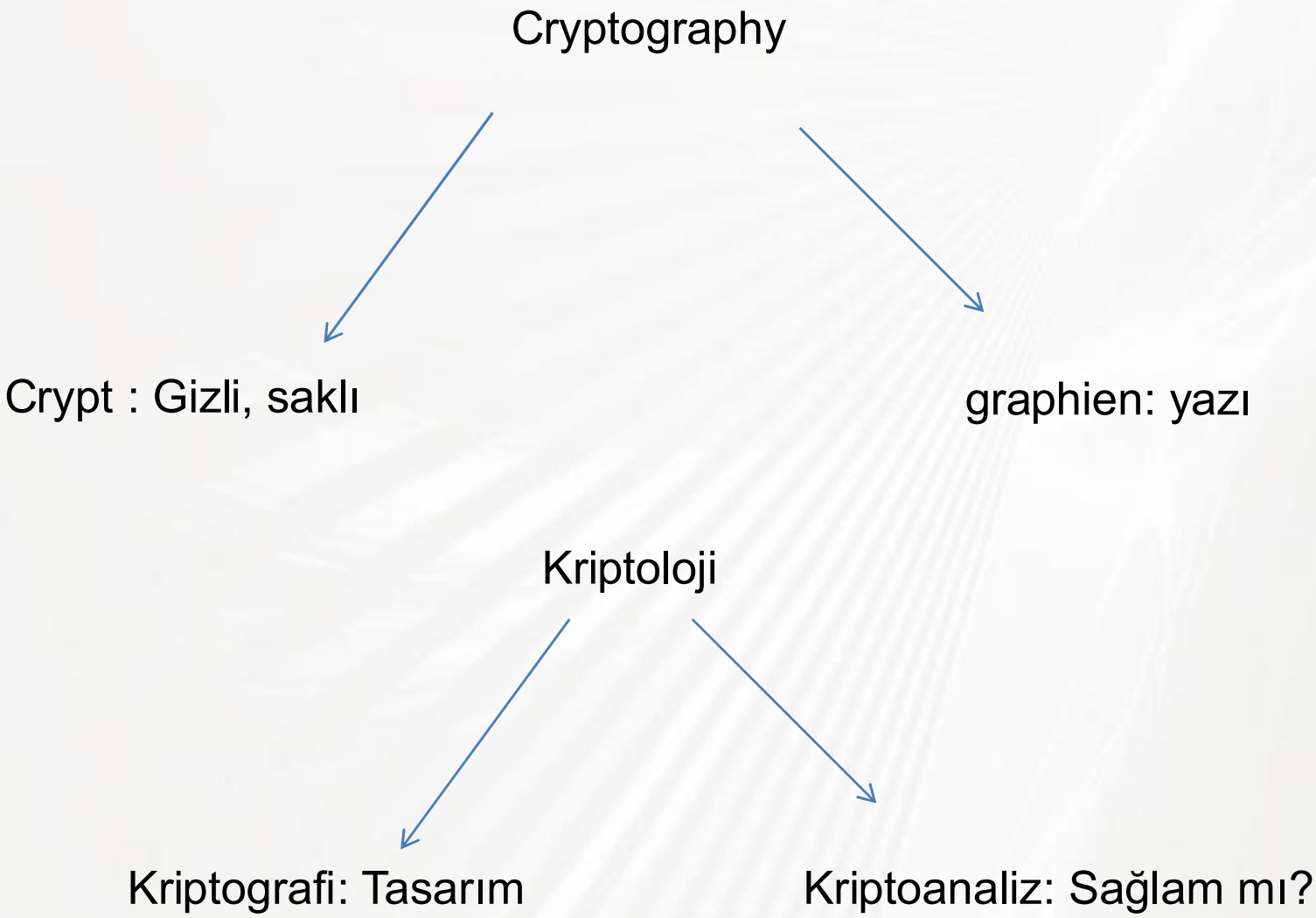
Kriptoloji


Cryptography
Crypt : Gizli, saklı
graphien: yazı
Kriptoloji
Kriptografi: Tasarım
Kriptoanaliz: Sağlam mı?

Veri Güvenliği

TÜBİTAK

Hassas verinin güvenliği deyince ne anlıyoruz?

Verinin korunması? Ama nerede? Depolarken, transfer ederken?

Veriye üçüncü şahısların ulaşamaması?

Veriyi yetkisizlerin değiştirememesi?

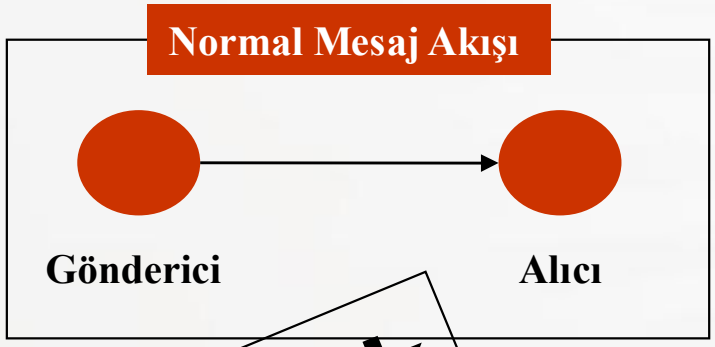
Veriyi yetkisizlerin oluşturamaması?

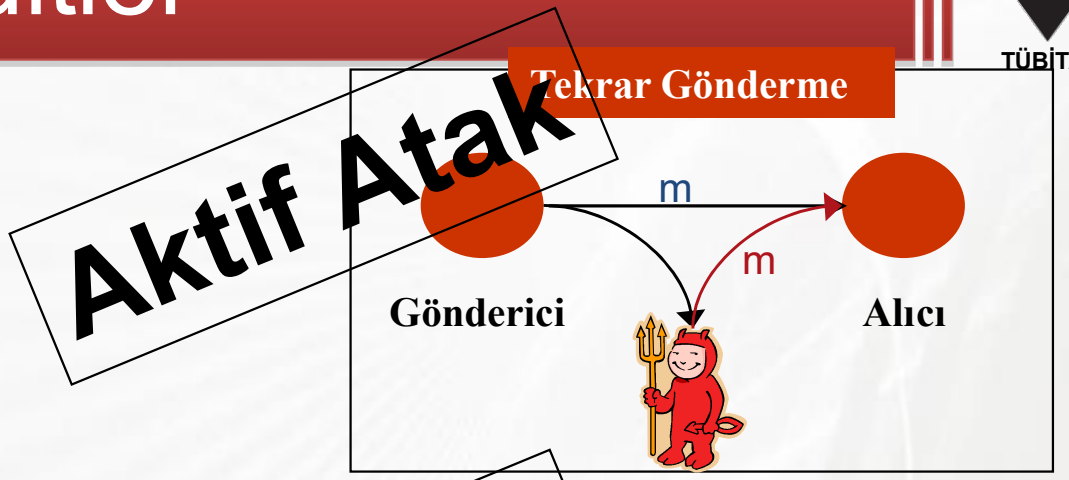
Yetkililerin veride yaptığı değişiklikleri kabullenmesi?

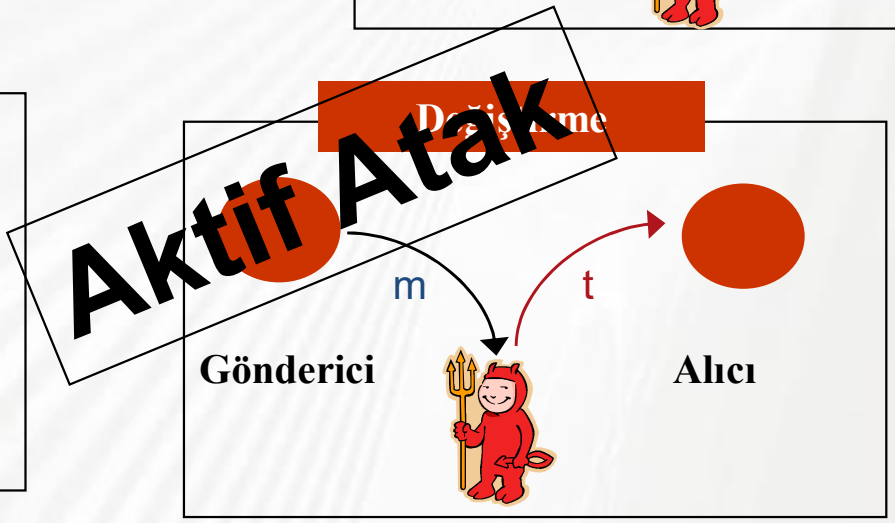
Ama nasıl?

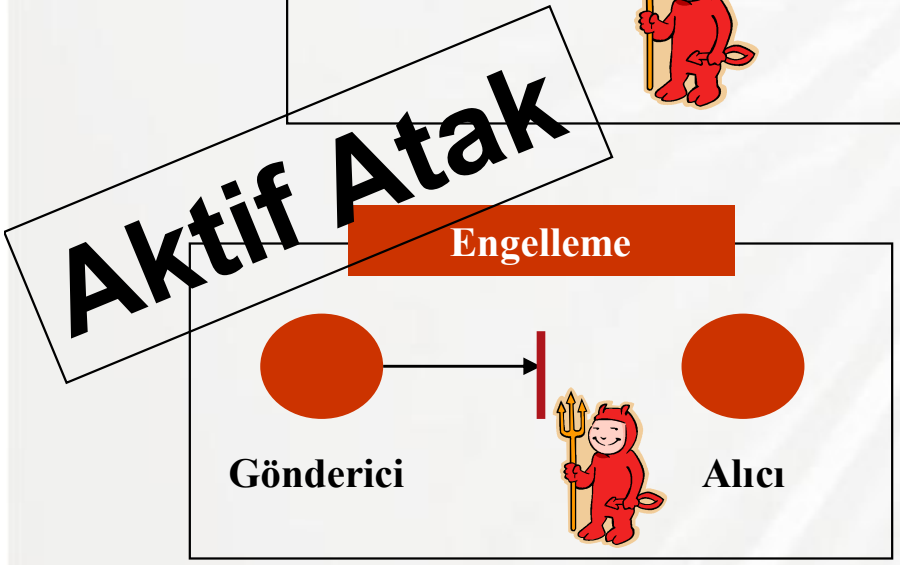
Her yiğidin bir yoğurt yiyişi var: Kriptolojinin yöntemi matematiksel problemler! Bu dersin ana kapsamı kriptolojinin temel yöntemlerini tanımak

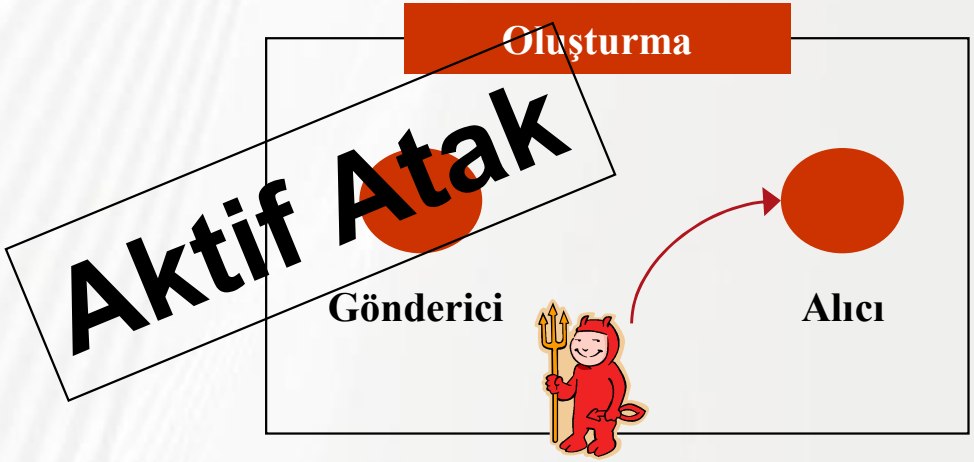
Açık Kanalda Tehditler











Kriptoloji nedir?

Mesajım Ayşe'ye gitti mi?

Erişebilirlik

Mesajım Ayşe'den başkasına gitti mi?

Gizlilik

Arada üçüncü şahıslar mesajı görmüş müdür?

Bora

Gerçekten Bora mı gönderdi?

Kaynak Doğrulama!

Mesaj yolda değişmiş olabilir mi?

Bütünlük!

Ayşe

Bora "Ben göndermedim" der mi?

İnkar Edemezlik!

Kriptolojinin Tanımı

TÜBİTAK

Gizlilik, veri bütünlüğü, kimlik doğrulama inkar edemezlik gibi

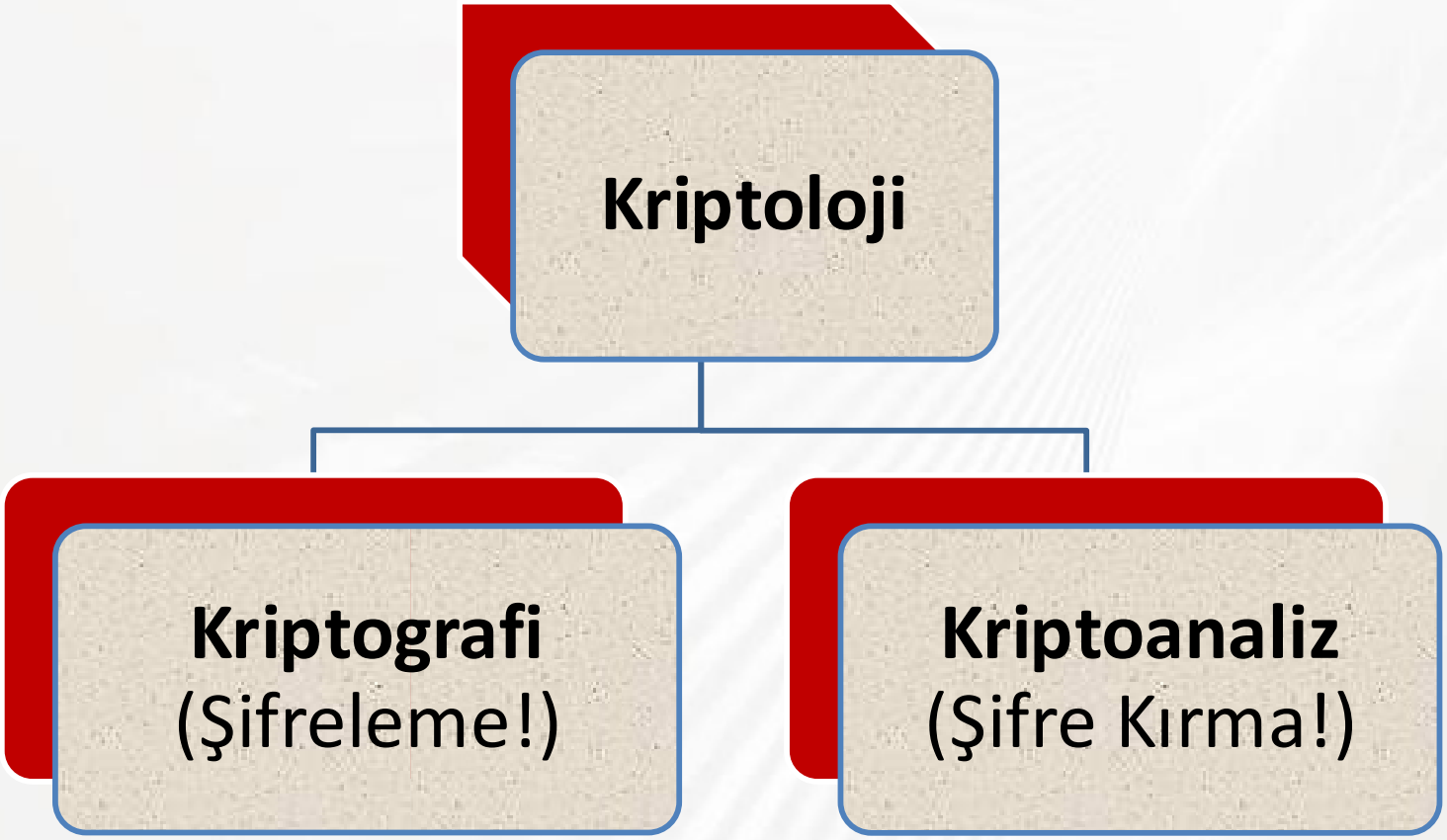
bilgi güvenliği problemlerine

matematiksel yöntemler kullanarak

çözüm getirme ve bu çözümleri çürütme bilimidir.

Kriptoloji sadece şifreleme/şifre kırma değildir!

TÜBİTAK



Matematiksel Yöntem?

TÜBİTAK

- Bilgi güvenliği hizmetini bir matematik probleminin çözümünün zorluğuna dayandırma
- Problemi çözen kripto hizmetini de çözümü oranında ihlal eder (sistemi kırar!)
- Çözüm zorluğu: Çözüm algoritmasının karmaşık olması. Eksponansiyel ya da alteksponansiyel zamanda çözüm
- Örnek: Ayrık logaritma problemi, çarpanlara ayırma problemi, doğrusalsız denklem sistemi çözme problemi

Kriptoanaliz: Şifre Kırmak

TÜBİTAK

Güvenlik Yaklaşımları

- Şartsız güvenlik (Mükemmel güvenlik)
- Hesapsal güvenlik

Kripto Sistemini Kırmak: Belirlenmiş bir hesaplama gücüne karşı sağlandığı iddia edilen bir kripto hizmetinin daha az hesaplama gücüyle engellenmesi

Kriptoanaliz: Kripto sistemini kırma çalışmaları

Hesapsal Güvenlik: Bütün kriptolar kırılabilir!

Hesapsal güvenlik ile sağladığı güvenlik: 10^4 şifre denemesi

Daha az deneme ile şifreyi bulan sistemi kırmış olur!

Kriptografi-Steganografi

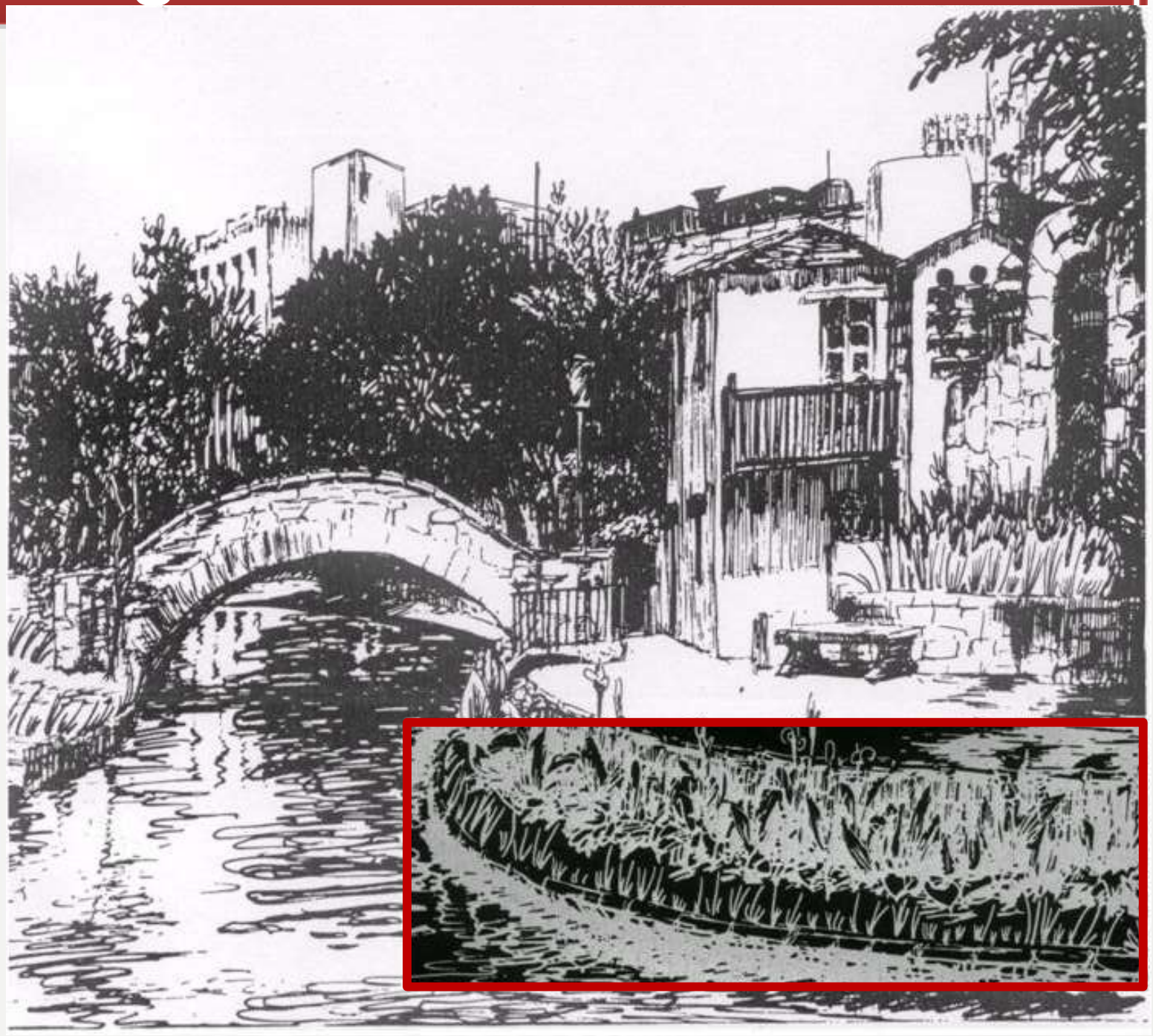
TÜBİTAK

Kriptografi ile gizlilik: gizli yazının yapıtaşlarının matematiksel işlemlerden geçirilip karıştırılması ve değiştirilmesi

Steganografi ile gizlilik: gizli yazının varlığının saklanması

Steganografi

TÜBİTAK



Kriptografik Hizmetler

TÜBİTAK

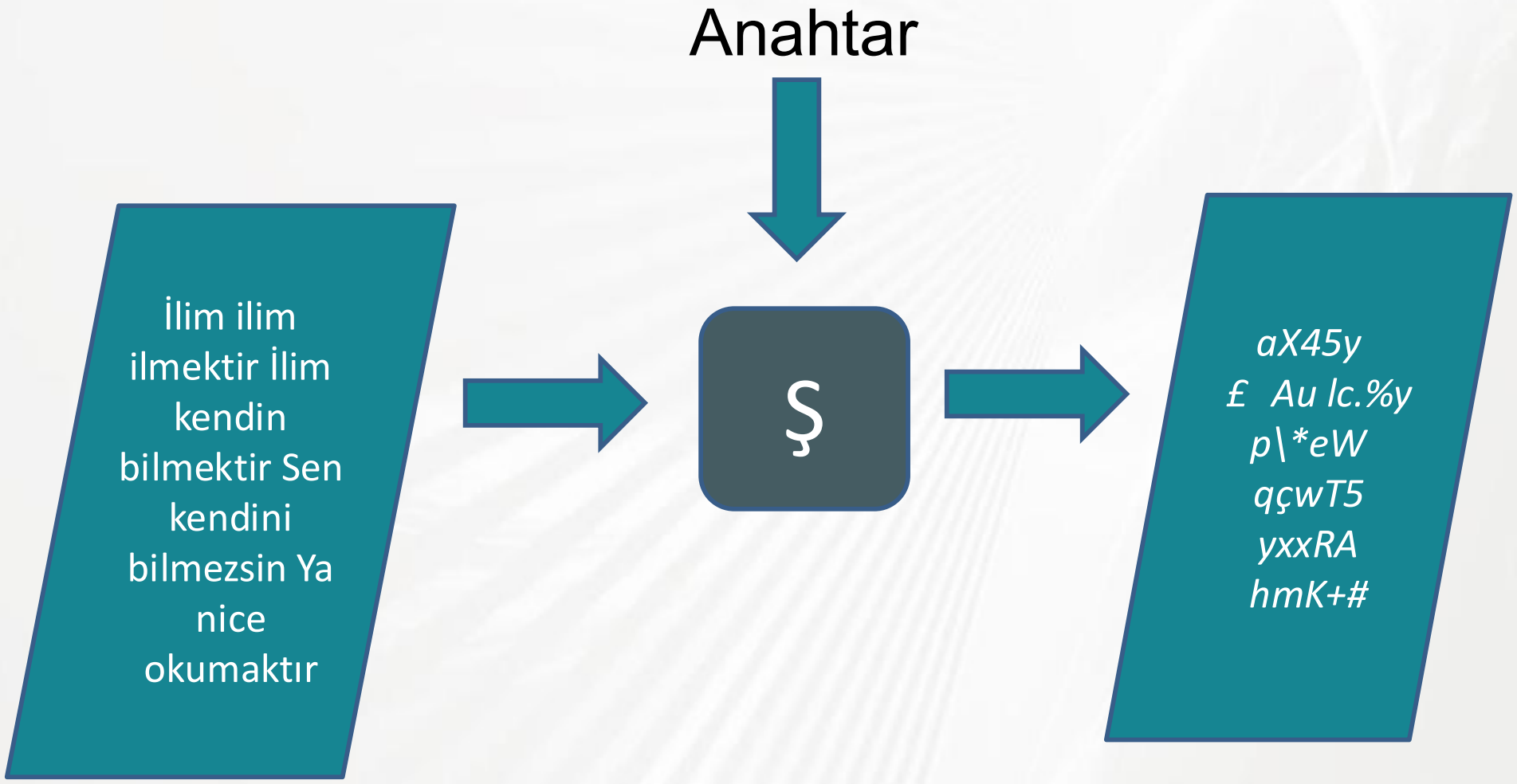
- Gizlilik
- Veri Bütünlüğü
- Asıllama (Doğrulama)
  - Kimlik doğrulama
  - Kaynak doğrulama
- İnkar Edememe
- Anonimlik/ Mahremiyet
- Tazelik
- Erişebilirlik/Kullanılırlık

Kripto Protokolleri

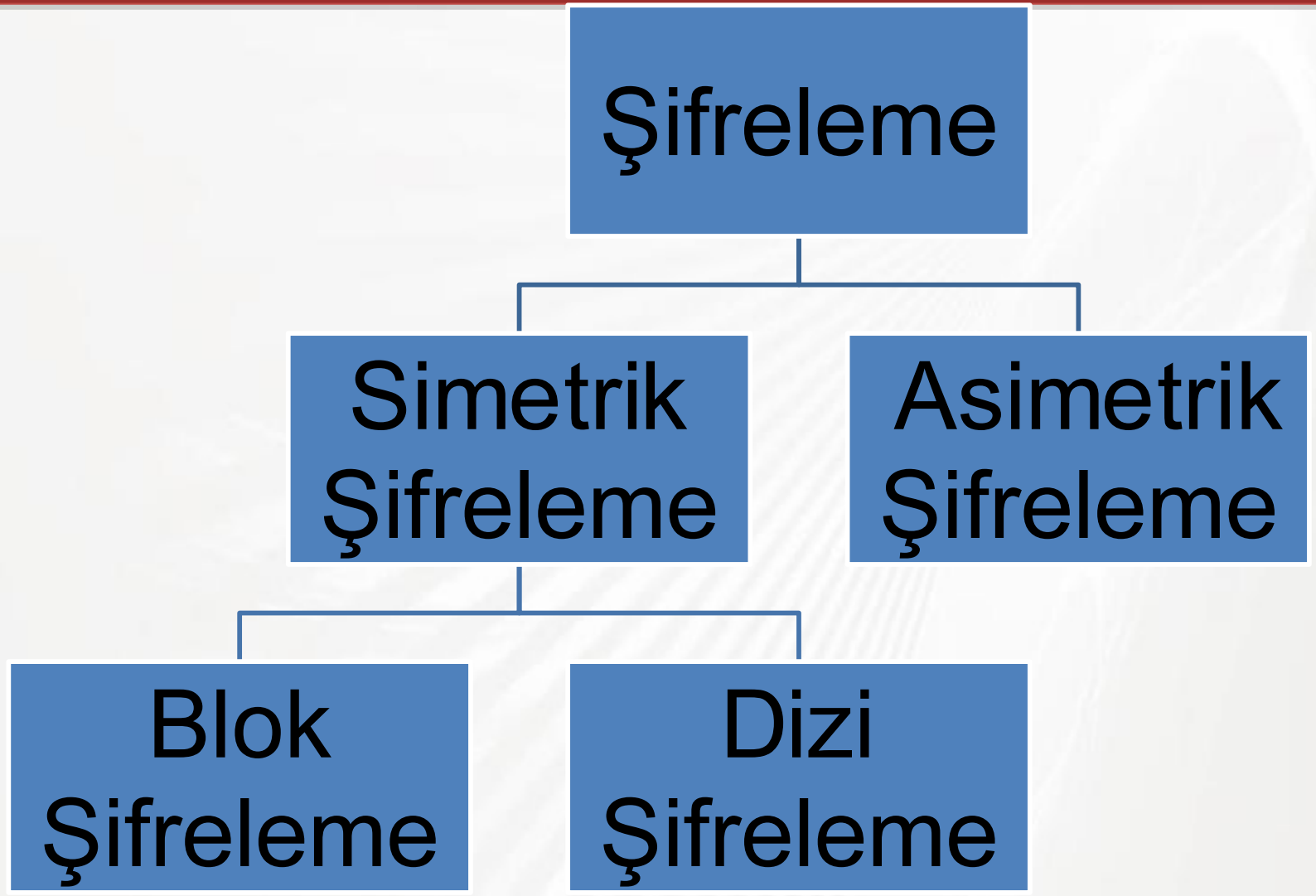
Kriptografik algoritmalar kullanarak bir ya da birden fazla kriptografik hizmeti bir arada sağlayan kurallar dizisi

SSL/TLS, IPSec, WEP, WPA, PGP: Anahtar dağıtımı, kimlik doğrulama, gizlilik, bütünlük

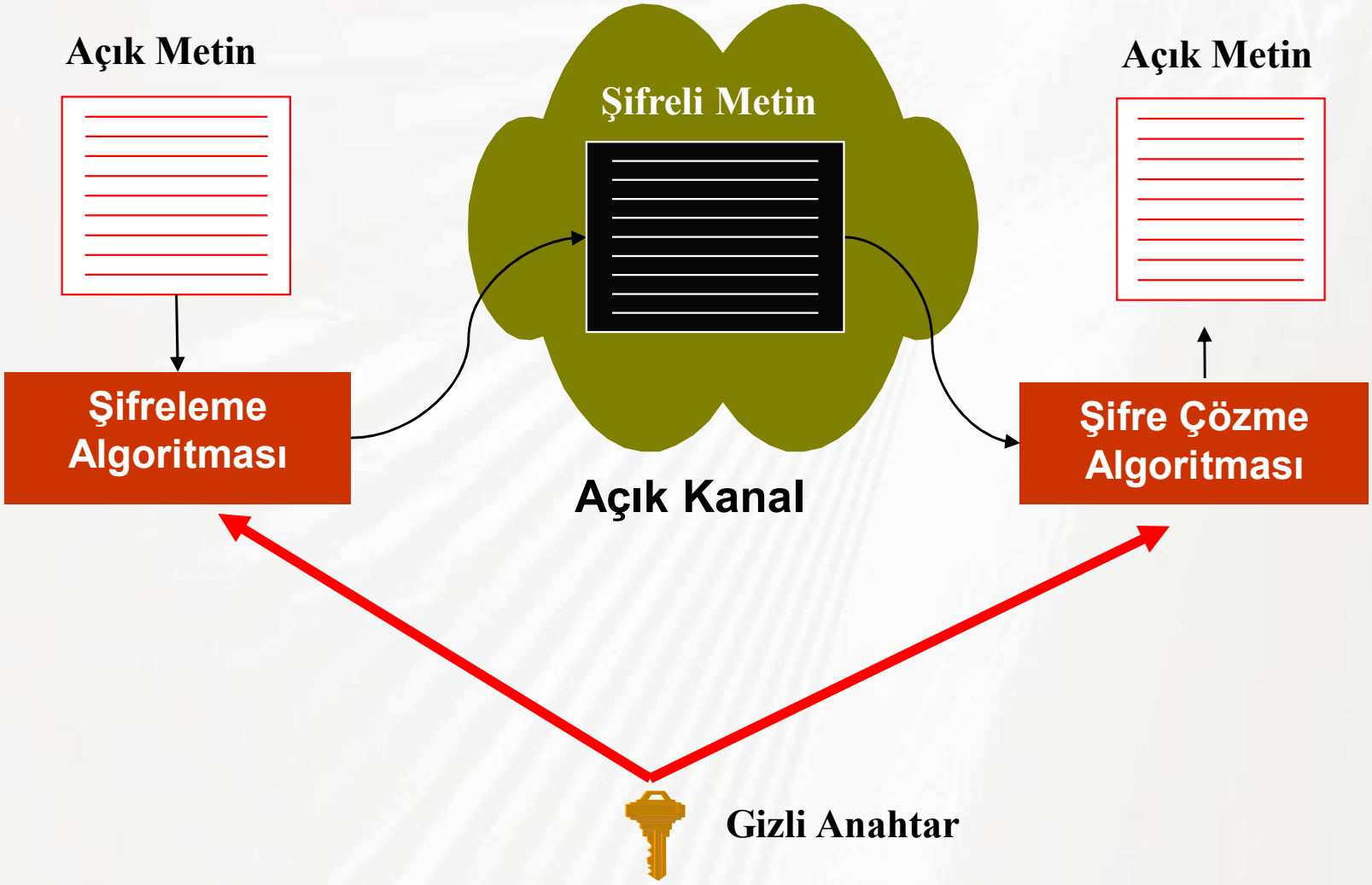
Gizlilik: Şifreleme



Gizlilik


Şifreleme
Simetrik Şifreleme
Asimetrik Şifreleme
Blok Şifreleme
Dizi Şifreleme

Simetrik Şifreleme



Simetrik Şifreleme Algoritmaları

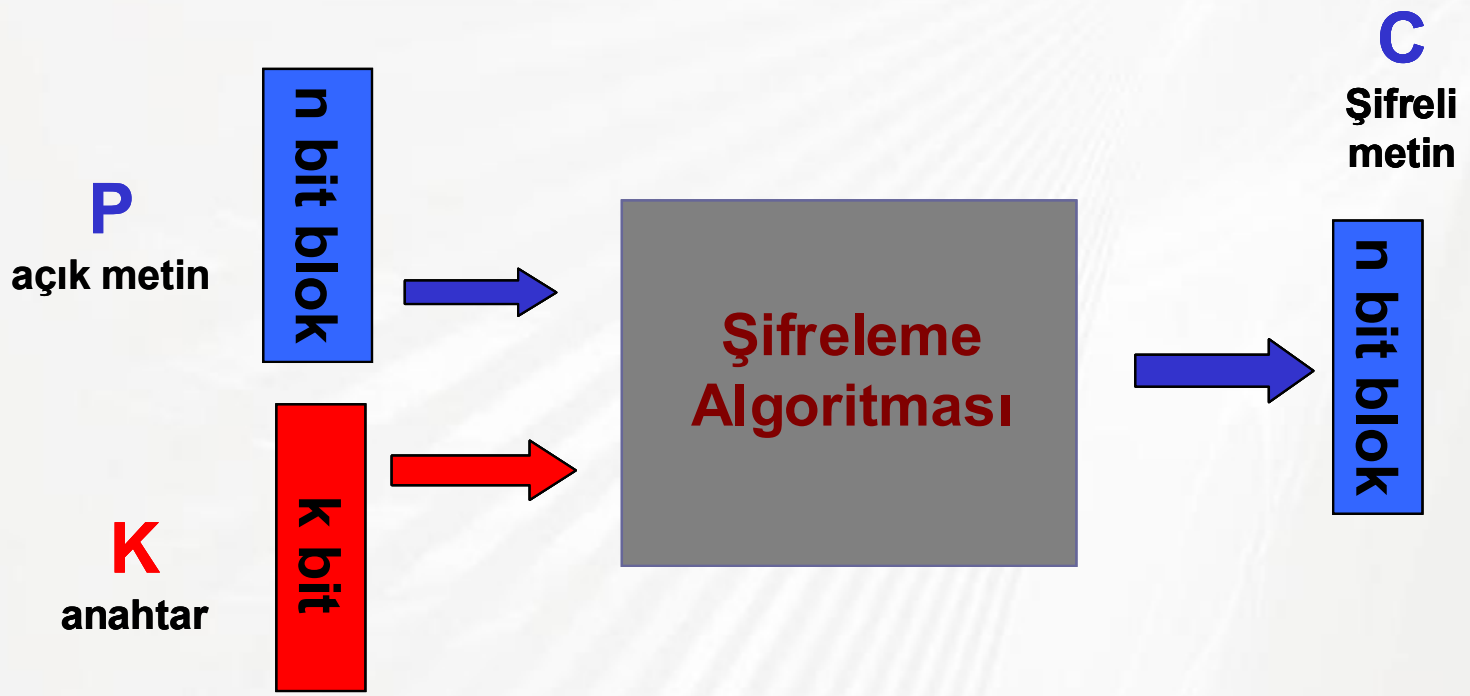
TÜBİTAK

- AES: Blok şifreleme, 128 bit blok, 128,192,256 bit anahtar
  - Vincent Rijmen, John Daemen, 2001 NIST standardı, SSL, TLS, PGP, WEP, WPA, IPSec,...
- DES: Blok şifreleme, 64 bit blok, 56 bit anahtar
  - IBM, 1976. 3DES, ATM cihazlarında...
- A5/1,A5/2: Dizi şifreleme, 64 bit anahtar, GSM
- E0: Dizi şifreleme, 128 bit anahtar, Bluetooth

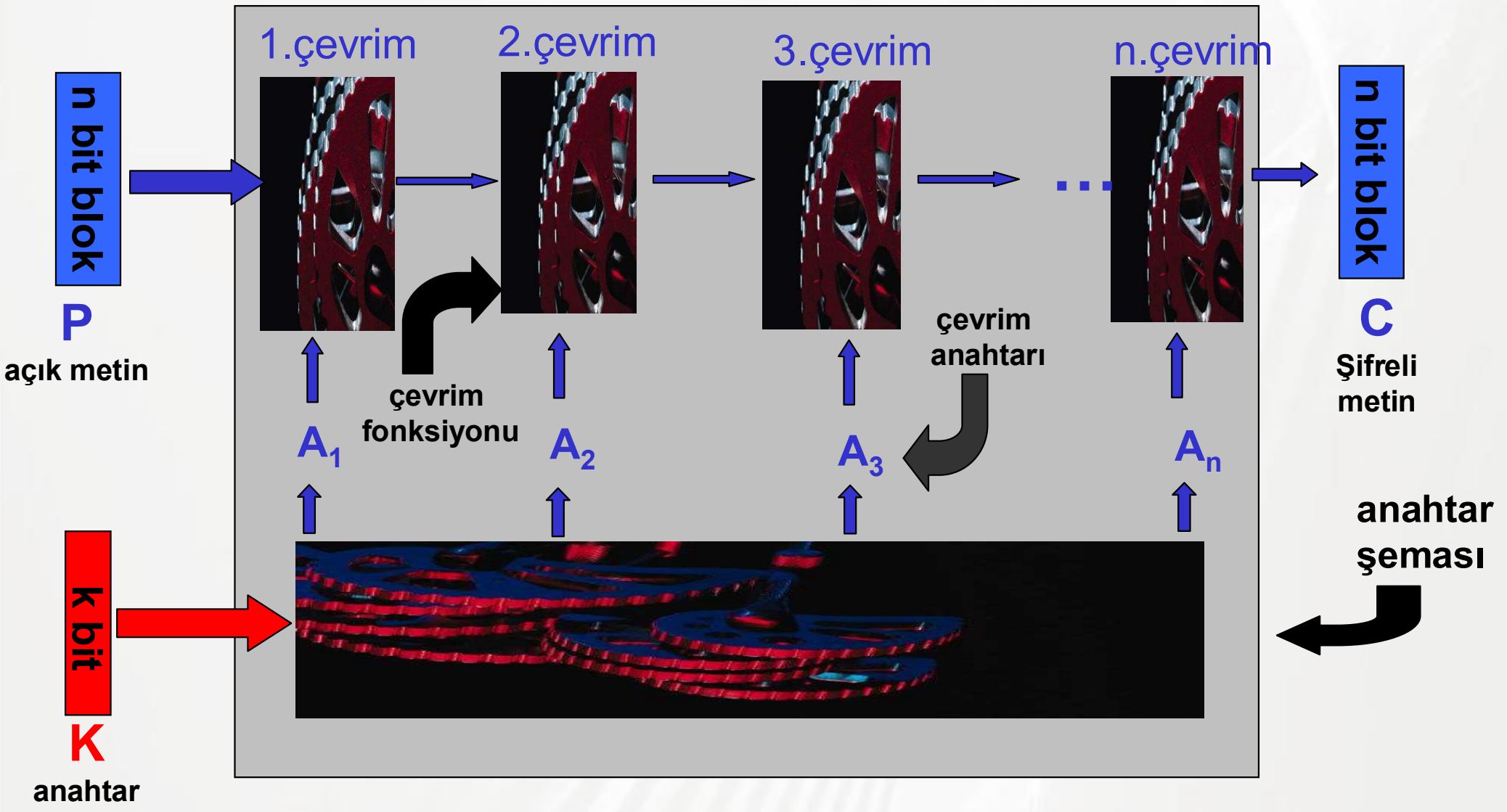
Blok Şifreleme

- Açık metin bloklara bölünür ve her blok diğerlerinden bağımsız şifrelenir
- Döngüseldir: Her döngü bir çevrim
- Her çevrimde farklı bir gizem kullanılır: alt anahtar
- Alt anahtarlar ana anahtardan anahtar şeması algoritmasıyla türetilir
- Hafızasızdır

Blok Şifreleme

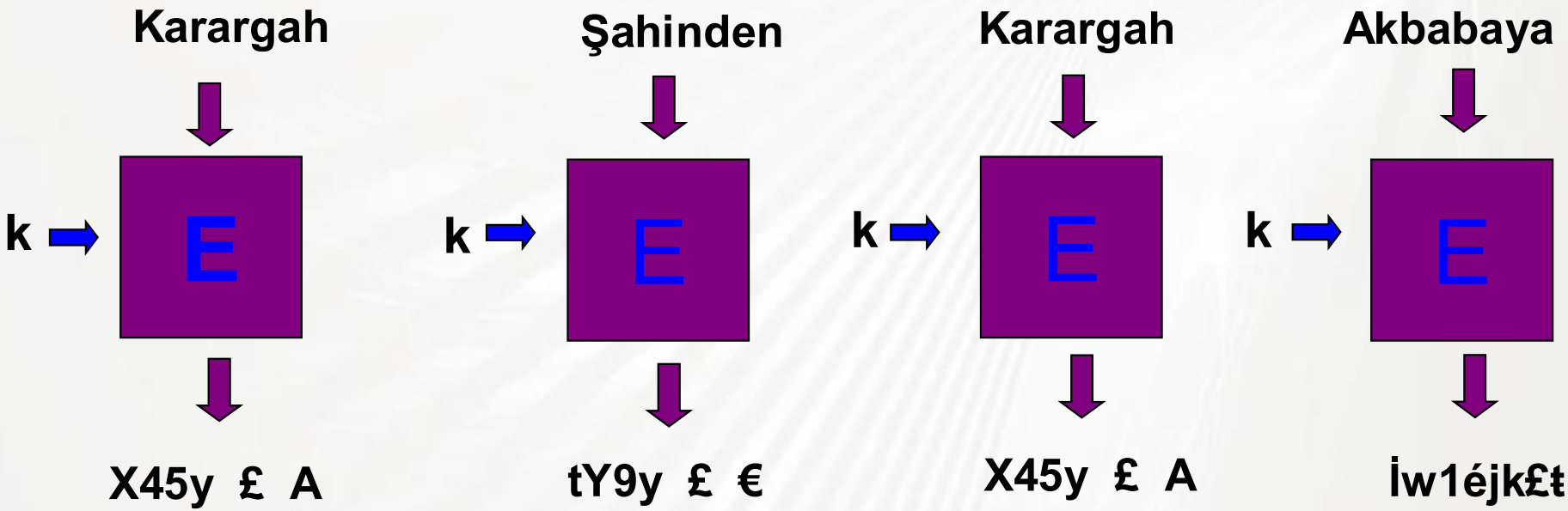


Blok Şifreleme



Blok Şifreleme

- EKK (Elektronik Kod Kitabı) olarak kullanım: Aynı açık metin blokları aynı kapalı metin blokları oluşturur!

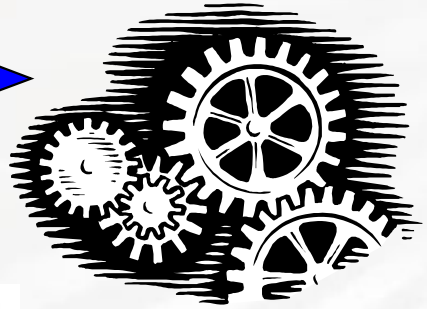


Dizi Şifreleme

TÜBİTAK

Kayan Anahtar Üreteci

K →



Üretecin hafızasında zamanla değişen içsel durum kayıtlı

Kayan Anahtar

1011110101001000011101000110001000….

⊕

P → 1111100101000101010000010101000110…

=

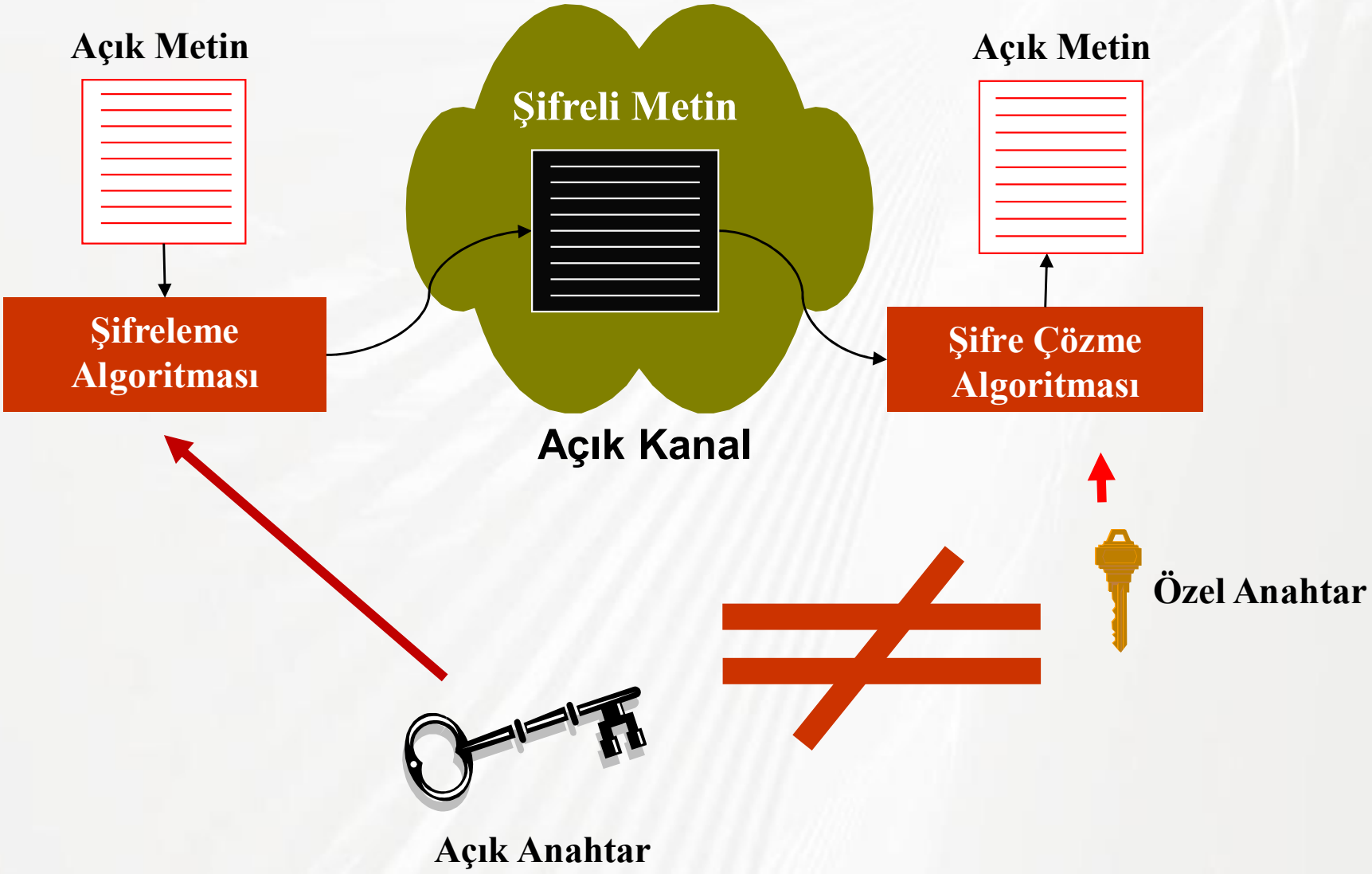
C → 0100010001011010111001001001010001…

Blok Şifreleme ⟷ Dizi Şifreleme

TÜBİTAK

- Blok şifreleme daha esnektir
  - Blok şifreleme dizi şifreleme modunda kullanılabilir
  - Özet fonksiyonu
  - Kimlik doğrulama, RSÜ
- Dizi şifreleme genellikle daha hızlıdır ve daha az yer kaplar
  - Yazılım:HC128 3 c/byte, AES 12 c/byte
  - Donanım: Trivium 3000 GE, Grain 2400 GE, AES 5000-100.000 GE, KATAN 600 GE
- Dizi şifrelemenin tasarım kriterleri gelişmemiş
- Dizi şifrelemede eş zamanlama için ek mekanizma gerekli: Mekanizmada zayıflık riski
- Dizi şifrelemede güvenlik riski yüksek:
  - Kayan anahtarın tek kullanımlık özelliği
  - Kayan anahtarın rastsallığı
  - Bütünlük gereken uygulamalar

Asimetrik Şifreleme (Açık Anahtarlı Şifreleme)

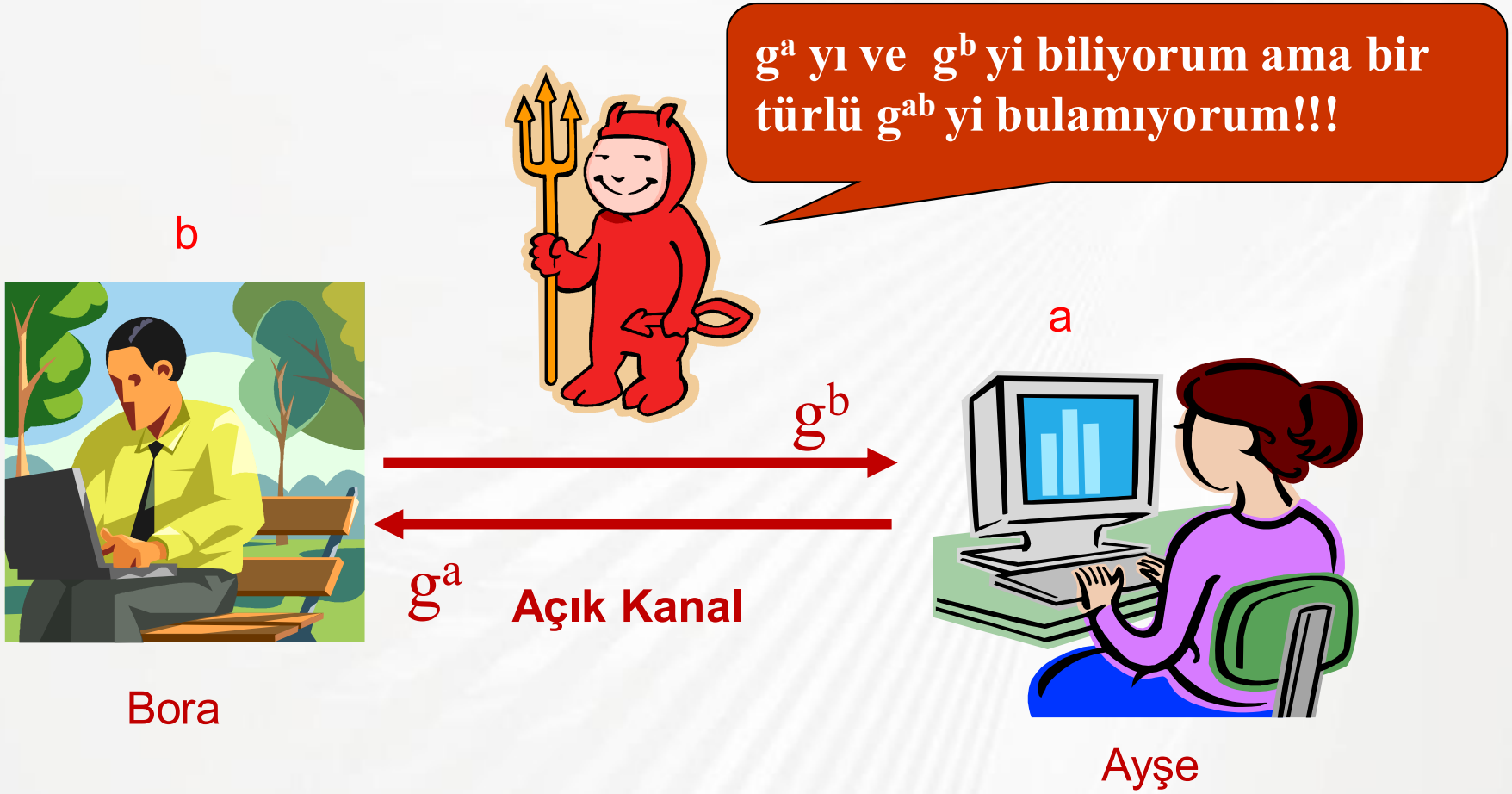


Açık Anahtarlı Kripto Sistemler

TÜBİTAK

- Diffie-Hellman 1976
- RSA: Rivest Shamir Adleman, 1977
- ElGamal, 1985
- Sayısal imzalar:
  - DSA: Sayısal İmza Algoritması
  - ECDSA: Eliptik Eğri Tabanlı Sayısal İmza Algoritması

Diffie Hellman Anahtar Paylaşım Protokolü



Ortak Anahtar: g^{ab}

Veri Bütünlüğü: Özet fonksiyonları

TÜBİTAK

- Herhangi uzunlukta mesajdan sabit uzunlukta veri
- Aynı özeti veren iki mesaj bulunamasın!

  (Hesapsal Güvenlik)
- Kullanım yerleri

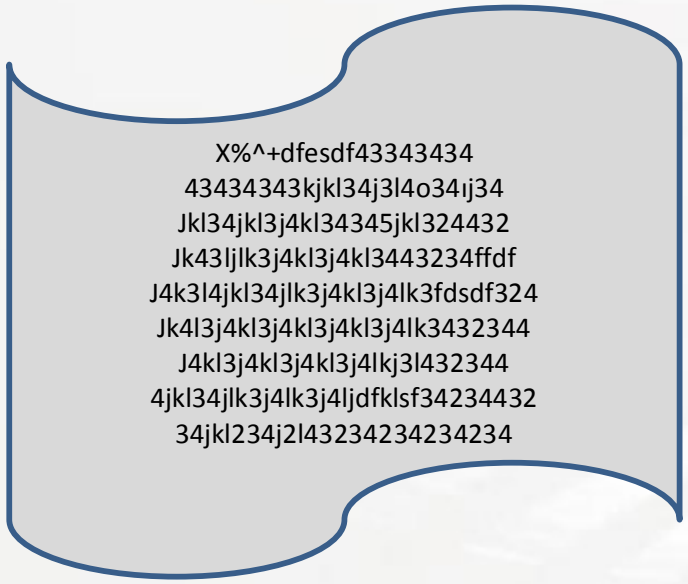
  Sayısal imza

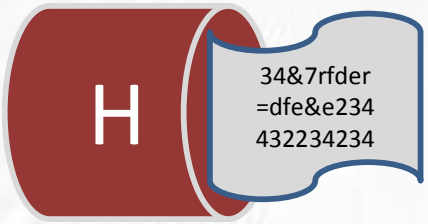
  Parola Saklama

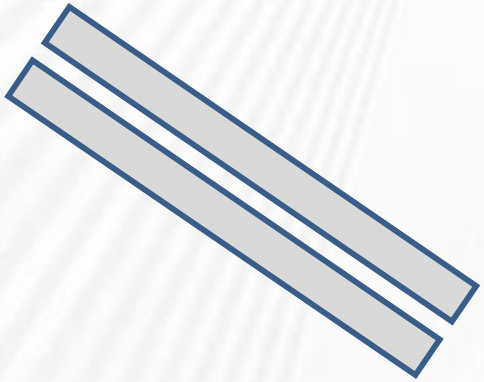
  Arşivleme

  İnternette dosya indirme
- SHA ailesi: SHA-1, SHA-2
- MD ailesi: MD4, MD5

Özet fonksiyonları







Mesaj (herhangi uzunlukta olabilir)

Özet mesajın parmak izi olsun,
Mesajı temsil etsin!

Mesajın Özeti
(sabit uzunlukta)

Özet fonksiyonunun güvenlik özellikleri

TÜBİTAK

- Çakışmaya dayanıklılık (Collision Resistance): Aynı özeti veren iki mesaj bulmak hesapsal olarak imkansız. Eşik güvenlik $2^{n/2}$, *n:* özet boyu

- Ters Görüntüye dayanıklılık – Tek yönlülük (Preimage Resistance – one way function): Verilmiş bir özet değerine sahip mesaj bulmak hesapsal olarak imkansız. Eşik güvenlik 2^{n} , *n:* özet boyu

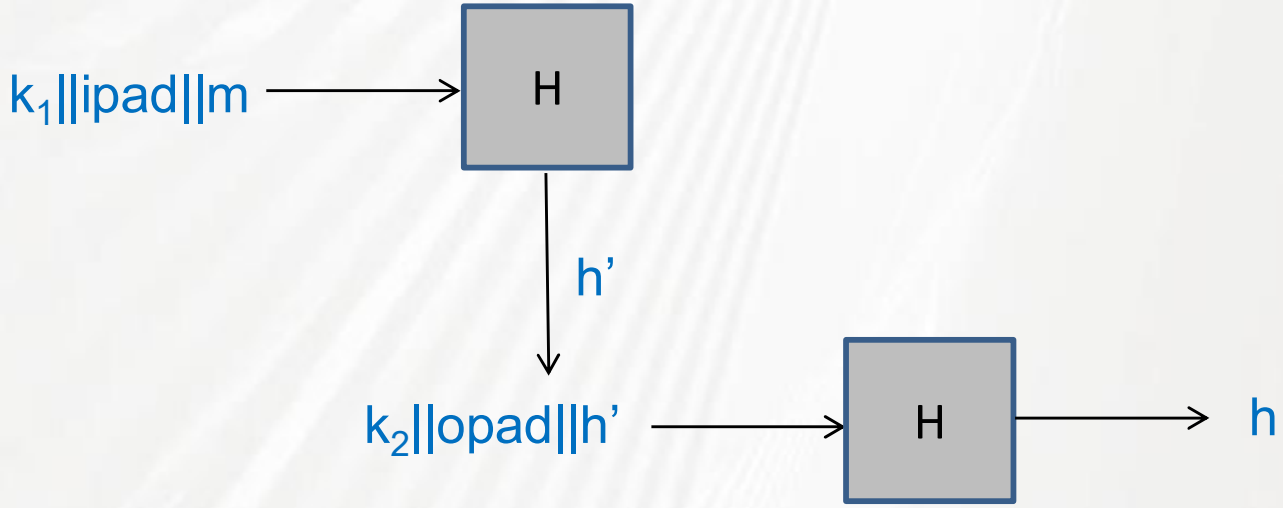
- İkinci Ters Görüntüye dayanıklılık (Second Preimage Resistance): Verilmiş bir mesajla aynı özeti veren başka bir mesaj bulmak hesapsal olarak imkansız. Eşik güvenlik 2^{n} *n:* özet boyu

Anahtarlı Özet: HMAC

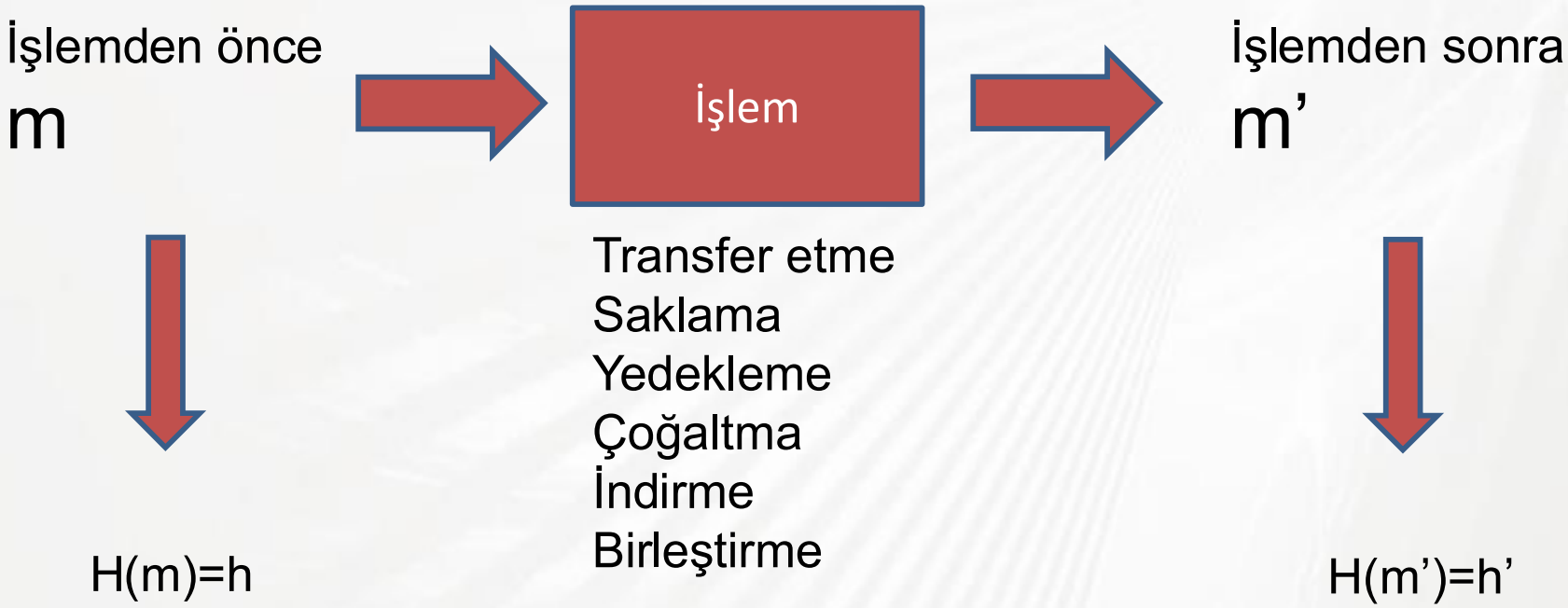
- Anahtar ve mesajdan özet üretiliyor
- HMAC(k,m)=H(k || m)? Mesaj uzatma atağı!
- HMAC(k,m)=H(m || k)? Çakışma olan mesajlar!
- FIPS PUB 198 standardı: SHA-1 ve MD-5 kullanılıyor
- HMAC-SHA-1, HMAC-MD5
- IPSec ve TLS protokollerinde

$$HMAC(k,m)=H(k_2||opad||H((k_1||ipad)\ ||m))$$

- opad ve ipad sabit değerler



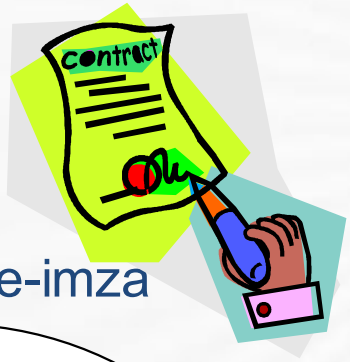
Özet fonksiyonu kullanım alanı



h=h'?

Doğrulama (Asıllama)

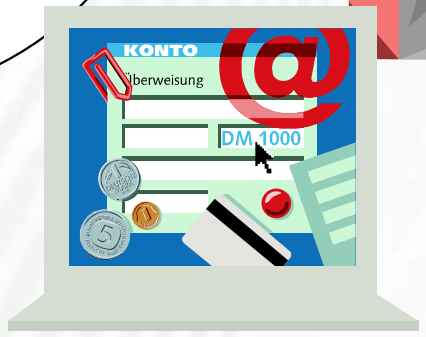
IFF



e-imza

- Sayısal imza
- ATM cihazları
- İnternet bankacılığı
- Çağrı merkezleri
- Parolalar

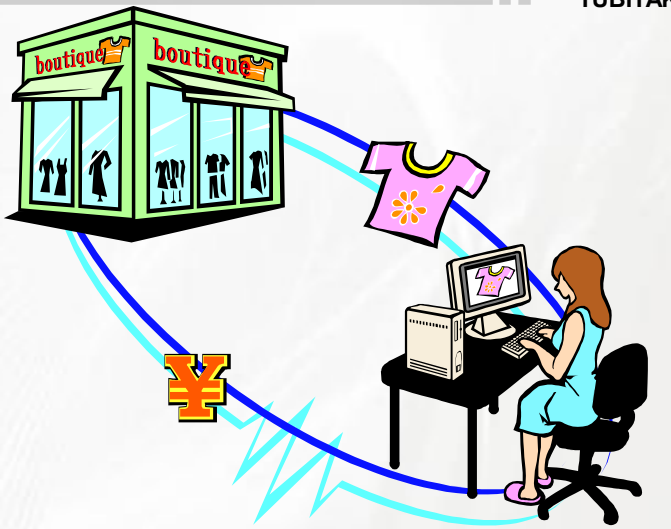
-gün ay yıl olarak doğum tarihiniz?
-annenizin kızlık soyadı?



www.internetbank.com.tr

İnkar Edememe

- Asimetrik sistem
- Sayısal imza
- e-Ticaret
- İnternet bankacılığı
- İnternet alışverişi



Sayısal İmza

Açık Anahtarlı İmzalama