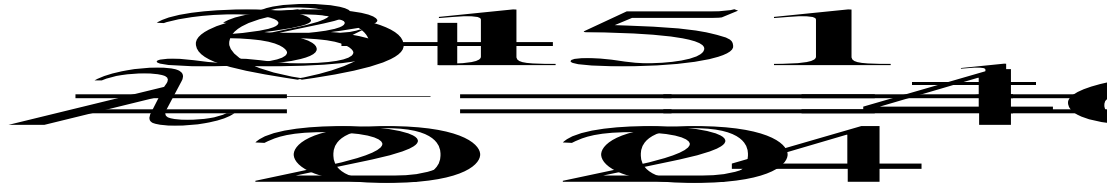
$$y_3 = 11(3 - (-6)) - 10 = 11(9) - 10 = 89 \equiv 20 \pmod{23}.$$

Bundan dolayı $P + Q = (17, 20)$.

Eliptik Eğriler – Örnek İki kat alma

$$E(\mathbb{F}_{23}) \quad y^2 = x^3 + x + 1$$

$P = (3, 10)$ olsun. $2P = P + P = (x_3, y_3)$:



$4 \cdot 6 \equiv 1 \pmod{23}$ olduğundan $4^{-1} = 6$ 'dır. Son olarak,

$$x_3 = 6^2 - 6 = 30 \equiv 7 \pmod{23} \text{ ve}$$

$$y_3 = 6(3 - 7) - 10 = -24 - 10 = -34 \equiv 12 \pmod{23}.$$

Buradan $2P = (7, 12)$.

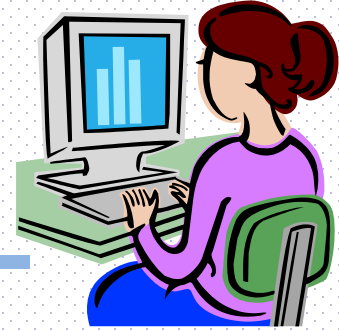
Eliptik Eğrilerde Ayırık Logaritma Problemi

- Eliptik eğri üzerindeki Ayırık Logaritma Problemi, eğri üzerindeki bir P noktasının k ile çarpımına denk olan $kP=Q$ noktası verildiği zaman n sayısının k bulunmasıdır.
- Çarpma işlemi toplama ve iki katı alma işlemleri kullanılarak uygulanır.

Eliptik Eğrilerde Ayrik Logaritma Problemi

$$\mathbf{E}(F_{23}) \quad y^2 = x^3 + 9x + 17$$

$P = (16, 5)$ ve $k \in F_{23}$ için $Q = k \cdot P = (4, 5)$ olsun. \Rightarrow **k** = ?



ECDSA'da Anahtar Oluşturma

- Ayşe F_p de tanımlı bir eliptik eğri E 'yi seçer.
- $E(F_p)$ 'nin n elemanlı alt grubunun üretici olan P bulur.
- $1 < d < (n-1)$ olan d seçer.
- $Q = dP$ 'yi hesaplar

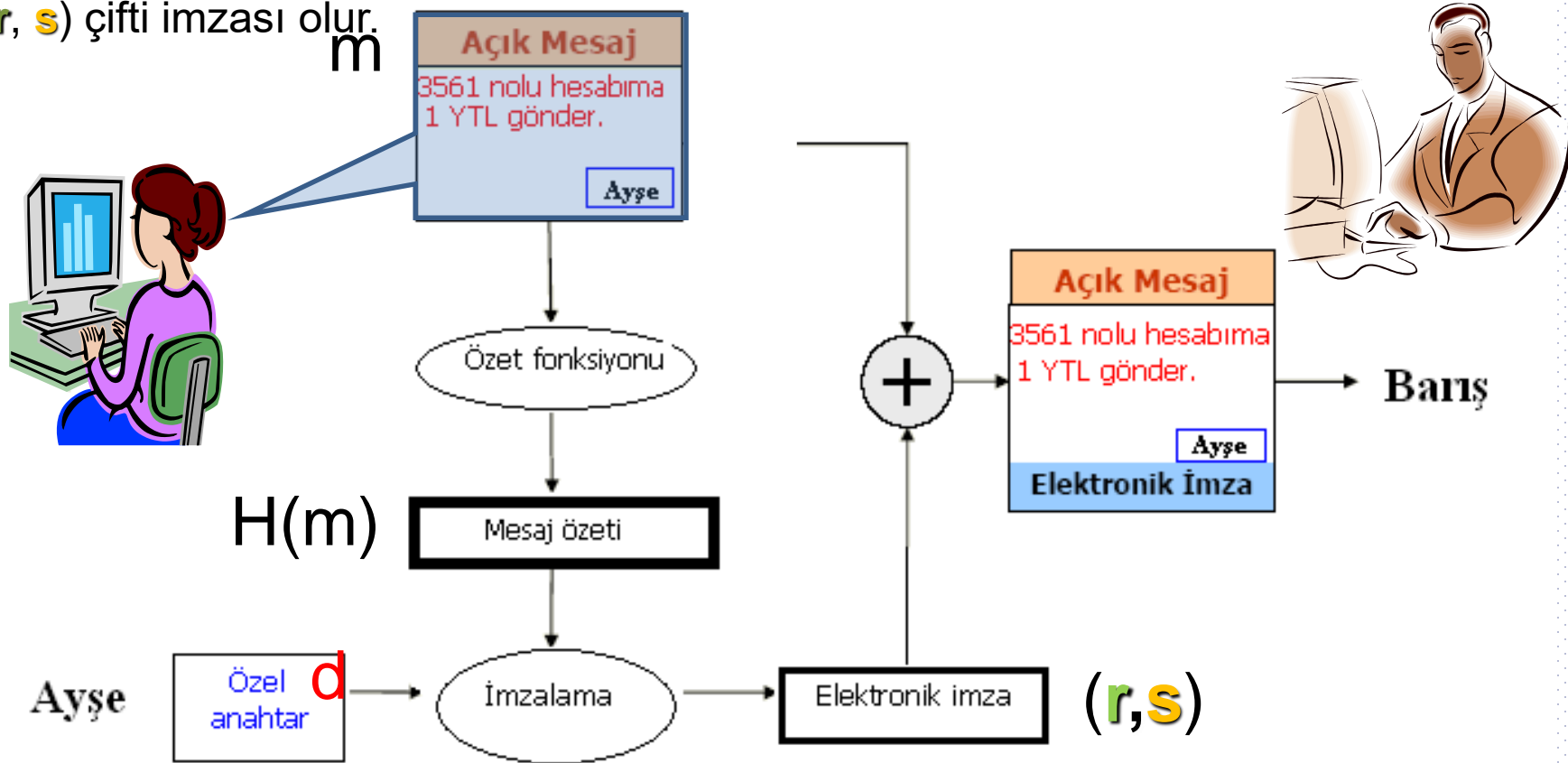
Açık Anahtarlar: E , P , n , Q

Gizli Anahtar: d

ECDSA - İmzalama

Ayşe,

- $1 < k < n-1$ olan bir k seçer ve $k^{-1} \bmod n$ 'i bulur.
- $kP = (x_1, x_2)$ ve $r = x_1 \bmod n$ hesaplar.
- $s = k^{-1} (H(m) + dr) \bmod n$ 'i elde eder.
- (r, s) çifti imzası olur.



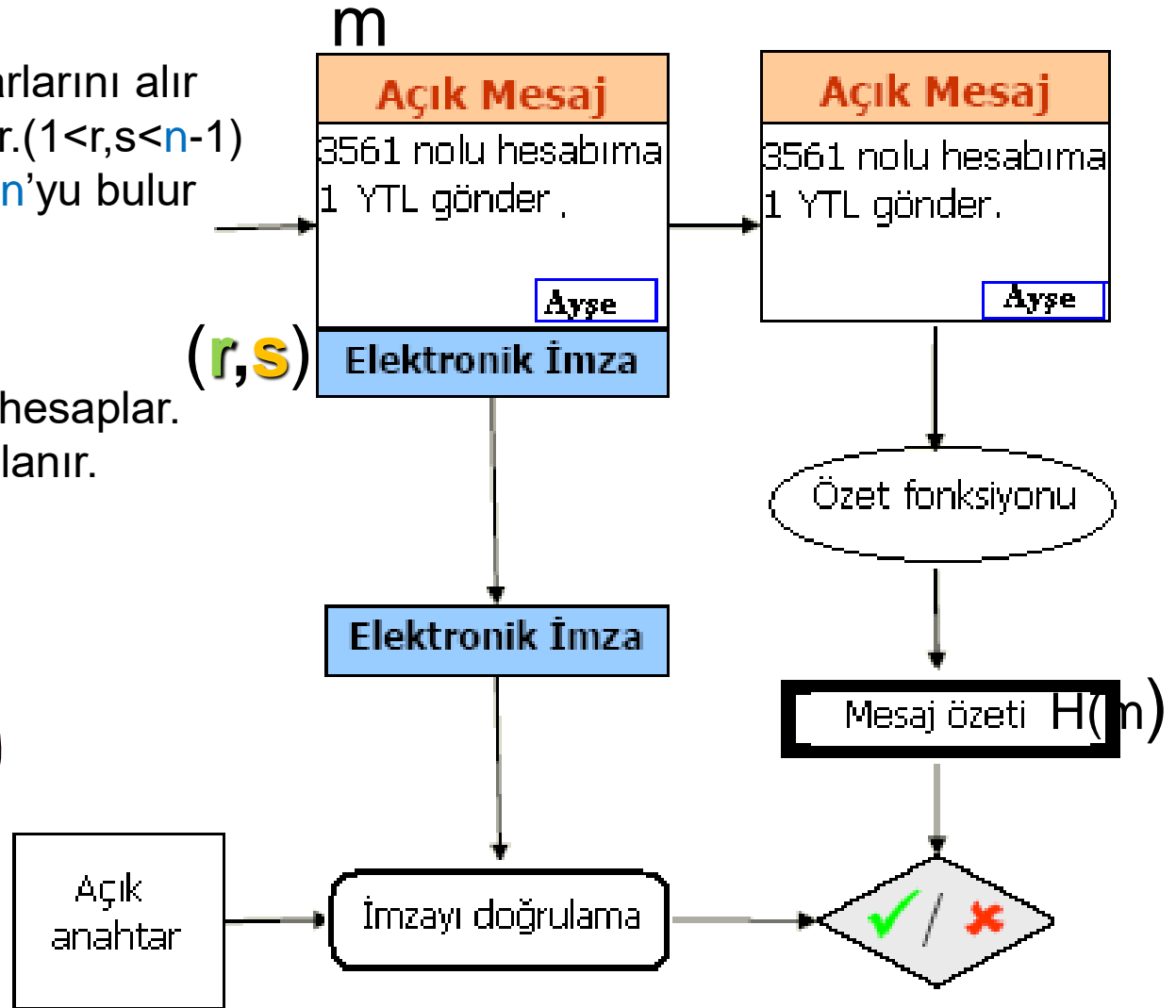
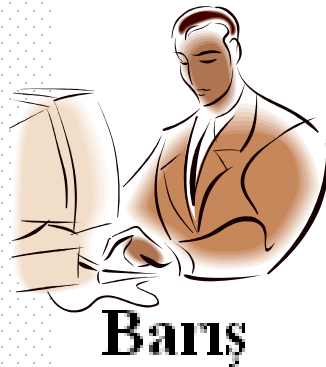
Açık: E, P, n, Q Gizli: d

Dr. Fatih KALEMKÜŞ

ECDSA - İmza doğrulama

Barış,

- Ayşe'nin açık anahtarlarını alır
- r ve s 'yi kontrol eder. ($1 < r, s < n-1$)
- $H(m)$ ve $w = s^{-1} \text{ mod } n$ 'yu bulur
- $u_1 = H(m) * w \text{ mod } n$
- $u_2 = r * w \text{ mod } n$
- Son olarak;
- $v = u_1 P + u_2 Q \text{ mod } n$ 'i hesaplar.
- $r = v$ ise imza doğrulanır.



DSA - ECDSA

Grup	F_p^*	$E(F_p)$
Grup elemanları	Tam sayılar $\{1,2,\dots,p-1\}$	Eğrideki noktalar ve ∞
Grup İşlemi	Mod p 'de çarpma	Noktaları toplama ve iki kat alma
Gösterimler	Elemanlar: g, h Çarpma: $g \cdot h$ Bir elemanın tersi: g^{-1} Bölme: g/h Üs alma: g^x	Elemanlar: P, Q Toplama: $P + Q$ Bir elemanın tersi: $-P$ Çıkarma: $P+(-Q)$ Kat alma: kP
Ayrık Logaritma Problemi	$g \in Z_p$ ve $h = g^x \text{ mod } p$ ise x kaçtır?	$P \in E(F_p)$ ve $Q = kP$ ise k kaçtır?

Asimetrik Sistemlerin Karşılaştırılması

	Şifreleme	İmzalama	Anahtar Paylaşımı
RSA	Evet	Evet	Evet
Diffie-Hellman	Hayır	Hayır	Evet
DSA	Hayır	Evet	Hayır
Eliptik Eğriler	Evet	Evet	Evet

Açık Anahtarlı Şifreleme ile Simetrik Şifreleme Anahtarı Paylaşımı

- Simetrik Şifreleme için, gizli anahtar (secret key) mutlaka haberleşecek iki kişi arasında güvenli bir şekilde paylaşılmalıdır (örneğin Ayşe and Bülent arasında).
- Bir yaklaşım “Diffie-Hellman anahtar değişimi algoritmasını” kullanmak. Yaygın kullanılıyor fakat basit halinde kullanımı kimlik doğrulama olmadığı için kullanılmalıdır.
- Diğer bir güçlü yaklaşım açık anahtar sertifikaları (alıcının açık anahtarı edinmenin yolu) kullanmaktır:
 - Bülent, Ayşe ile güvenli haberleşmede bulunmak ister. Bunun için Bülent izleyen yolları takip eder:
 - 1) Mesaj M yi hazırlar
 - 2) Bu mesajı belirlediği gizli anahtar K (belki bir kere kullanmak üzere) ile simetrik bir şifreleme sistemi ile şifreler (AES-192 gibi): $E_K(M)=C$ 3)
 - Ek olarak gizli anahtar K yı, Ayşe'nin açık anahtarı PU_a ile bir açık anahtar şifreleme algoritması ile şifreler: $E_{PU_a}(K)=K'$
 - 4) Bülent K' ve C yi Ayşe'ye gönderir.
 - Ayşe $D_{PRa}[K']=D_{PRa}[E_{PU_a}(K)]=K$ elde eder ve ayrıca M yi

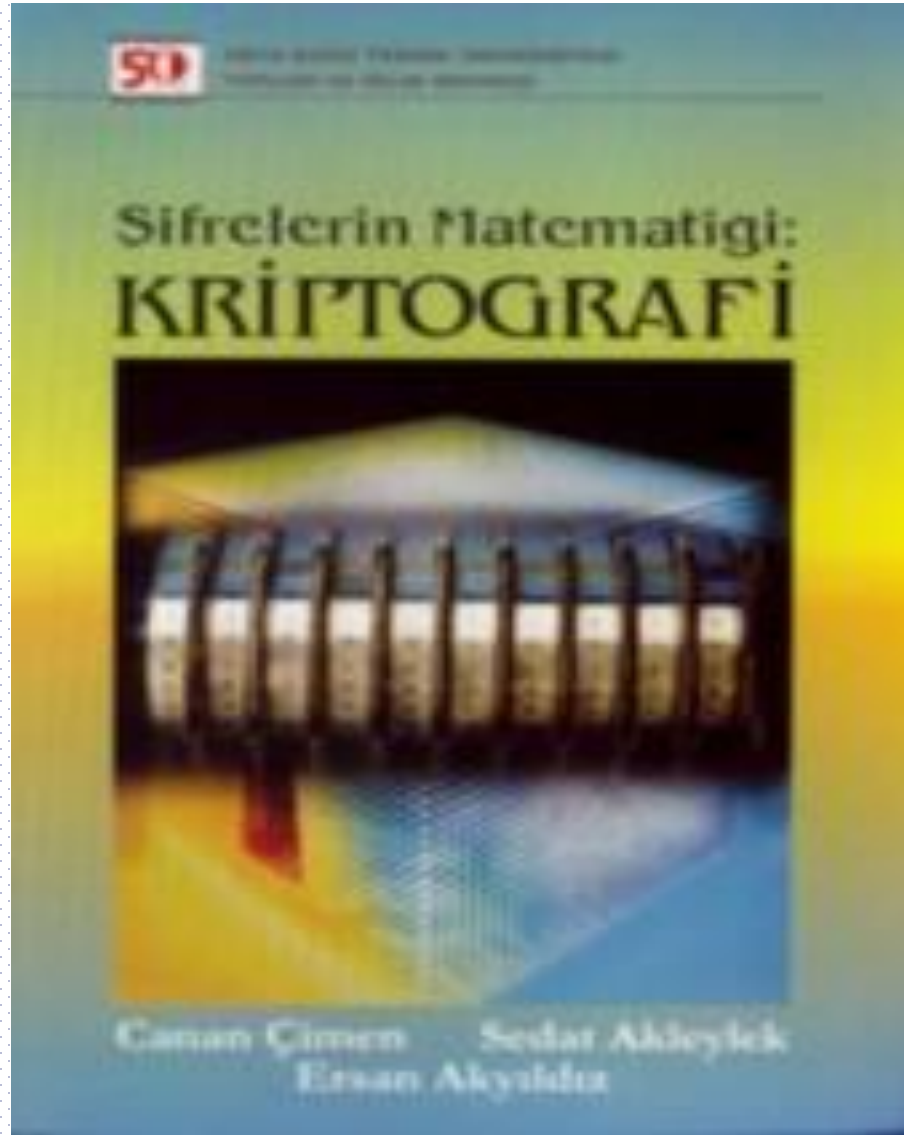
7.05.2025 hesaplar: $D_K(C)=M$

Kriptografi Standartları



- ETSI TS 102 176-1 V2.0.0 Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms
- IEEE P1363 (2000): "Standard Specifications for Public-Key Cryptography".
- ANSI X9.62, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), 2005.
- FIPS PUB 140-1-2-3, Security Requirements for Cryptographic Modules (prepared by National Institute of Standards and Technology: NIST, US federal agency)
- IETF RFC 3647: Internet X.509 PKI Certification Plan (prepared by the Internet Society)
- PKCS #1: RSA Cryptography Standard
- PKCS #3: Diffie-Hellman Key Agreement Standard
- PKCS #5: Password-Based Cryptography Standard
- PKCS #7: Cryptographic Message Syntax Standard
- PKCS #10: Certification Request Syntax Standard
- PKCS #11: Cryptographic Token Interface Standard
- PKCS #12: Personal Information Exchange Syntax Standard
- PKCS #13: Elliptic Curve Cryptography Standard

Dr. Fatih KALEMKUŞ



Dr. Fatih KALEMKUŞ

Sorular



Dr. Fatik KALEMKUŞ



TEŞEKKÜRLER

Dr. Fatih KALEMKUŞ