

ELEKTRONİK İMZA KANUNU ve ELEKTRONİK İMZA TEKNOLOJİLERİ

Dr. Tolga TÜFEKÇİ

TÜBİTAK

Bilgi Teknolojileri ve Elektronik Araştırma Enstitüsü





İçerik

- Neden elektronik imza?
- (Güvenli) elektronik imza nedir?
- Elektronik (sayısal) imza
 - Kriptografi
 - Elektronik (sayısal) imza tekniği
 - Teknik açıdan güvenlik
- İdari açıdan güvenlik
 - Elektronik sertifika hizmet sağlayıcıları
 - Nitelikli elektronik sertifika
 - Genel işleyiş
- Demo



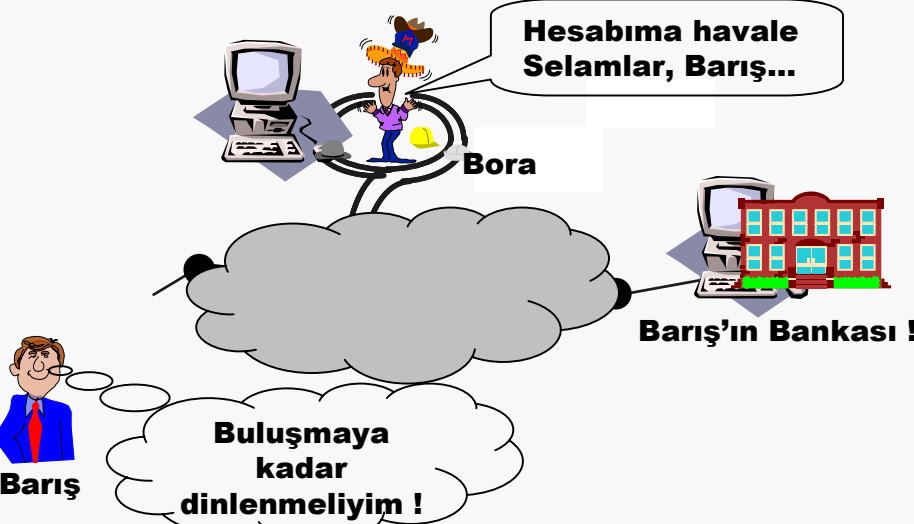
Mesajınız dinlenebilir (Gizlilik)



Mesajınız değiştirilebilir (Bütünlük)



Kimliğiniz taklit edilebilir (Kimlik ispatı)



Yapan inkar edebilir (İnkâr edilememezlik)



Şifreleme

Elektronik İmza



Elektronik imza nedir ?

Madde 3.b

Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri

- Kullanıcı adı ve şifre?
- Tarayıcıdan geçirilmiş imza resmi?
- Ne kadar güvenli?






Güvenli elektronik imza?

- Mantıksal bağlantı nerede?
 - Veri tahrifatının tespiti: Sayısal imza ?!

Madde 4

- a) *Münhasıran imza sahibine bağlı olan*
 - b) *Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan*
 - c) *Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan*
 - d) *İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapıp yapılmadığının tespitini sağlayan*
- 



Şifreleme

- Sezar şifresi
 - $\text{Harf} = \text{harf} + 3$
 - $\text{ALİ} \rightarrow \text{DOL}$
- Simgeleme
 - $A \rightarrow B, B \rightarrow C, \dots Y \rightarrow Z, Z \rightarrow A$
 - $\text{ALİ} \rightarrow \text{BMJ}$
- Geliştirilmiş Sezar
 - $\text{Harf} = a * (\text{harf}) + b \bmod 29$, a ve b anahtarlar
 - a=1 ve b=3 iken sezar şifresi örneği



Kriptografi

Tek anahtarlı algoritmalar ile şifreleme



0984842...55



**Tek anahtarlı
algoritma**

Çıktı

khU/)+



Merhaba



0984842...55



**Tek anahtarlı
algoritma**

Girdi

khU/)+



Merhaba

DES, 3DES, AES





Anahtar çifti

Madde 3.d

Elektronik imza oluşturma verisi, imza sahibine ait olan, imza sahibi tarafından elektronik imza oluşturma amacıyla kullanılan ve bir eşi daha olmayan şifreler, kriptografik gizli anahtarlar gibi verilerdir

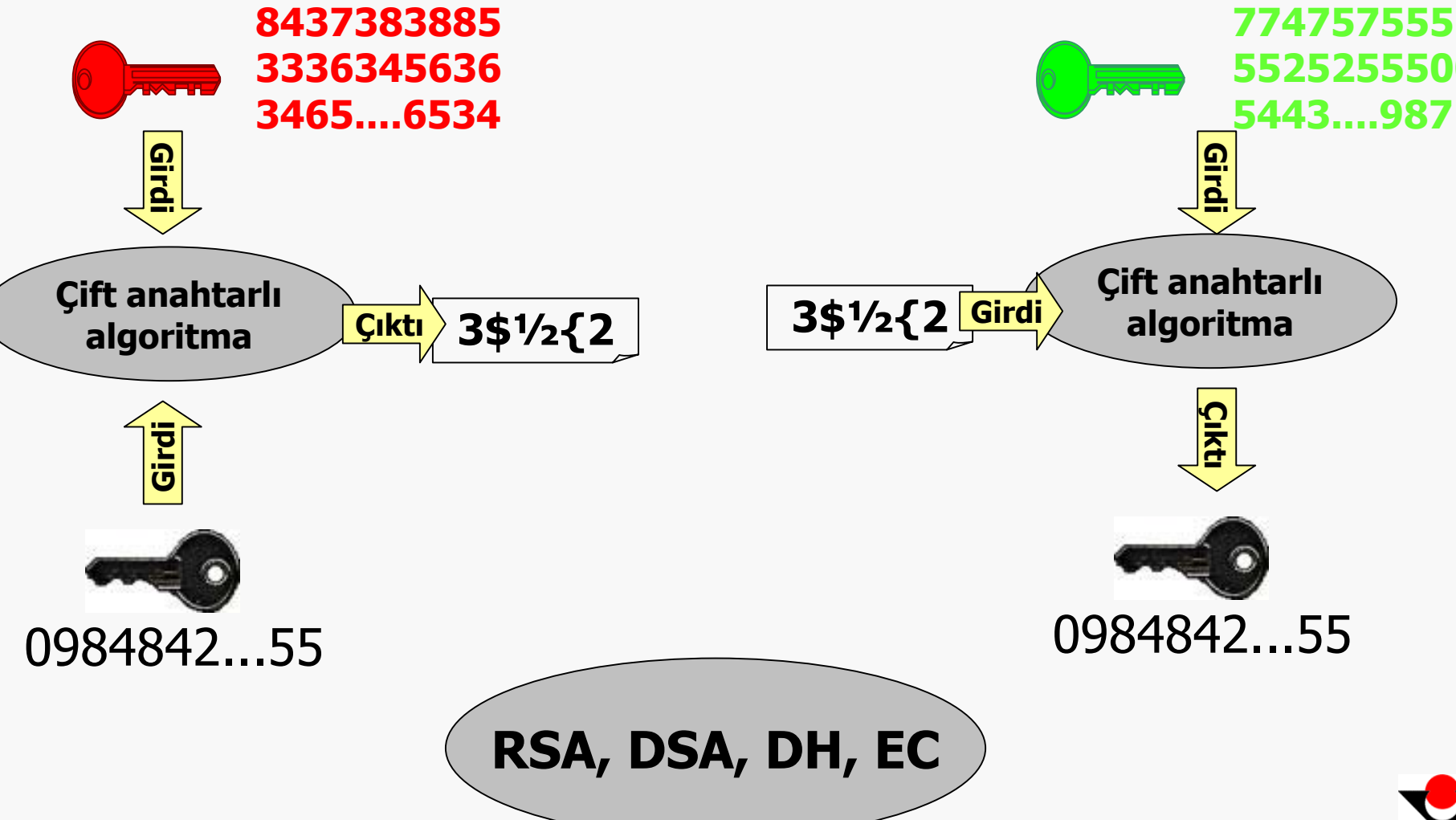
Madde 3.f

Elektronik imzayı doğrulamak için kullanılan şifreler, kriptografik açık anahtarlar gibi verilerden oluşan imza doğrulama verisidir



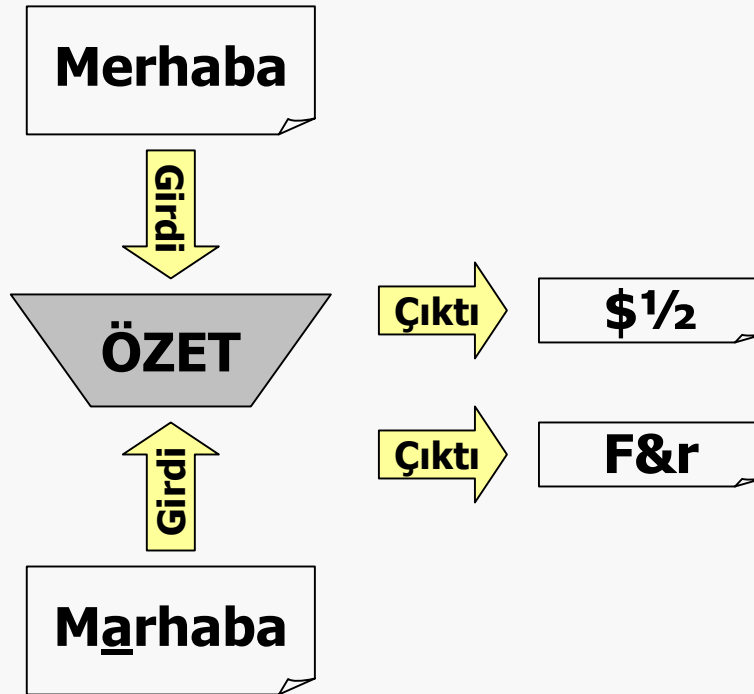
Kriptografi

Çift anahtarlı algoritmalar ile şifreleme



Kriptografi

Özet (hash) algoritmaları



■ Özet algoritmaları

- Mesajı her zaman ve aynı uzunlukta bir özete indirger
- Özetten yola çıkarak mesaj yeniden elde edilemez
- İki farklı mesajın özeti aynı olmaz

SHA-1, MD4, MD5



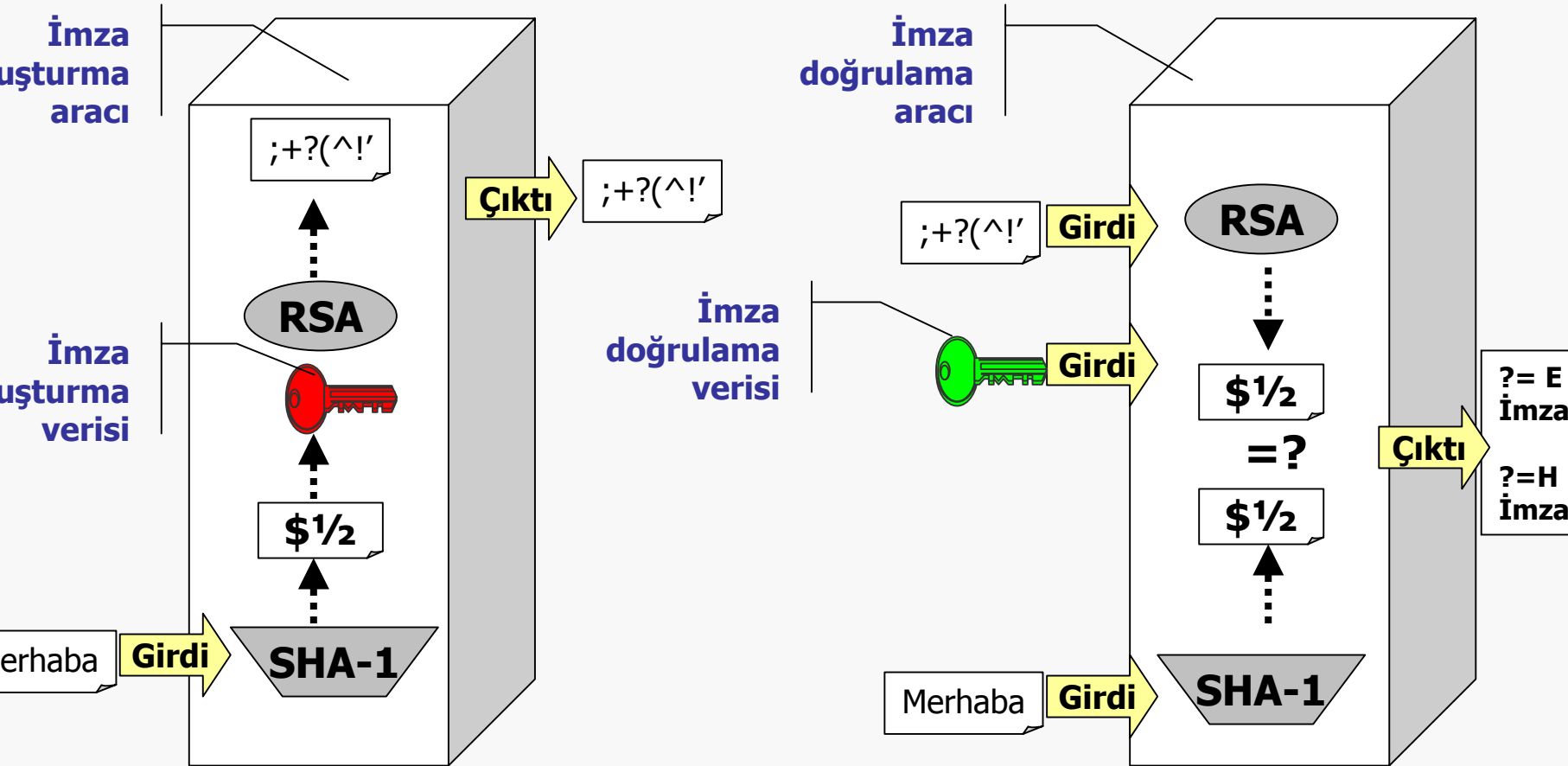


RSA

- p ve q rasgele iki büyük asal sayı (512 bit uzunluğunda)
 - $n = p \cdot q$ (1024 bit)
 - $e = 65,537$;
 $e \cdot d \equiv 1 \pmod{(p-1) \cdot (q-1)}$
 - İmza oluşturma verisi = d
İmza doğrulama verisi = (n,e)
- M = şifrelenecek metin
 - $S = M^d \pmod{n}$
 - $M = S^e \pmod{n}$
- $p = 5$; $q = 7$
 - $n = 35$
 - $e = 5$;
 $5 \cdot 5 \equiv 1 \pmod{24}$
 - İmza oluşturma verisi = 5
İmza doğrulama verisi = (35,5)
- $M = 4$
 - $9 = 4^5 \pmod{35}$
 - $4 = 9^5 \pmod{n}$

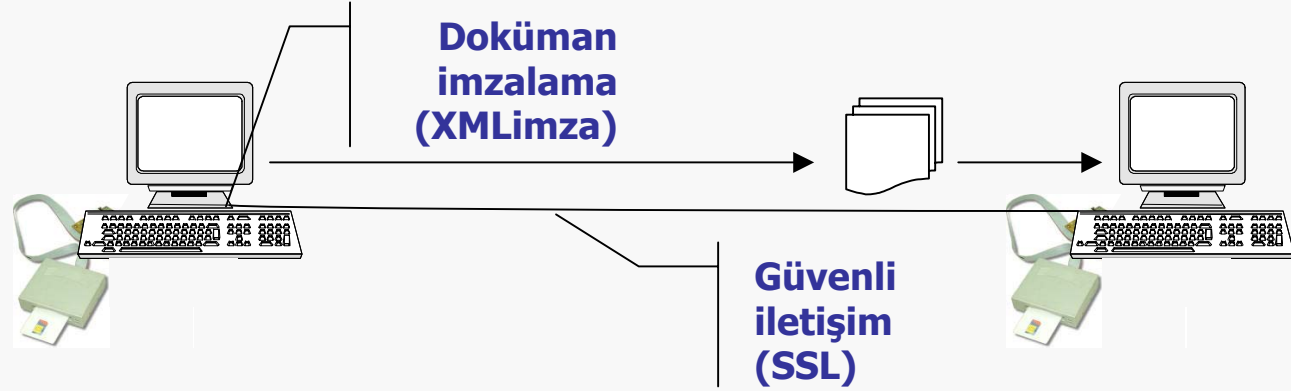


Elektronik imza tekniđi



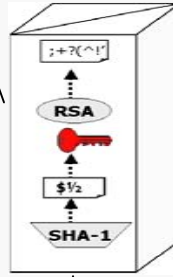
Teknik açıdan güvenlik

Uygulamalar Protokoller Ürünler

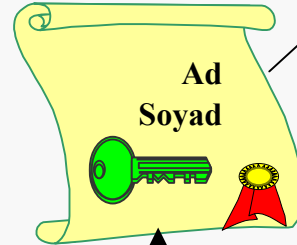


Ürünler Standartlar Yöntemler

PKCS.5
PKCS.7
PKCS.11
PKCS.12
ISO 7816



X.509



Yöntemler

RSA

SHA-1

Asallık testi

Rasgele sayı üretimi

Yöntemin güvenliği





Güvenli imza oluşturma aracı

Madde 6

- a) Ürettiği elektronik imza oluşturma verilerinin kendi aralarında bir eşi daha bulunmamasını,
- b) Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin araç dışına hiç bir biçimde çıkarılamamasını ve gizliliğini
- c) Ürettiği elektronik imza oluşturma verilerinin, üçüncü kişilerce elde edilememesini, kullanılamamasını ve elektronik imzanın sahteciliğe karşı korunmasını,
- d) İmzalanacak verinin imza sahibi dışında değiştirilememesini ve bu verinin imza sahibi tarafından imzanın oluşturulmasından önce görülebilmesini



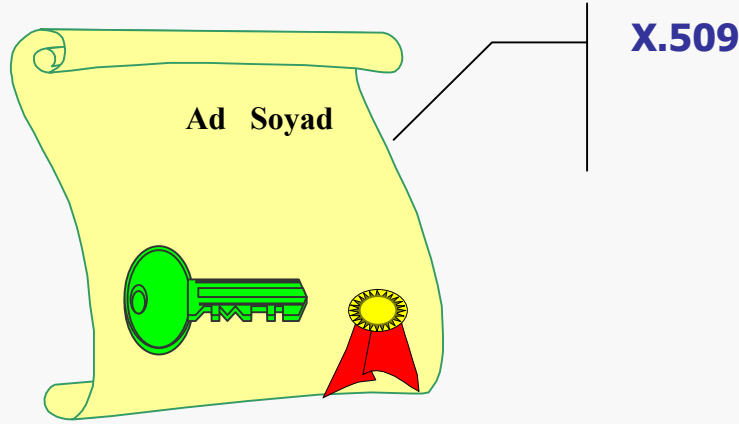


İdari açıdan güvenlik

- Hangi anahtar çiftinin kime ait olduğunun bilinmesi
 - Anahtar çifti üretimi
 - Doğru kimlik tespiti
- Güvenilir bir kurum tarafından anahtar çiftinin (doğrulama verisinin) kime ait olduğunun beyanı
 - Elektronik sertifika



Elektronik Sertifika



Madde 3.1

İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kaydı





Elektronik Sertifika Hizmet Sağlayıcısı

Madde 8

Elektronik sertifika hizmet sağlayıcısı, sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan gerçek veya tüzel kişilerdir

■ İlgili hizmetler

- Nitelikli elektronik sertifika başvuru, iptal, yenileme süreçlerinin yönetimi
- Sertifika durum bilgisi hizmetleri
- Kayıtların tutulması
- Zaman damgası hizmetleri



Nitelikli elektronik sertifika

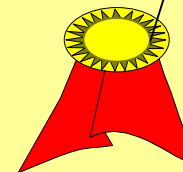
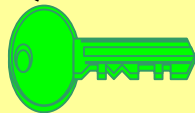
Nitelikli elektronik sertifika

- Sertifikanın seri numarası
- Sertifika hizmet sağlayıcısının kimlik bilgileri ve kurulduğu ülke
- Sertifikanın nitelikli olduğuna dair bir ibare
- Sertifika sahibinin teşhis edilebileceği kimlik bilgileri
- Diğer bir kişi adına hareket ediyorsa yetkisi
- Talep üzerine mesleki ve diğer kişisel bilgiler
- Varsa sertifikanın kullanım şartları
- Sertifikanın geçerlilik süresi

Madde 9

**Sertifika
hizmet
sağlayıcısının
elektronik
imzası**

**İmza
doğrulama
verisi**



Genel İşleyiş

YASAL ALTYAPI

MAHKEMELER



- Yasalar
- Yönetmelikler

DÜZENLEYİCİ KURUM



BİREYLER / KURUMLAR



- Kullanıcılar
- Güvenen Taraflar



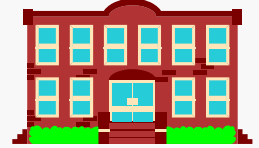
POLİTİKA ARAÇLARI ve ANLAŞMALAR



- CP ve CPS
- Kullanıcı Anlaşmaları
- Güvenen Taraf Anlaşmaları



SERTİFİKA HİZMET SAĞLAYICILARI



SÜREÇLER

- Anahtar Yönetimi
- Sertifika Dağıtımı
- Sertifika İptali
- Diğer Kayıtlar



TEKNOLOJİ

Yazılım ve Donanım Ürünleri

STANDARTLAR

- ISO
- ITU
- ANSI
- RSA Labs
- NIST

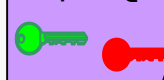


MEKANİZMALAR

- Sayısal İmzalama
- Şifreleme
- Mesaj Gönderme

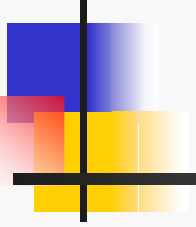


3\$1/2{2



KRİPTOGRAFİK ALGORİTMALAR

- Tek Anahtarlı Yöntemler
- Çift Anahtarlı Yöntemler



**İLGİNİZ VE SABRINIZ İÇİN
TEŞEKKÜRLER !**