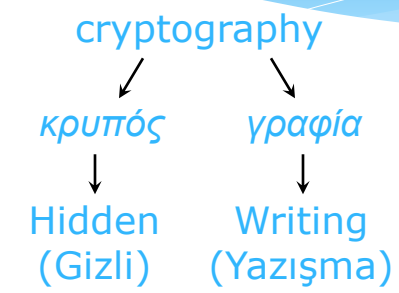
Şifreleme Sistemlerine Giriş ve Açık Anahtar Şifreleme

Yrd. Doç. Dr. Şadi Evren ŞEKER
Mühendislik ve Mimarlık Fakültesi



Şifre (TDK)

1. Gizli haberleşmeye yarayan işaretlerin tümü, kod:
   "İstanbul mümessilliği şifresiyle Mustafa Kemal Paşa'ya, bekledikleri malumatı iletmiştim."- Y. K. Karaosmanoğlu.

2. Gizliliği olan kasa, kapı, çanta vb. şeylerin açılması için gereken rakam

cryptology

κρυπός → Hidden (gizli)

λογια → Speaking (Konuşma)

Kripto (TDK)

1. Siyasi inancını gizleyen kimse.
2. Saklı yazı.

cryptoanalysis

Gizlilik

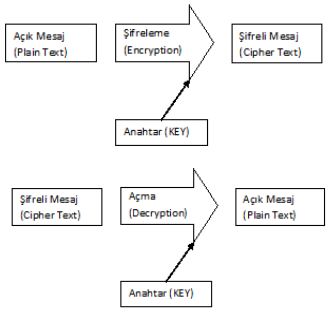
Analizi

Şifreleme (Cryptography)
Güvenlik (Security)

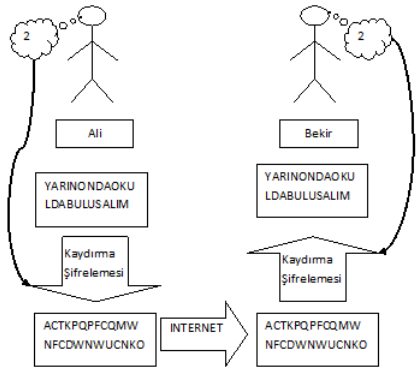
Şifreleme ≠ Güvenlik
Şifreleme ∈ Güvenlik

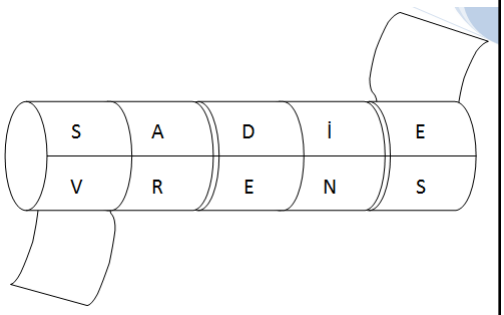
İlkel Şifrelemeler

* Bilgiye Dayalı Şifrelemeler
* Simetrik Şifrelemelerdir



İlkel Şifrelemeler



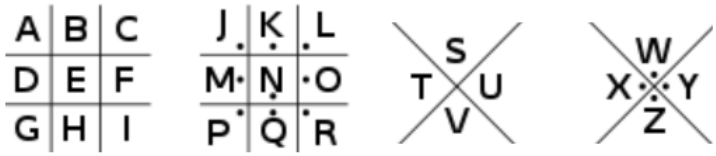


Gizlilik Şifreleme

1883 Auguste Kerchoff tarafından, «La Cryptographie Militaire» yayınlanan esaslar:

- Matematiksel olmasa bile pratik olarak çözülemez bir sistem.
- Gizli tutulmasına ihtiyaç duyulmamalı (Düşmanın eline geçebilir)
- Anahtar iletilebilir ve değiştirilebilir olmalı
- Telgraf ortamında iletilebilmeli
- Taşınabilir olmalı
- Makul seviyede karmaşık ve vakit alıcı olmalı

Pigpen (Mason) Şifrelemesi



SADI EVREN SEKER

RSA

- Yeterince büyük iki adet asal sayı seçilir: Bu sayılar örneğimizde p ve q olsunlar.
- n=pq
- $\varphi(n) = (p-1)(q-1)$
- $1 < e < \varphi(n)$
- $de \equiv 1 \bmod (\varphi(n))$.

- **Şifreleme işlemi:**
- $c = m^e \bmod n$
- **Şifrenin Açılması:**
- $m = c^d \bmod n$

RSA Örnek

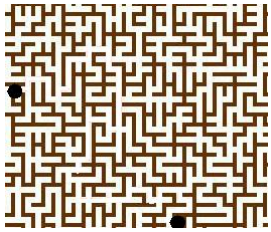
- **Örnek:**
- İki asal sayı seçilir
- $p = 61$ ve $q = 53$
- n değeri hesaplanır n = pq şeklinde
- n = 61 * 53 = 3233
- Totient fonksiyonu hesaplanır
- φ(n) = (p-1)(q-1)
- φ(n) = (61-1)(53-1) = 3120
- totient fonksiyon sonucu ile aralarında asal olan ve 1 den büyük bir sayı seçilir
- e > 1 => e = 17 (3120 ile aralarında asal) , bu sayı aynı zamanda umumî şifredir.
- Hususî şifre olması için bir d sayısı seçilir:
- de ≡ 1 mod(n) olacak şekilde d sayısı bulunur , d = 2753 (çünkü 17 * 2753 = 46801 = 1 + 15 * 3120) Bu sayının hesaplanması sırasında uzatılmış öklit (extended euclid) yöntemi kullanılmıştır.
- Örneğin mesaj olarak 123 gönderilecek olsun:
- 123^{17} mod 3233 = 855 olarak şifreli metin bulunur.
- açacak taraf için tersi işlem uygulanır:
- 855^{2753} mod 3233 = 123 şeklinde orjinal mesaj geri elde edilir.

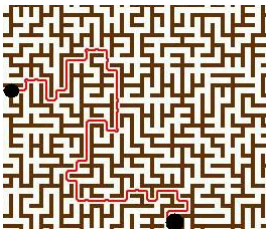
Diffie Hellman Anahtar Değişimi

- Sistemin çalışma mantığı basit bir matematiksel gerçeğe dayanmaktadır buna göre $g^{ab} = g^{ba}$
- Örnek:
  - Anahtar değişimi yapacak iki taraf da p=23 ve g=5 sayılarını kararlaştırıyorlar (bu sayılar ik itaraftan da biliniyor ve umumî şifreler).
  - Alice hususî anahtarı olarak a=6, seçer ve Bob'a gönderir (g^a mod p)
    - 5^6 mod 23 = 8.
  - Bob hususî anahtarı olarak b=15, ve Alice'e gönderir (g^b mod p)
    - 5^{15} mod 23 = 19.
  - Alice (g^b mod p)^a mod p *denklemini hesaplar*
    - 19^6 mod 23 = 2.
  - Bob (g^a mod p)^b mod p *denklemini hesaplar*
    - 8^{15} mod 23 = 2.

Matematiksel Zorluk

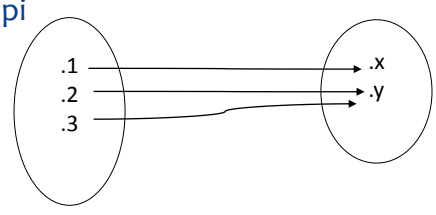
* Karmaşıklık Teorisi (Complexity Theory)
* NP-Hard ve NP-Complete Kümeleri





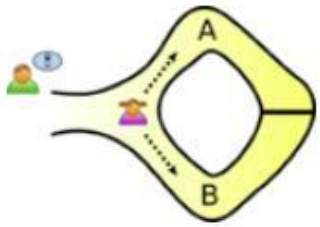
Mesaj Özetleri (Hashing)

* Tek Yönlü Fonksiyonlar (Yazı Tura)
* Çakışma (collision) oranı
* Entropi

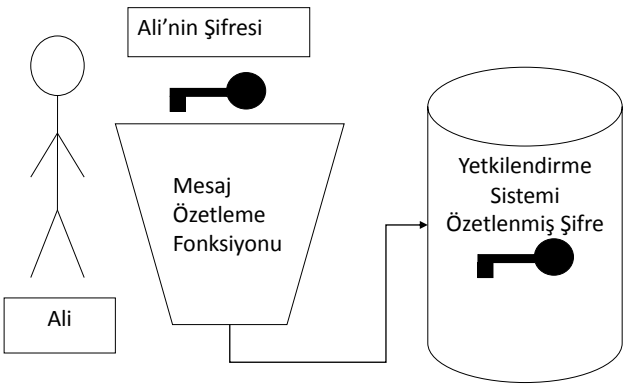


Güvenlik Protokolleri (Security Protocols)

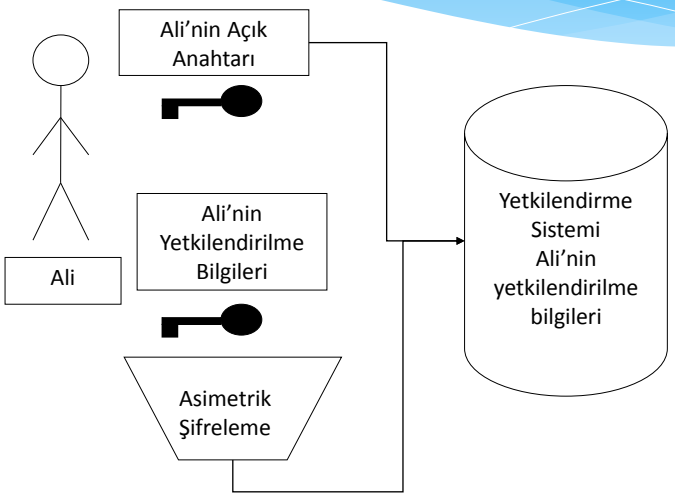
* Sıfır Bilgi İspatı (Zero Knowledge Proof)
* Satrançta Büyük Usta Problemi



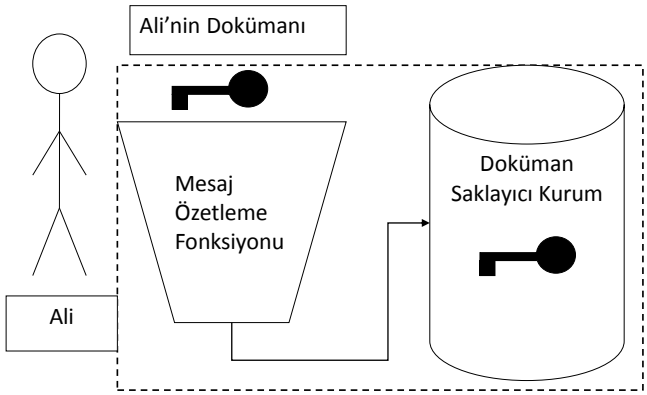
Yetkilendirme (Authentication)



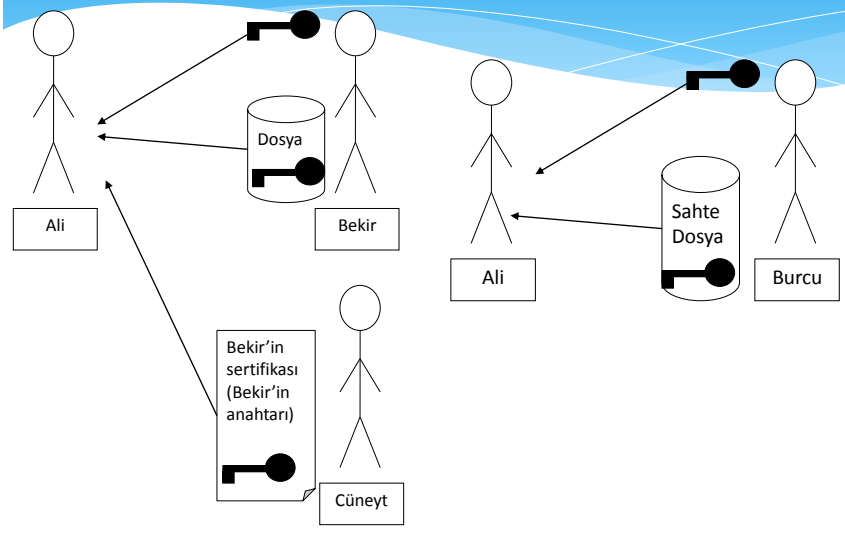
Dijital İmza



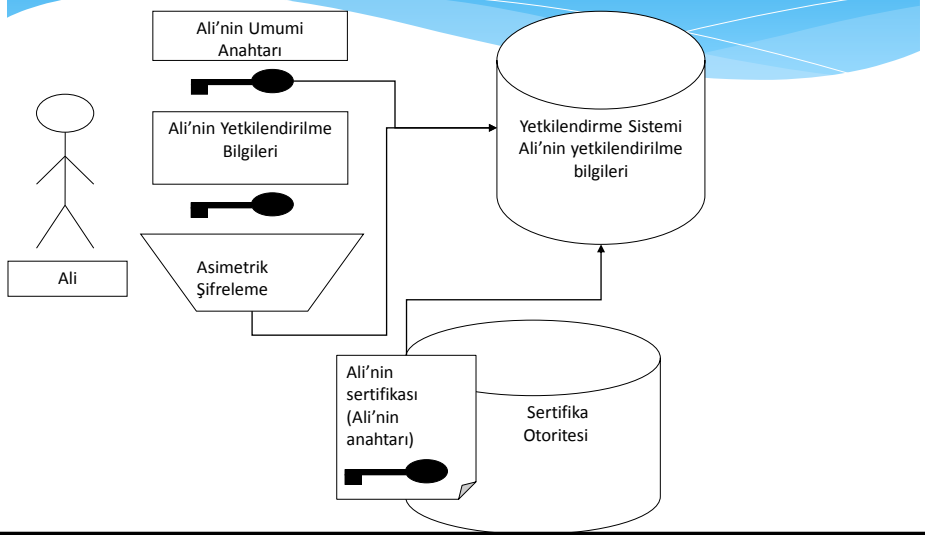
Kör İmzalar (Blind Signatures)



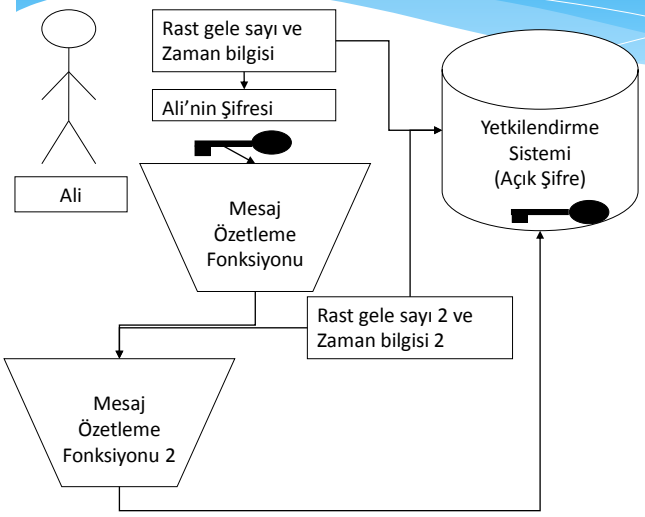
Sertitikalar (Certificates)



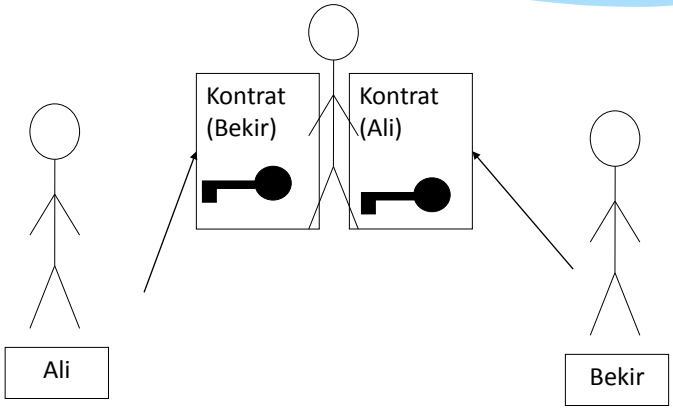
Sertifika ile Yetkilendirme (Authentication by Certificate)



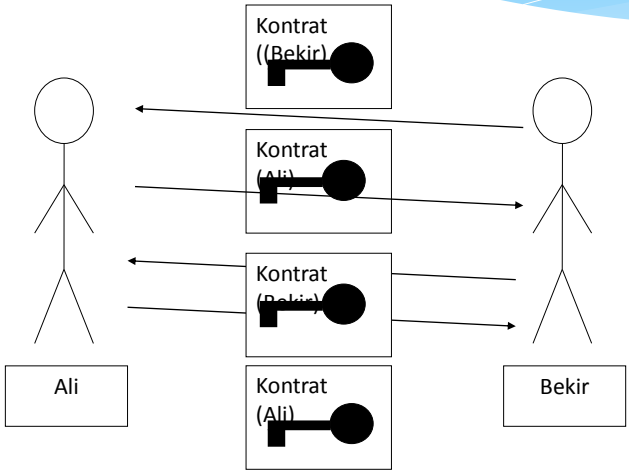
Çift Güçlü Şifre Girişleri (Double Strength Password Login)



Eş zamanlı Kontrat İmzalama



Eş zamanlı bilgi değişimi



Teşekkürler

http://www.SadiEvrenSEKER.com
http://www.BilgisayarKavramlari.com