TASNİF DIŞI

Temel Kriptoloji ve Bilgi Güvenliği

Emrah DURMAZ

Uzman Araştırmacı
E-Posta: emrah.durmaz@kamusm.gov.tr

TÜBİTAK
KAMU SERTİFİKASYON MERKEZİ

Sunum Planı

- Kriptoloji Nedir
- Elektronik Tehditler ve Güvenlik
- Basit Şifreleme - Güvenli Şifreleme
- Simetrik Kriptografi - Gizli Anahtarlı Sistemler
- Asimetrik Kriptografi - Açık Anahtarlı Sistemler
- Elektronik İmza

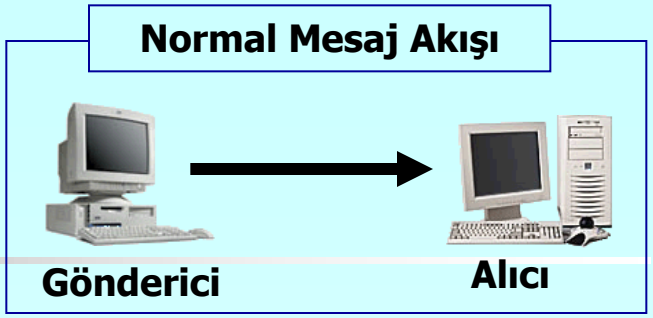
Kriptoloji Nedir?

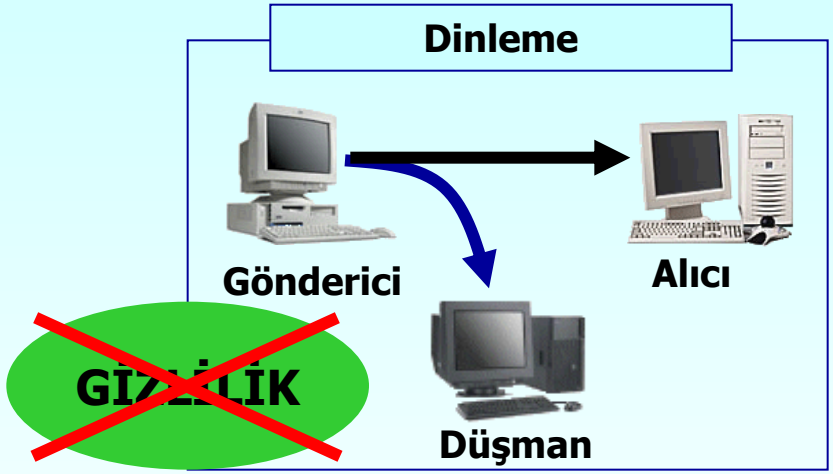
- Kryptos (gizli dünya) logos (bilimi)
- Kriptoloji = Kriptografi + Kriptoanaliz
- Kriptografi, haberleşen iki veya daha fazla tarafın bilgi alışverişini emniyetli bir şekilde yapmasını sağlayan, temeli matematiksel zor problemlere dayanan teknik ve uygulamaların bütünüdür.
- Kriptoanaliz, kriptografik sistemlerin kurduğu mekanizmaları inceler ve çözmeye çalışır.

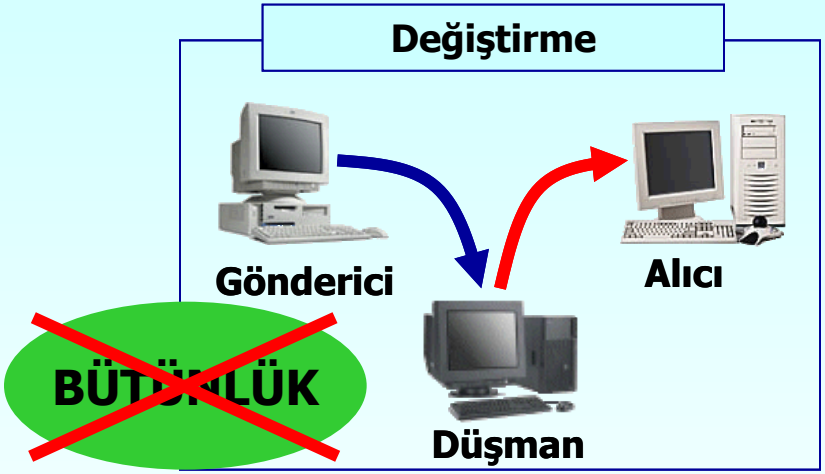
Haberleşmede Güvenlik Ögeleri

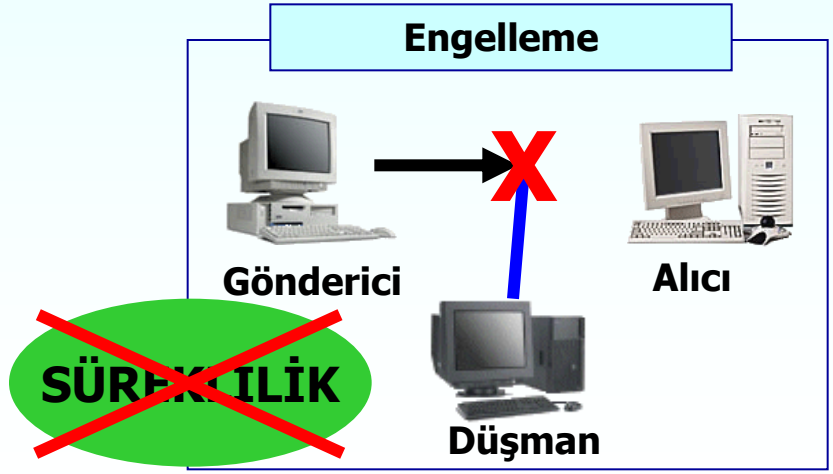
- Gizlilik (Confidentiality of Content)
- Bütünlük (Integrity of Content)
- Kimlik Doğrulaması (Authentication of Origin)
- İnkar Edememezlik (Non-repudiation)
- Süreklilik

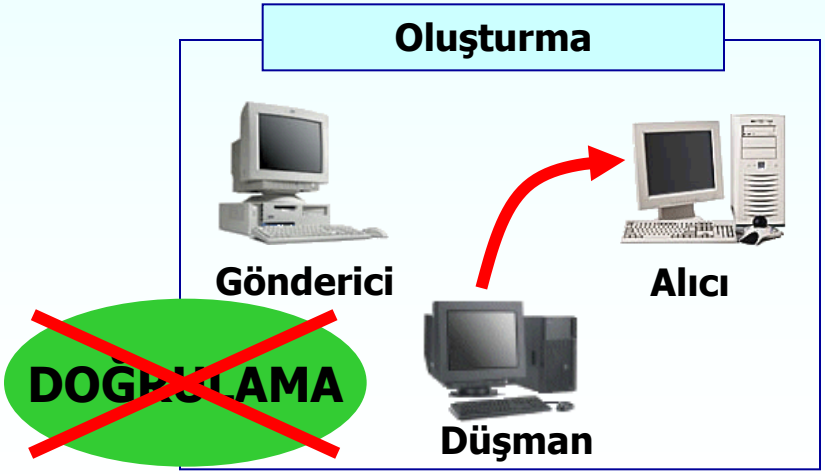
Elektronik Tehditler











Basit Şifreleme Yöntemleri

Mono Alfabetik Şifreleme

Sezar Şifresi : $c_i = E(p_i) = p_i + 3$

Açık Mesaj : Gizli Bilgi

Şifreli Mesaj : Ilcol Dloıl

Güvenli Şifreleme Yöntemleri

Açık Mesaj

3. Tümenin Doğu Trakya manevrasını 1 saat ertele

Şifreleme Algoritması

y=f(x)

Şifrelenmiş Mesaj

€ğ87.9!^f'+^%/d %++TGHEé^'^@V Rşou wrfhwrf RWR^^!"^^+ ..iü(()qedfhf sjsd

Anahtar

01001011

Güvenli Şifreleme Yöntemleri

- 64 bitlik bir anahtar
- 64 bitlik bir anahtarı tahmin yoluyla elde etme olasılığı $1/2^{63} \sim= 1/10^{19}$
- (2^{63} = 9.223.372.036.854.775.808)

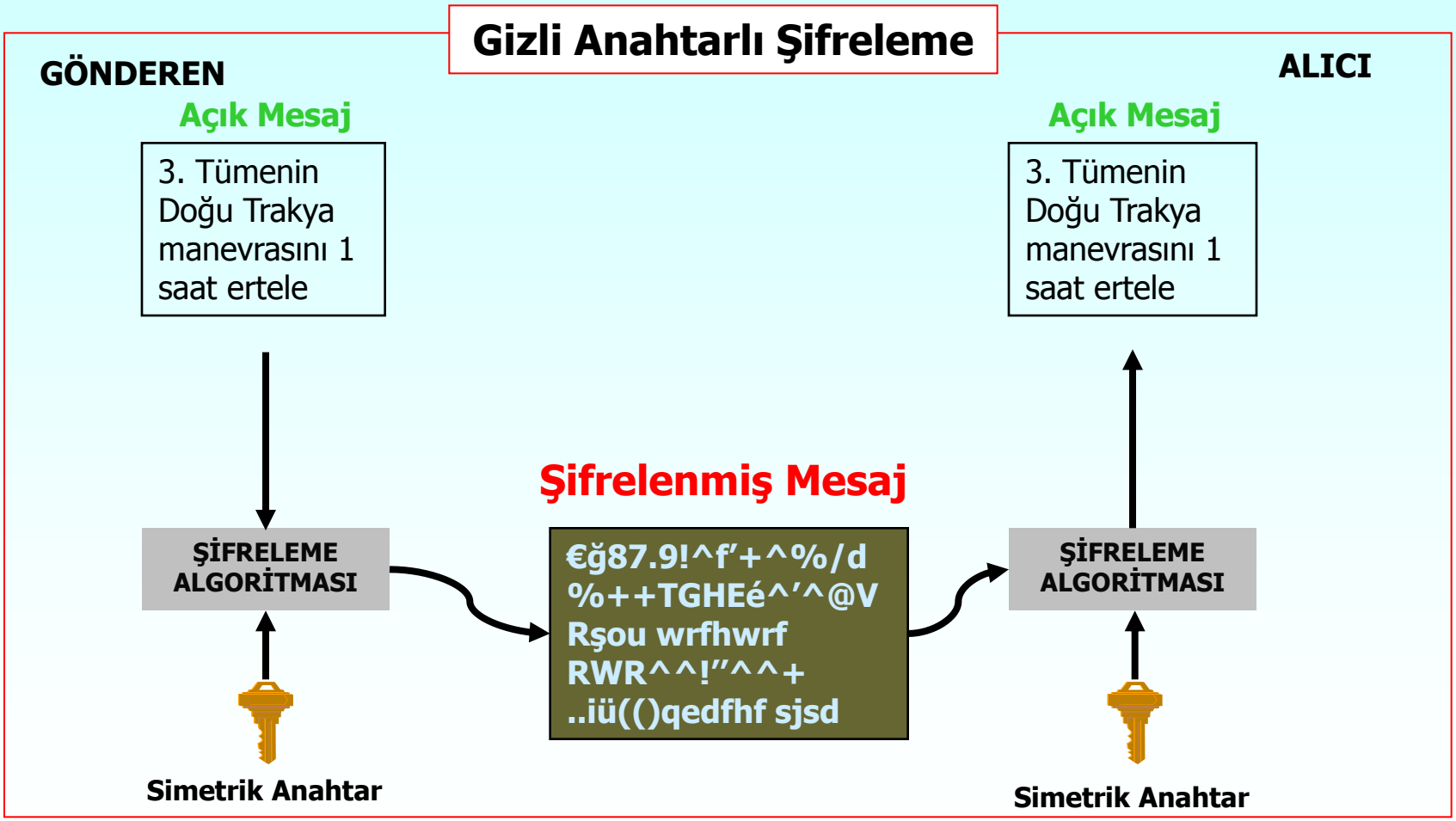
1100101010110001 0001101000000111
0110100010011110 1100111010011011

Güvenli Şifreleme Algoritmaları

İki temel kriptografik teknik vardır

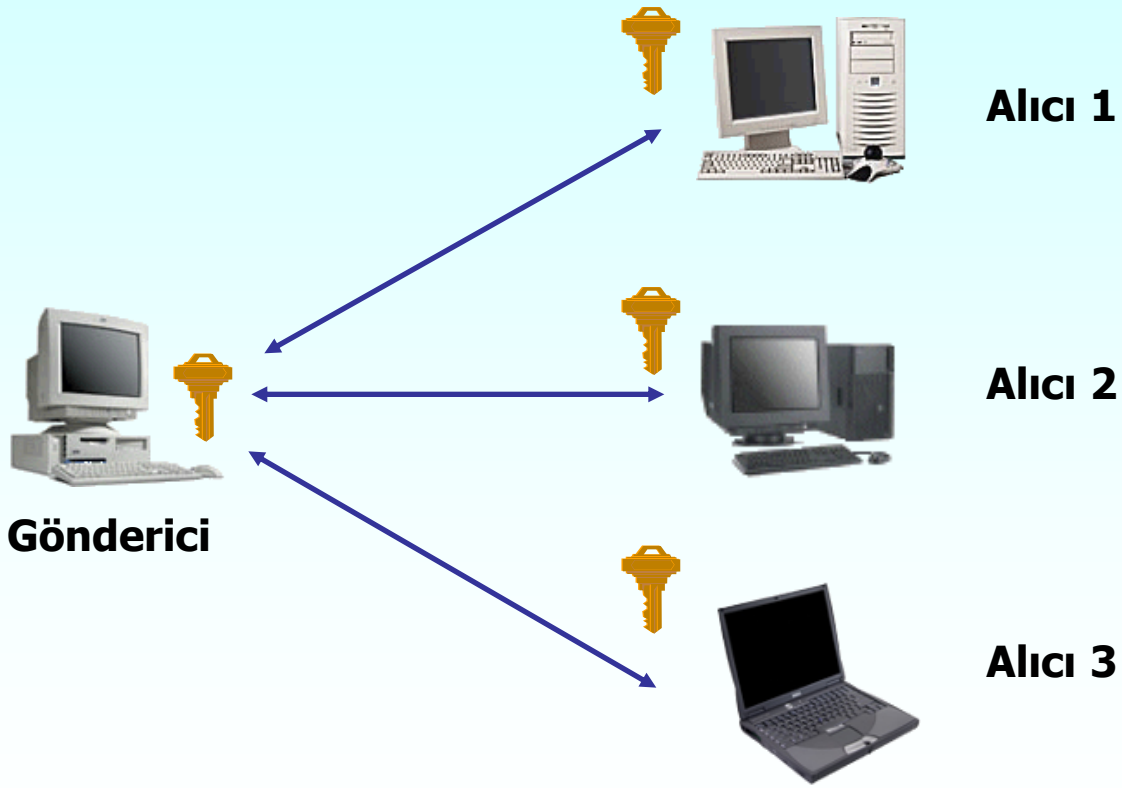
- Simetrik kriptografi
- Asimetrik kriptografi

Simetrik Kriptografi Kullanım Senaryosu



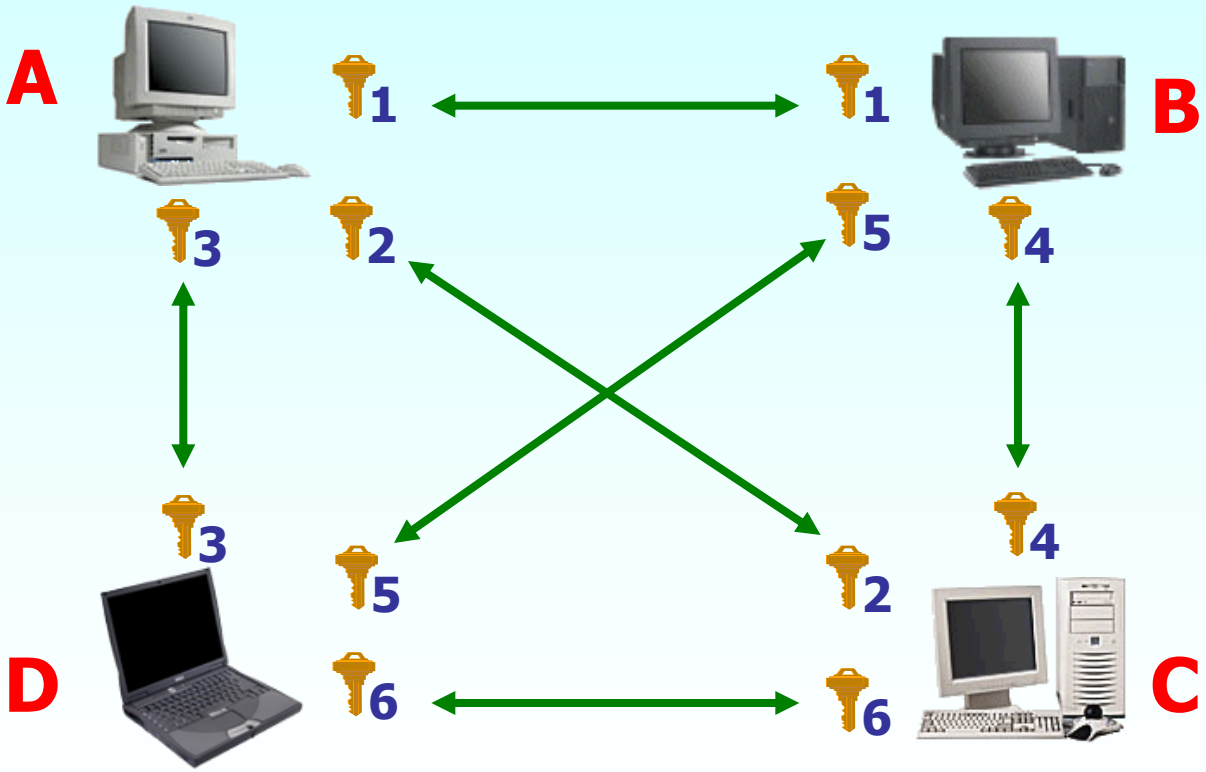
Simetrik Kriptografi Anahtar Yönetimi

Birden-Çoğa (One-to-Many)



Simetrik Kriptografi Anahtar Yönetimi

Çoktan-Çoğa (Many-to-Many)



Kullanıcı Sayısı	Anahtar Sayısı
3	3
4	6
10	45
100	4,950
1,000	499,500
10,000	49,995,000
	!!!?

Simetrik Kriptografi
Artılar Eksiler

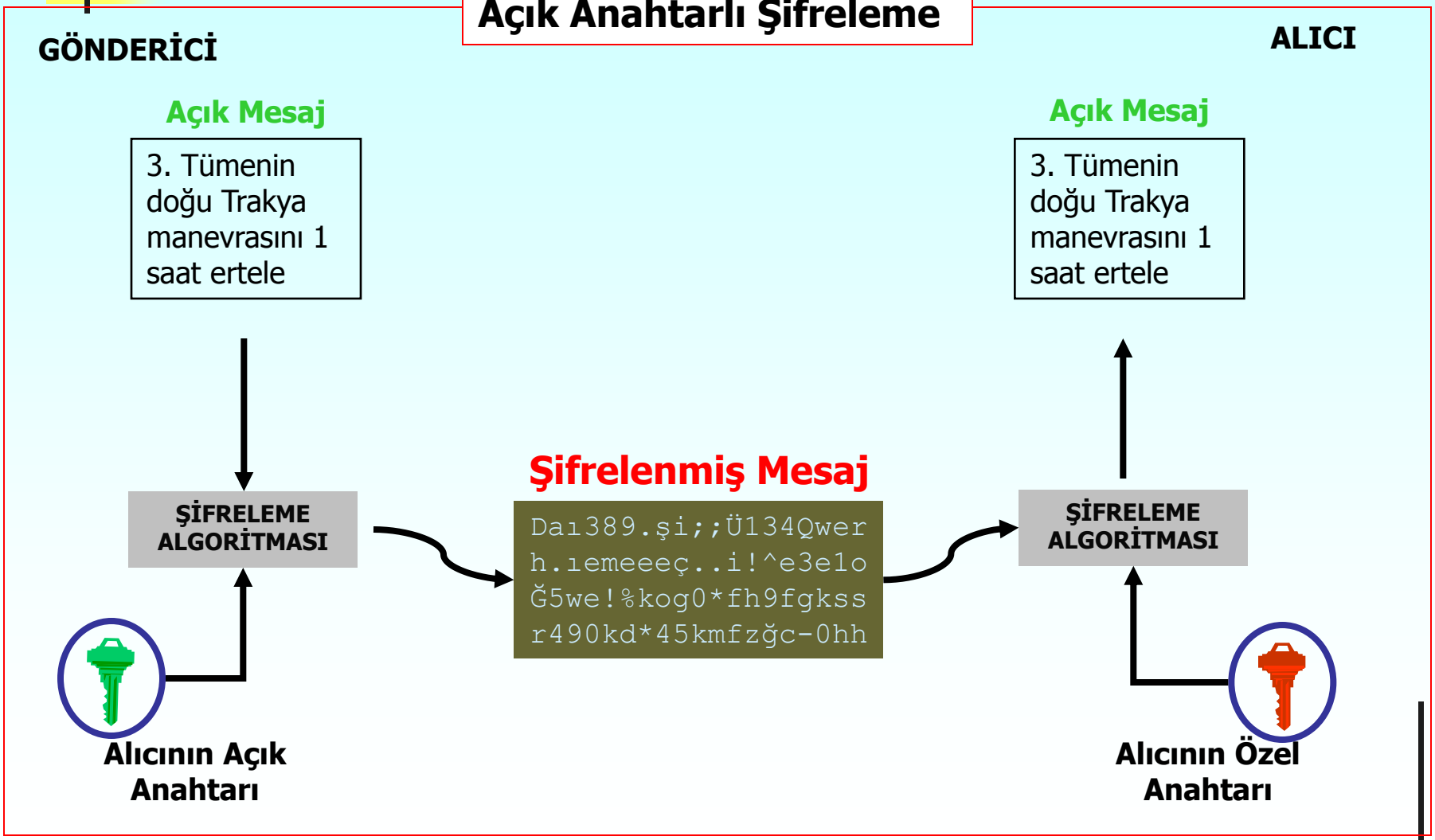
Artılar

- Algoritmalar hızlı
- "Gizlilik" güvenlik hizmetini yerine getirir

Eksiler

- Ölçeklenebilir değil
- Emniyetli anahtar dağıtımı ve yönetimi zor
- Bütünlük, Kimlik Doğrulama ve İnkar Edememe güvenlik hizmetlerini gerçeklemiyor

Asimetrik Kriptografi Kullanım Senaryosu



Asimetrik Kriptografi
Artılar Eksiler

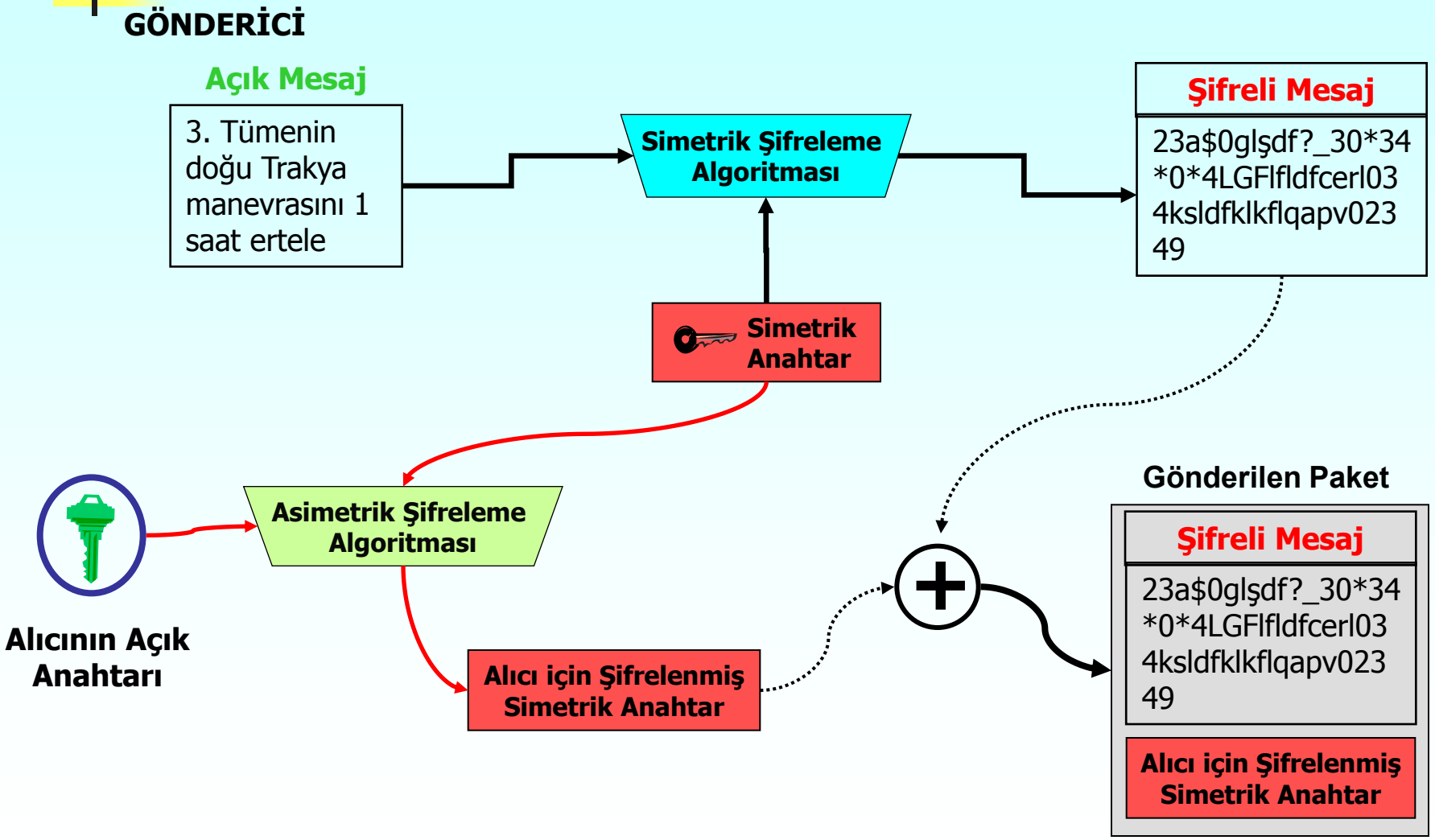
Artılar

- Anahtar yönetimi ölçeklenebilir
- Bütünlük, Kimlik Doğrulama ve İnkar Edememezlik güvenlik hizmetleri sağlanabilir

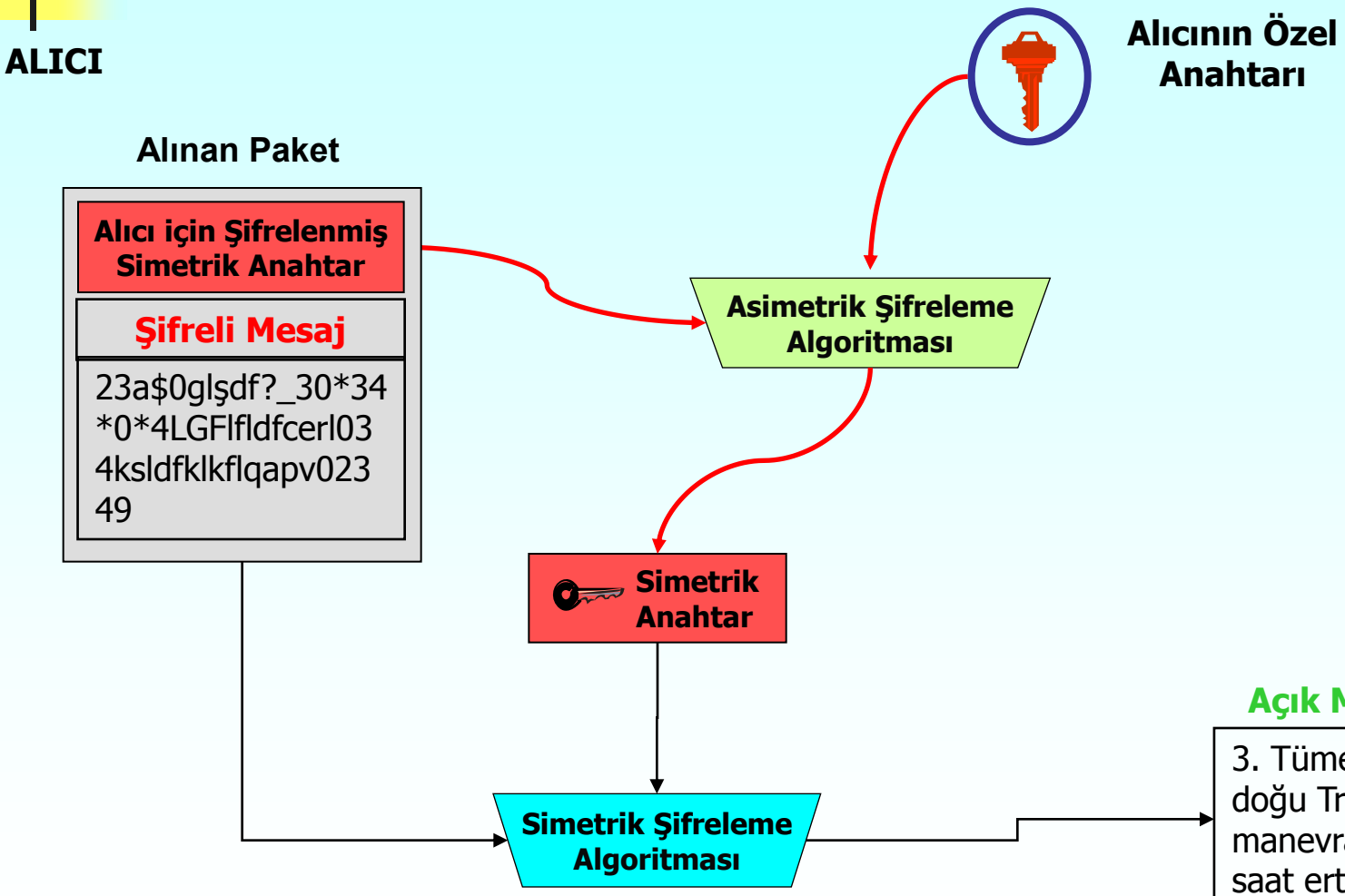
Eksiler

- Algoritmalar genel olarak yavaş (Simetrik algoritmalara göre 10-100 kat!)

Şifreli Mesaj Oluşturma



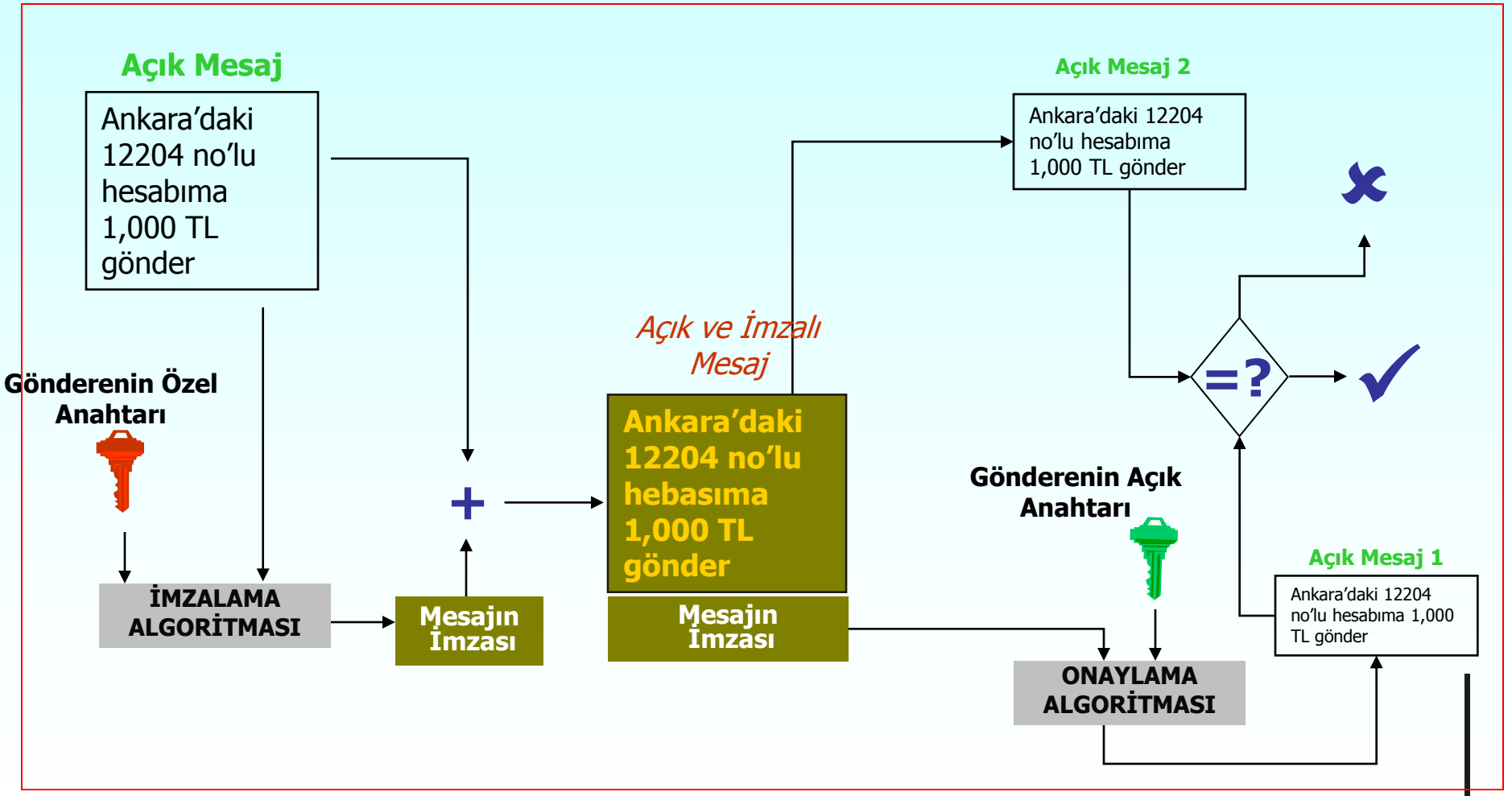
Şireli Mesaj Çözme



Elektronik İmza

- Mesajın sonuna eklenir
- Mesajı alanın, mesajın göndericisinin kimliğini doğrulamasını ve mesajın bütünlüğünü kontrolünü sağlar
- İnkar edememezlik hizmetini sağlar
- Asimetrik kriptografi kullanır

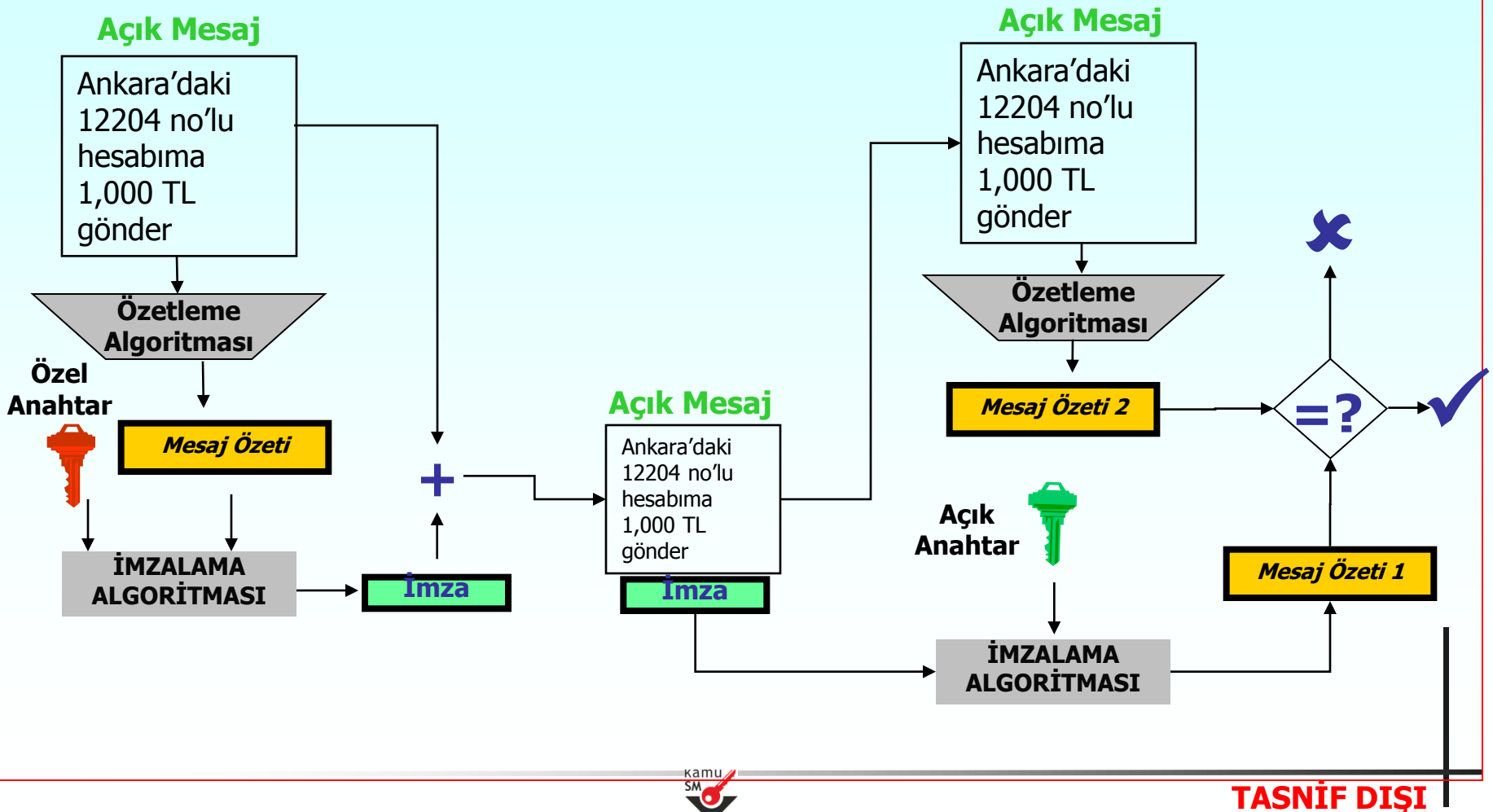
Elektronik İmza Nasıl Atılır ve Doğrulanır?



Özetleme Fonksiyonu

- Sabit çıkış uzunluğu (mesajdan çok kısa)
- Mesajdaki küçük değişiklikler bile özette büyük değişikliklere yol açabilir.
- Kriptografik tek yönlü fonksiyon
  - Bir mesajın özetini elde etmek kolay
  - Bir özetten asıl mesajı çıkarmak çok zor

Elektronik İmzada Özetleme Fonksiyonu Kullanım Senaryosu



Bora, Ayşe'ye İmzalı Bir Mesaj Nasıl Gönderir?

Açık Mesaj

Ankara'daki 12204 no'lu hesabıma 1,000 TL gönder

Özetleme Algoritması

Mesaj Özeti

İmzalama Algoritması

Özel Anahtar

Bora

Elektronik İmza

Gönderilen Paket

Açık Mesaj

Ankara'daki 12204 no'lu hesabıma 1,000 TL gönder

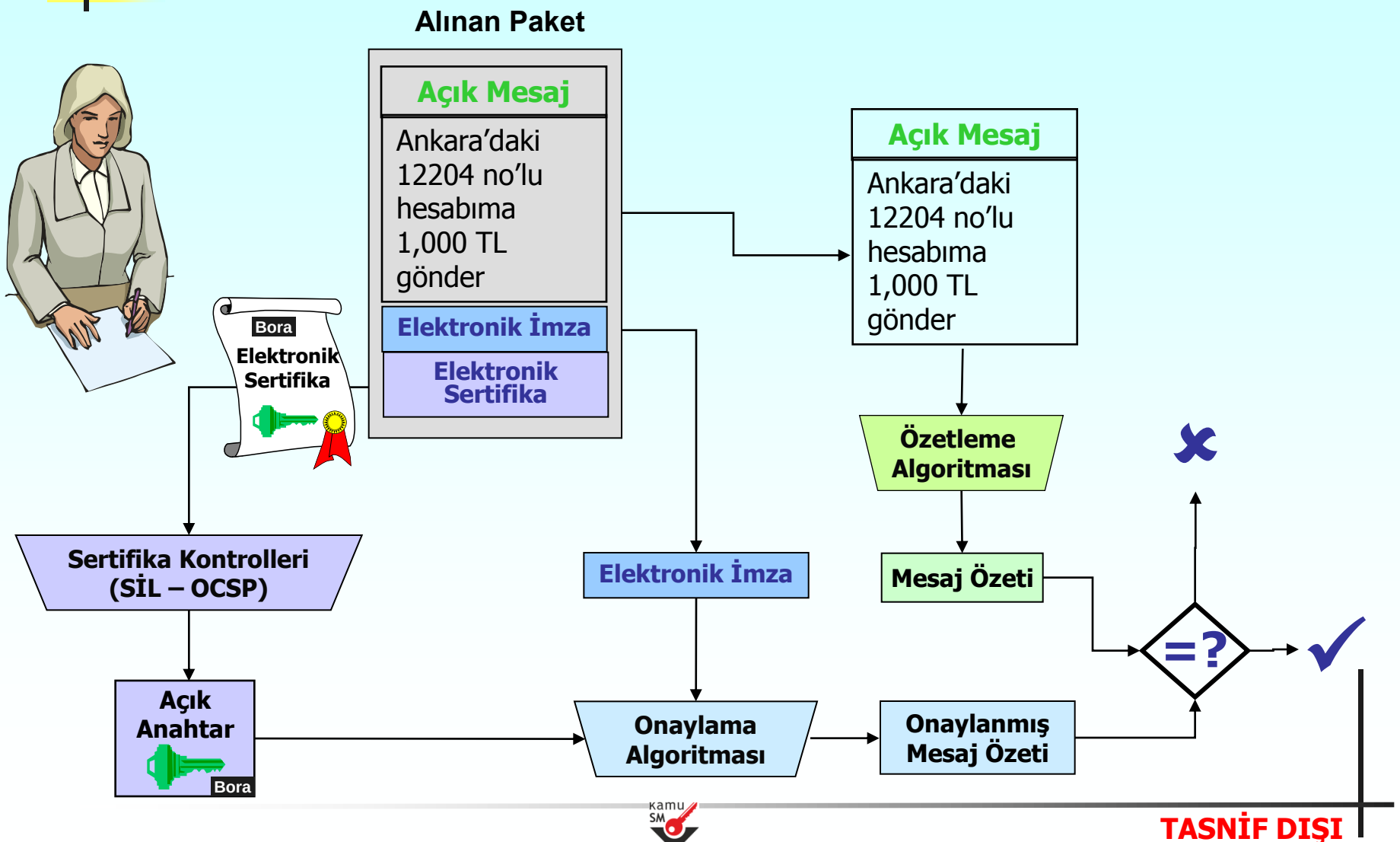
Elektronik İmza

Elektronik Sertifika

Bora

Güvenli Elektronik İmza Aracı

Ayşe, Bora'dan Gelen İmzalı Bir Mesajı Nasıl Doğrular?



Bora, Ayşe'ye Şifreli Bir Mesaj Nasıl Gönderir?

Açık Mesaj

Ankara'daki 12204 no'lu hesabıma 1,000 TL gönder

Simetrik Şifreleme Algoritması

Simetrik Anahtar

Şifreli Mesaj

23a$0glşdf?_30*34 *0*4LGFlfldfcerl03 4ksldfklkflqapv023 49

Açık Anahtar

Ayşe

Asimetrik Şifreleme Algoritması

Ayşe Elektronik Sertifika

Ayşe için Şifrelenmiş Simetrik Anahtar

Dizin Sistemi

Gönderilen Paket

Şifreli Mesaj

23a$0glşdf?_30*34 *0*4LGFlfldfcerl03 4ksldfklkflqapv023 49

Ayşe için Şifrelenmiş Simetrik Anahtar

Ayşe, Bora'dan Gelen Şifreli Bir Mesajı Nasıl Çözer?

Özel Anahtar
Ayşe

Ayşe

Asimetrik Şifre Çözme Algoritması

Alınan Paket

Ayşe için Şifrelenmiş Simetrik Anahtar

Şifreli Mesaj

23a$0glşdf?_30*34*0*4LGFlfldfcerl034ksldfklkflqapv02349

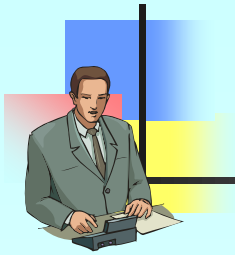
Simetrik Anahtar

Açık Mesaj

Ankara'daki 12204 no'lu hesabıma 1,000 TL gönder

Simetrik Şifre Çözme Algoritması

Bora, Ayşe'ye İmzalı ve Şifreli Bir Mesaj Nasıl Gönderir?



Açık Mesaj

Ankara'daki 12204 no'lu hesabıma 1,000 TL gönder

Bora

Özel Anahtar (Bora)

Özetleme Algoritması

Mesaj Özeti

İmzalama Algoritması

Açık Mesaj

Ankara'daki 12204 no'lu hesabıma 1,000 TL gönder

Elektronik İmza

Elektronik Sertifika

Elektronik İmza

Simetrik Şifreleme Algoritması

Şifreli Mesaj

Lk903kdksoıernvn
nxnasd903909kdfk
00_er0*0wejjksdf
^43re*0*erklslklk

Simetrik Anahtar

Dizin Sistemi

Ayşe Elektronik Sertifika

Açık Anahtar (Ayşe)

Asimetrik Şifreleme Algoritması

Ayşe için Şifrelenmiş Simetrik Anahtar

Gönderilen Paket

Ayşe için Şifrelenmiş Simetrik Anahtar

Şifreli Mesaj

Lk903kdksoıernvn
nxnasd903909kdfk
00_er0*0wejjksdf
^43re*0*erklslklk

Ayşe, Bora'dan Gelen Şifreli ve İmzalı Bir Mesajı Nasıl Çözer ve Doğrular

Alınan Paket

Ayşe için Şifrelenmiş Simetrik Anahtar

Şifreli Mesaj

Lk903kdksoıernvn
nxnasd903909kdfk
00_er0*0wejjksdf
^43re*0*erklslklk

Asimetrik Şifre Çözme Algoritması

Özel Anahtar — Ayşe

Ayşe

Simetrik Anahtar

Simetrik Şifre Çözme Algoritması

Mesaj Özeti

=?

Özetleme Algoritması

Açık Mesaj

Ankara'daki 12204 no'lu hesabıma 1,000 TL gönder

Elektronik İmza

Elektronik Sertifika

Onaylama Algoritması

Onaylanmış Mesaj Özeti

Bora Elektronik Sertifika

Sertifika Kontrolleri (SİL – OCSP)

Açık Anahtar — Bora

kamu SM

TASNİF DIŞI