

Bilgisayar Programcılığı Uzaktan Eğitim Programı

**e-BİLG 121 AĞ TEKNOLOJİLERİNİN
TEMELLERİ**

Öğr. Gör. Bekir Güler

E-mail: bguler@fatih.edu.tr

12. Hafta: Ağ güvenliği I

8.1 Ağ güvenliği nedir?

8.2 Şifreleme ilkeleri

8.3 Mesajın bütünlüğü

8.4 Güvenli e-posta

8.1 Ağ güvenliği nedir?

Gizlilik (Confidentiality): sadece gönderen ve alıcı mesajın içeriğini anlamalıdır

- Gönderen mesajı şifreler
- Alıcı şifrelenmiş mesajı çözer ve mesajı alır

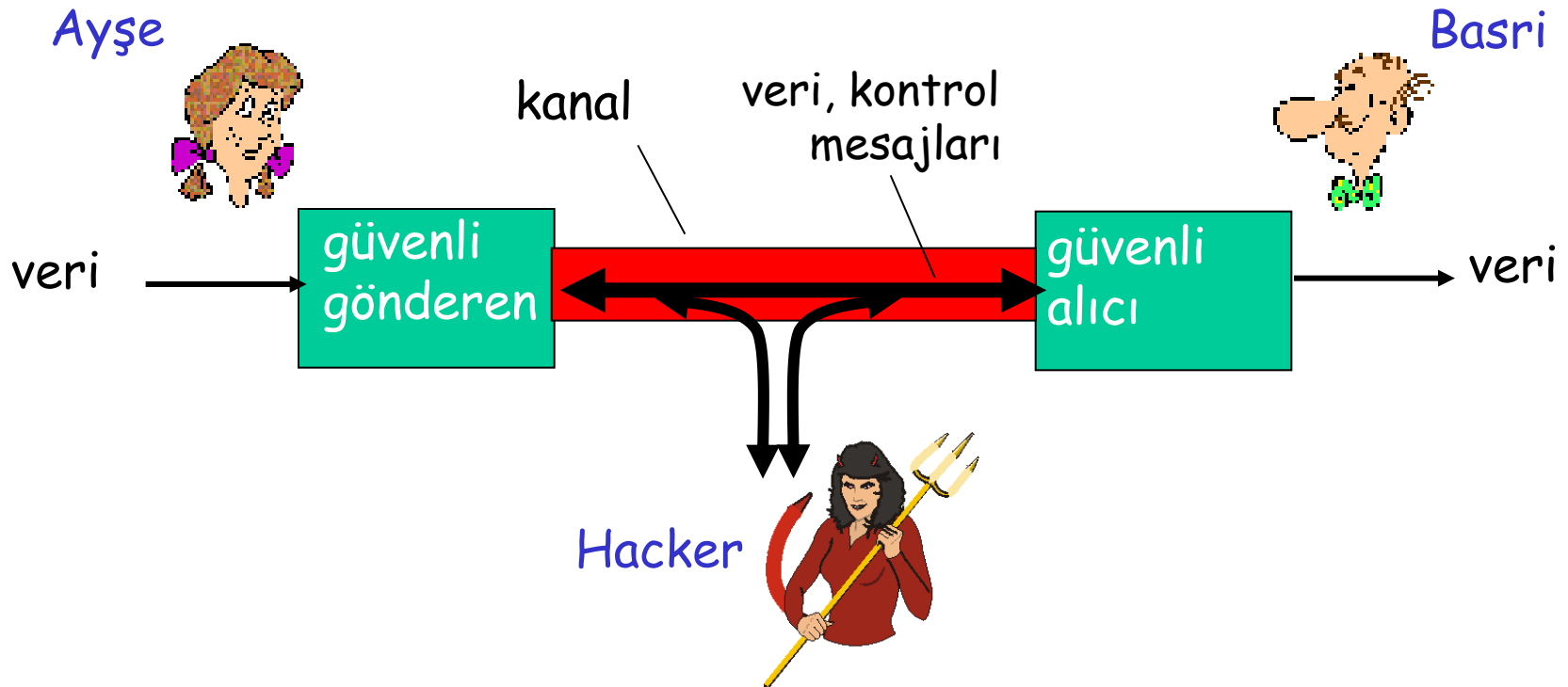
Kimlik doğrulaması (Authentication): Gönderen ve alıcı birbirlerinin kimliklerini doğrulamak isterler

Mesajın bütünlüğü: Gönderen ve alan mesajın değişmediğinden emin olmak ister

Erişim ve kullanılabilirlik: Ağdaki hizmetlerin erişilebilir ve kullanılabilir olması gerekir

Ayşe, Basri ve Hacker

- Ali ve Ayşe güvenli bir şekilde iletişim kurmak istiyorlar
- Hacker mesajları silebilir, ekleyebilir ve değiştirebilir



Ayşe ve Basri kim olabilir?

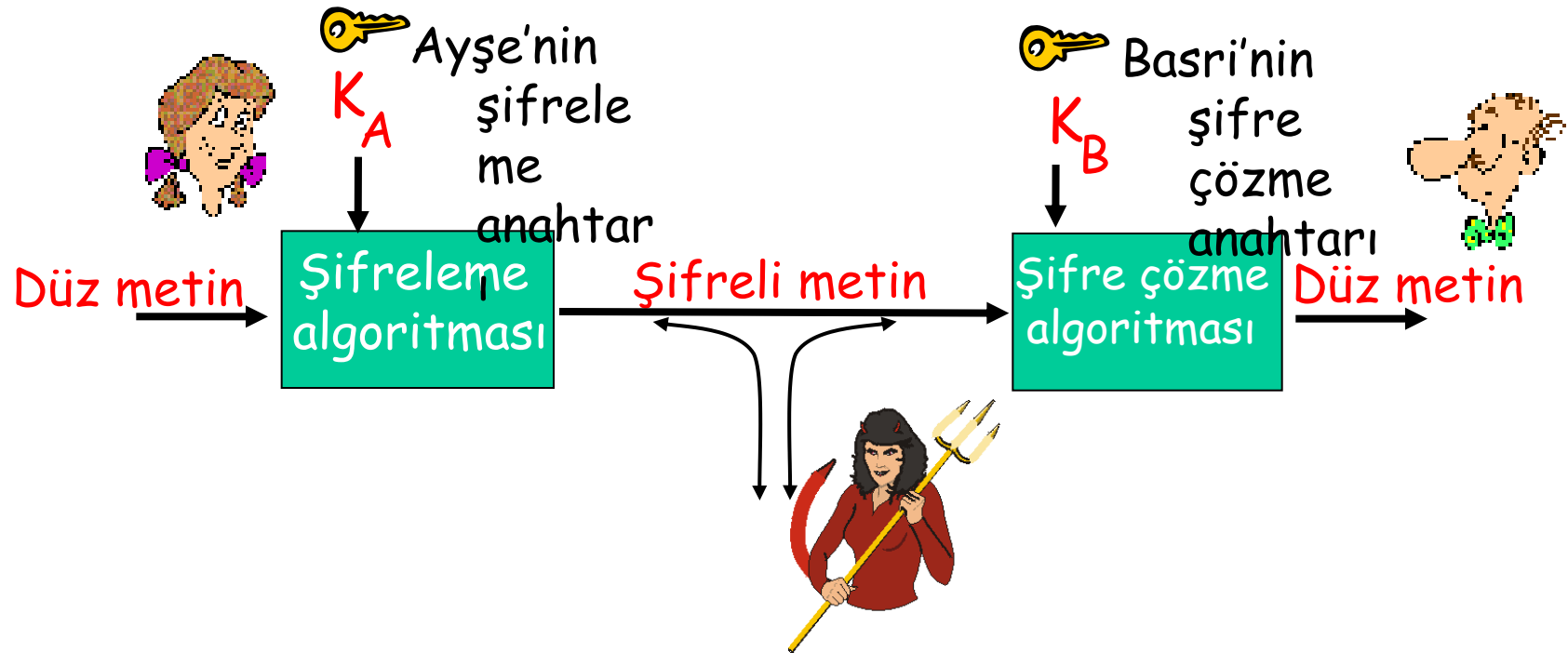
- ❑ İnternet üzerinden alışverişte web tarayıcı/sunucu olabilir
- ❑ İnternet üzerinden yapılan bir bankacılık işlemi olabilir
- ❑ DNS sunucular

S: Hacker ne yapabilir?

C: Aşağıdaki işlemleri yapabilir

- Mesajlara dinleyip kesebilir
- Bağlantıya mesaj ekleyebilir
- Mesajın kaynak adresini değiştirerek farklı bir kimliğe bürünebilir
- Bir hizmetin başkaları tarafından kullanılmasını engelleyebilir (örneğin, kaynaklara aşırı yüklenerek)

8.2 Şifreleme ilkeleri





m : düz metin mesajı

$K_A(m)$: Düz metin, K_A anahtarı ile şifrelendi

$m = K_B(K_A(m))$: Şifreli metin K_B anahtarı ile çözüldü

Basit şifreleme düzeni

Yerin koyma: Bir karakter yerine başka bir karakter koyma

Düz metin:	abcdefghijklmnopqrstuvwxyz
	 
Şifreli metin:	mnbvcxzasdfghjklpoiuytrewq

Örnek:

Düz metin:	merhaba
Şifreli metin:	hcoamnm

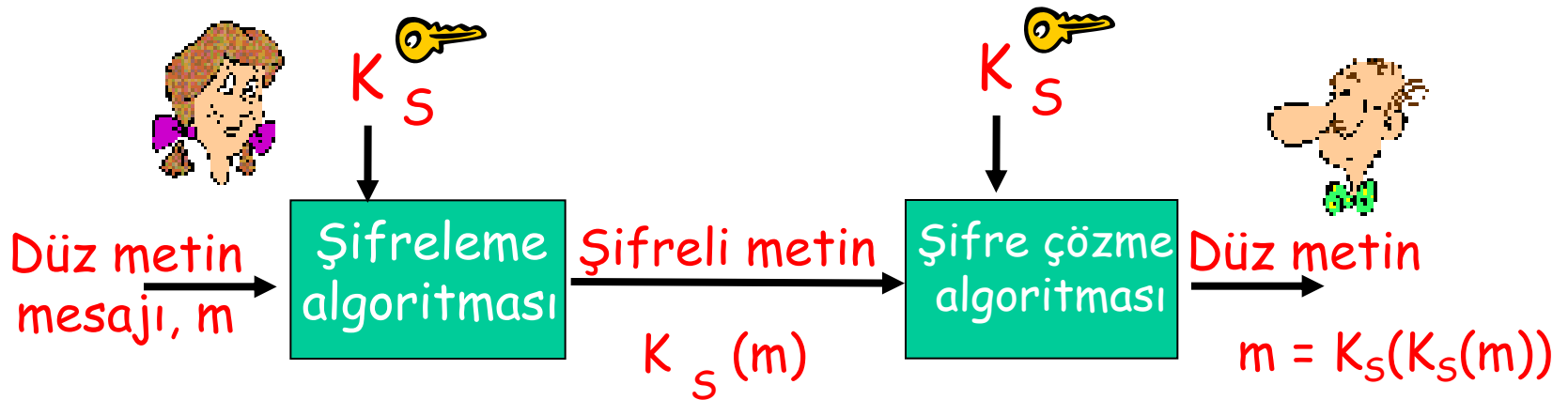
Şifreleme düzenini kırma

- ❑ Şifreli metin elde varsa: Hacker, analiz edebileceği şifreli metne sahiptir
- ❑ 2 yaklaşım:
 - Şifreli metinden düz metin elde edilene kadar tüm anahtarlar ile arama yapılır
 - İstatistiksel analiz
- ❑ Hacker bazı şifreli metinlere karşılık gelen düz metinleri biliyorsa

Kriptografi (Cryptography) türleri

1. Kripto anahtarları kullanır:
 - Kullanılan algoritma herkes tarafından bilinir
 - Sadece anahtarlar gizlidir
2. Ortak (public) anahtar şifrelemesi
 - İki anahtar kullanılır
3. Simetrik anahtar şifrelemesi
 - Tek anahtar kullanılır
4. Hash (Mesajın özeti) fonksiyonları
 - Anahtar kullanılmaz
 - Gizli bir şey yok

3. Simetrik anahtar şifrelemesi



Simetrik anahtar şifrelemesi: Basri ve Ayşe aynı simetrik anahtarı: K_S paylaşıyorlar

S: Basri ve Ayşe anahtar değerinde nasıl anlaşırlar?

Simetrik şifre türleri

❑ Bit akışını (Stream) şifreleme

- Aynı anda tek bit şifreler

❑ Blok şifreleme

- Düz metin mesajı eşit büyüklükte bloklara bölünür
- Her blok bir bütün olarak şifrelenir

Bit akışı şifreleme



- Keystream'in her bir biti, düz metnin bir biti ile birleştirilerek şifreli metin elde edilir

RC4 bit akışı şifrelemesi

- ❑ RC4, yaygın kullanılan bit akışı şifrelemesidir
 - Anahtar 1 ile 256 bayt arası olabilir
 - WEP (802.11)'de kullanılır
 - SSL'de kullanılabilir

Blok şifreleme

- ❑ Mesaj k bitlik bloklara halinde şifrelenir (örneğin, 64 bitlik blok).
- ❑ k-bit blok düz metin ve k-bit blok şifreli metin bire bir eşleştirilir

Örnek: (k=3)

<u>giriş</u>	<u>çıkış</u>
000	110
001	111
010	101
011	100

<u>giriş</u>	<u>çıkış</u>
100	011
101	010
110	000
111	001

010110001111 şifreli metni nedir?

Simetrik anahtar şifreleme: DES

Veri şifreleme standardı

(Data Encryption Standard- DES)

- ❑ US şifreleme standardı (1993)
- ❑ 56-bit simetrik anahtar, 64-bit düz metin girişi
- ❑ Blok şifreleme
- ❑ DES ne kadar güvenli?
 - DES: 56-bit anahtar ile şifrelenen bir metin 1 günden az bir zamanda çözülüyor
 - Bilinen iyi bir analitik bir saldırı yok
- ❑ DES'i daha güvenli yapmak için:
 - 3DES: 3 farklı anahtar ile 3 kez şifrelenir

Gelişmiş şifreleme standardı (Advanced Encryption Standard- AES)

- ❑ DES'in yerine gelen yeni standart (2001)
- ❑ Verileri 128 bitlik bloklar halinde işler
- ❑ 128, 192 veya 256 bitlik anahtarlar kullanır
- ❑ Bütün ihtimaller denenirse şifreyi kırmak 149 trilyon yıl sürer

2. Ortak anahtar şifrelemesi

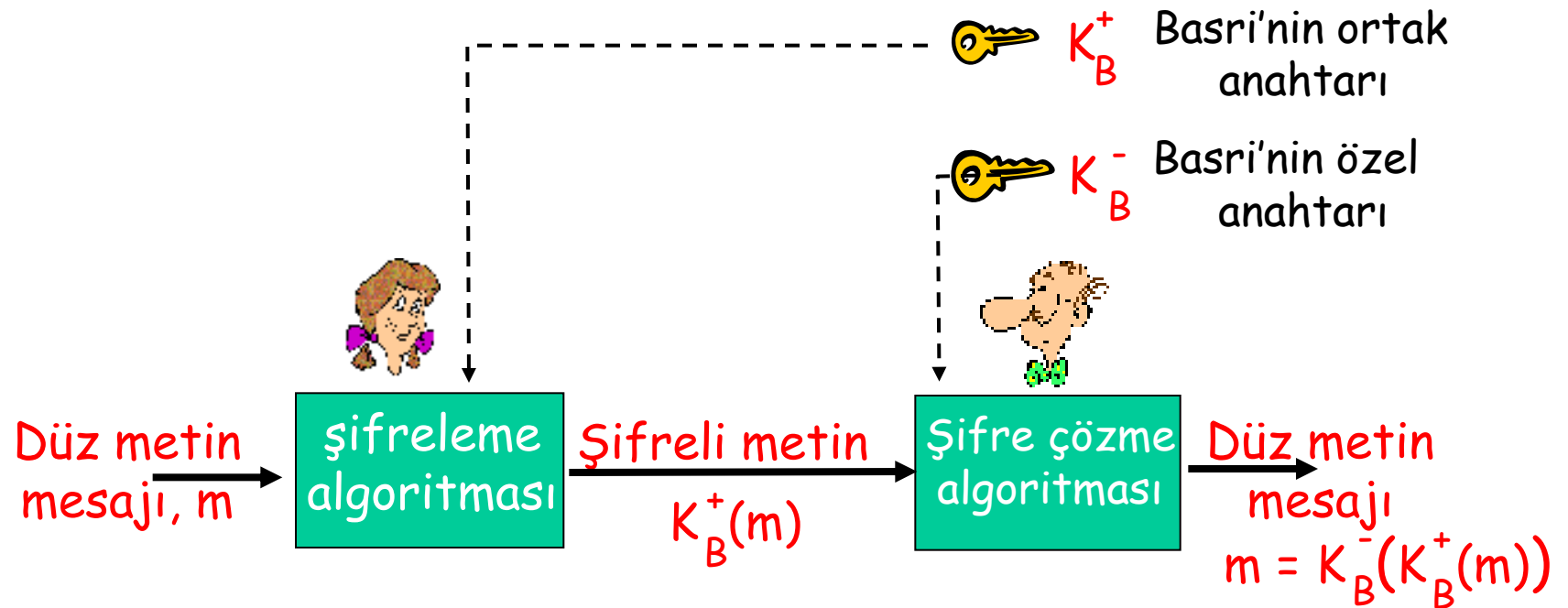
Simetrik anahtar şifrelemesi

- ❑ Gönderen ve alıcının paylaşılan gizli anahtarı bilmesi gerekir
- ❑ S: Gönderen ve alıcı ilk anahtarda nasıl anlaşır?

Ortak anahtar şifrelemesi

- ❑ Farklı bir yaklaşım
- ❑ Gönderen ve alıcı gizli bir anahtarı paylaşmaz
- ❑ *Ortak (public)* şifreleme anahtarını herkes bilir
- ❑ *Özel (private)* şifre çözme anahtarını sadece alıcı bilir

Ortak anahtar şifrelemesi



Ortak anahtar şifreleme algoritması

① $K_B^+(\cdot)$ ve $K_B^-(\cdot)$ anahtarlarına ihtiyaç var

$$K_B^-(K_B^+(m)) = m$$

② Ortak anahtar K_B^+ ile özel anahtar K_B^- hesaplamak mümkün değildir

RSA: Rivest, Shamir, Adelson algorithm

RSA

- ❑ Bir mesaj, bir bit dizisi biçimindedir
- ❑ Bir bit dizisi benzersiz bir tamsayı ile temsil edilebilir.
- ❑ Bir mesajı şifrelemek bir sayıyı şifrelemeye eşittir

Örnek

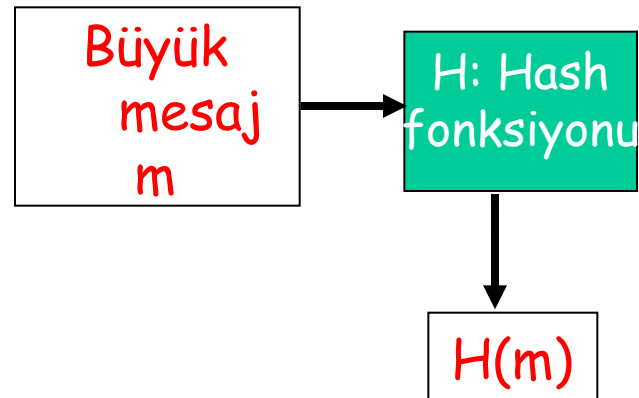
- ❑ $M = 10010001$. M mesajı onluk sistemde 145 sayısı ile temsil edilir
- ❑ M mesajını şifrelerken ona karşılık gelen 145 sayısı şifrelenir ve şifreli metin elde edilir

8.3 Mesajın bütünlüğü

- ❑ İletimde mesajların orijinal olduğu doğrulanmalıdır
 - Mesaj içeriğinin değişmediğinden emin olmak gerekir
 - Mesajın gönderenin değişmediğinden emin olmak gerekir
 - Mesaj başkası tarafından değiştirilip tekrar gönderilmemelidir
 - Mesaj sırası korunmalıdır

4. Hash (Mesajın özeti) fonksiyonu

$H()$ fonksiyonu rasgele uzunlukta bir mesajı giriş olarak alır ve çıkış olarak sabit uzunlukta bir string (karakter dizisi) verir. Bu string'e mesaj imzası da denir



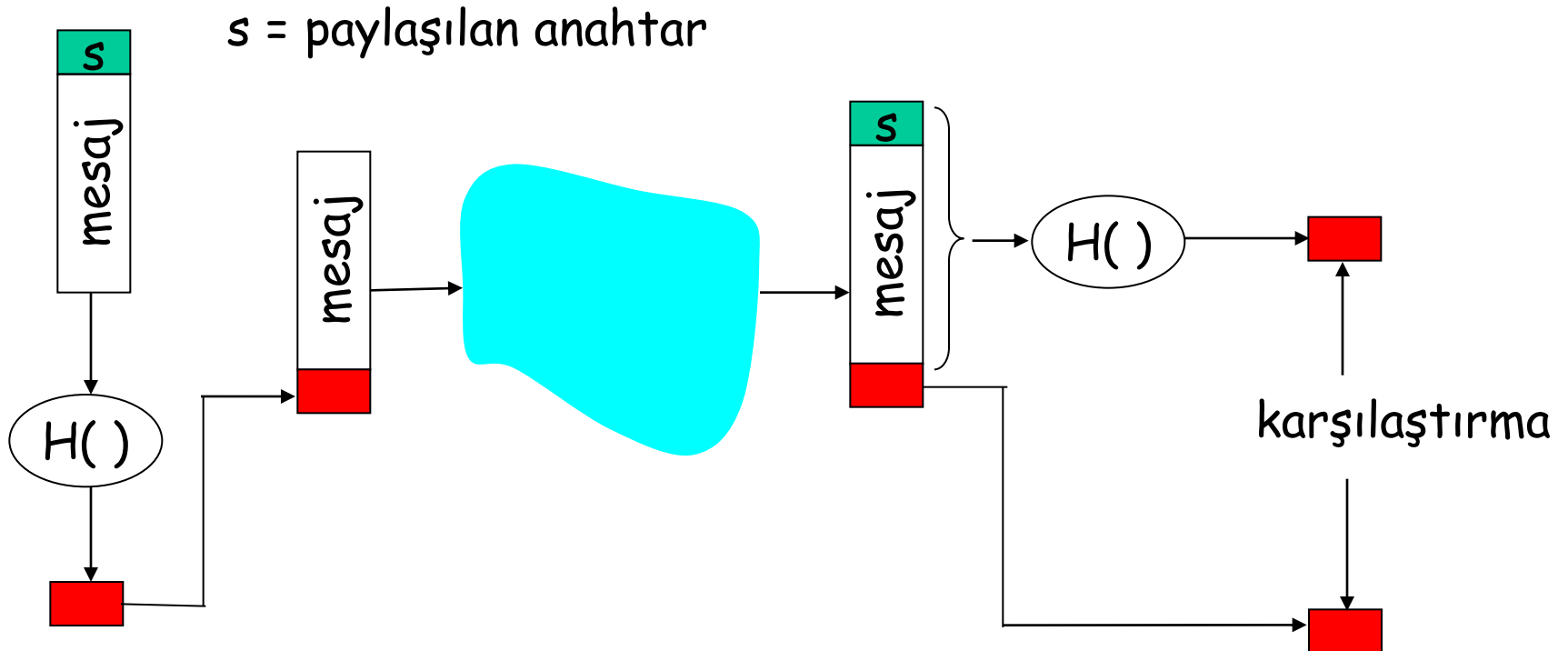
Internet checksum mesaj özeti

Internet checksum'da 16 bitlik bir mesaj özeti üretilir

Hash fonksiyon algoritmaları

- MD5 hash fonksiyonu yaygın kullanılır
 - 128-bit mesaj özeti hesaplar
- SHA-1 başka bir fonksiyondur
 - US standardı
 - 160-bit mesaj özeti hesaplar

Mesajın doğrulanması



- ❑ Gönderen mesaj özetini mesaja ekler
- ❑ Mesaj alındıktan sonra tekrar mesaj özeti hesaplanır ve mesaj ile gelen değer ile karşılaştırılır
- ❑ Değerler aynı ise mesaj değişmemiş demektir
- ❑ Şifreleme yok!

Hash Message Authentication Code-HMAC

Yaygın kullanılan mesaj doğrulama standardı

1. Gizli anahtar ve mesajı birleştirir
2. Sonra özeti alınır
3. Özeti önüne gizli anahtar tekrar eklenir
4. Tekrar özeti alınır

Dijital imzalar

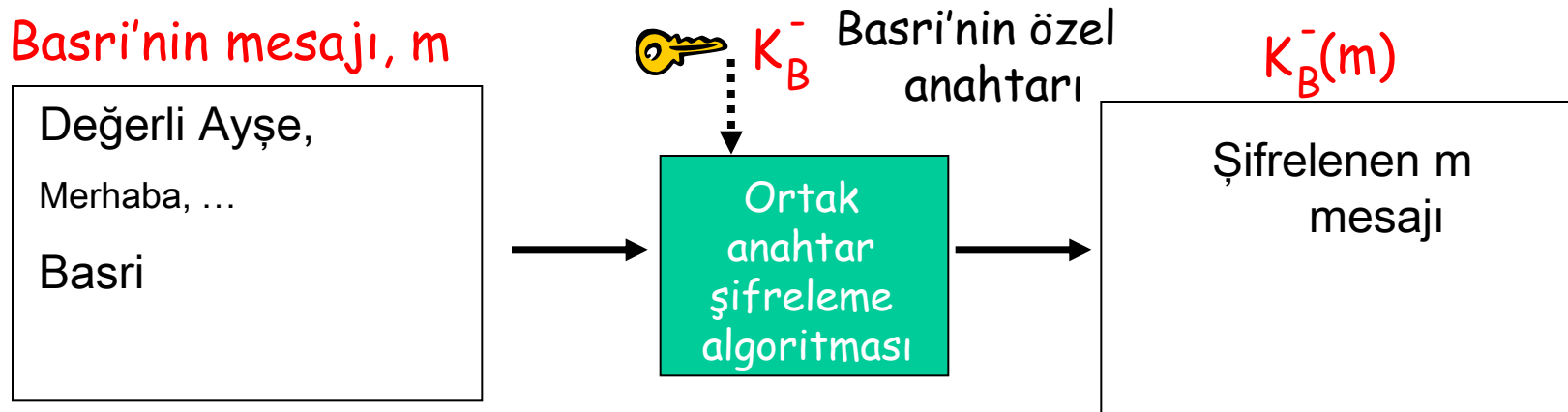
Şifreleme tekniği elle atılmış imzalara benzer

- Gönderen belgeyi dijital olarak imzalar, belgeyi oluşturan ve sahibi olduğunu belirtmiş olur
- Mesaj bütünlüğünün doğrulanmasına benzer, fakat burada ortak anahtar şifrelemesi kullanılır

Dijital imzalar

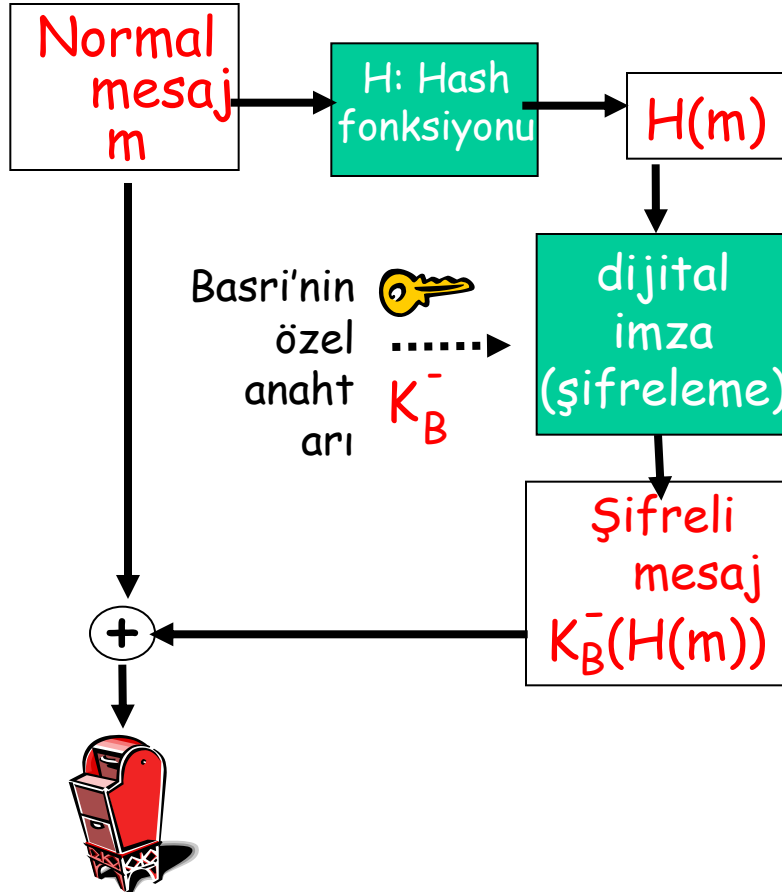
M mesajı için dijital imza:

- Basri m mesajını özel K_B^- anahtarı ile şifreler, imzalı $K_B^-(m)$ mesajını oluşturur

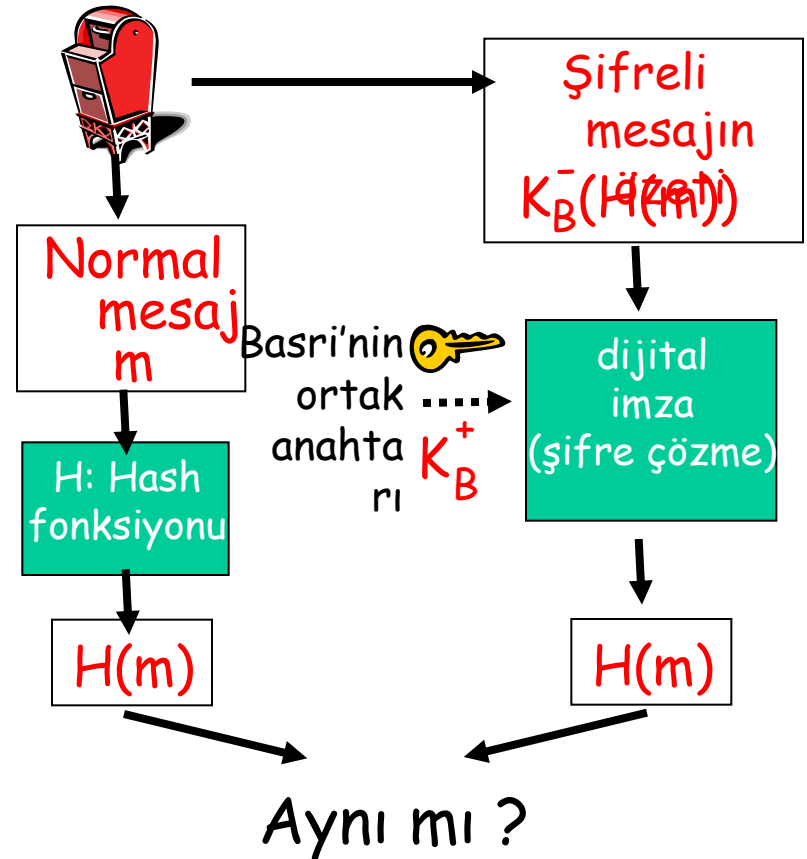


Dijital imza = imzalı mesaj özeti

Basri dijital imzalı mesajı gönderir

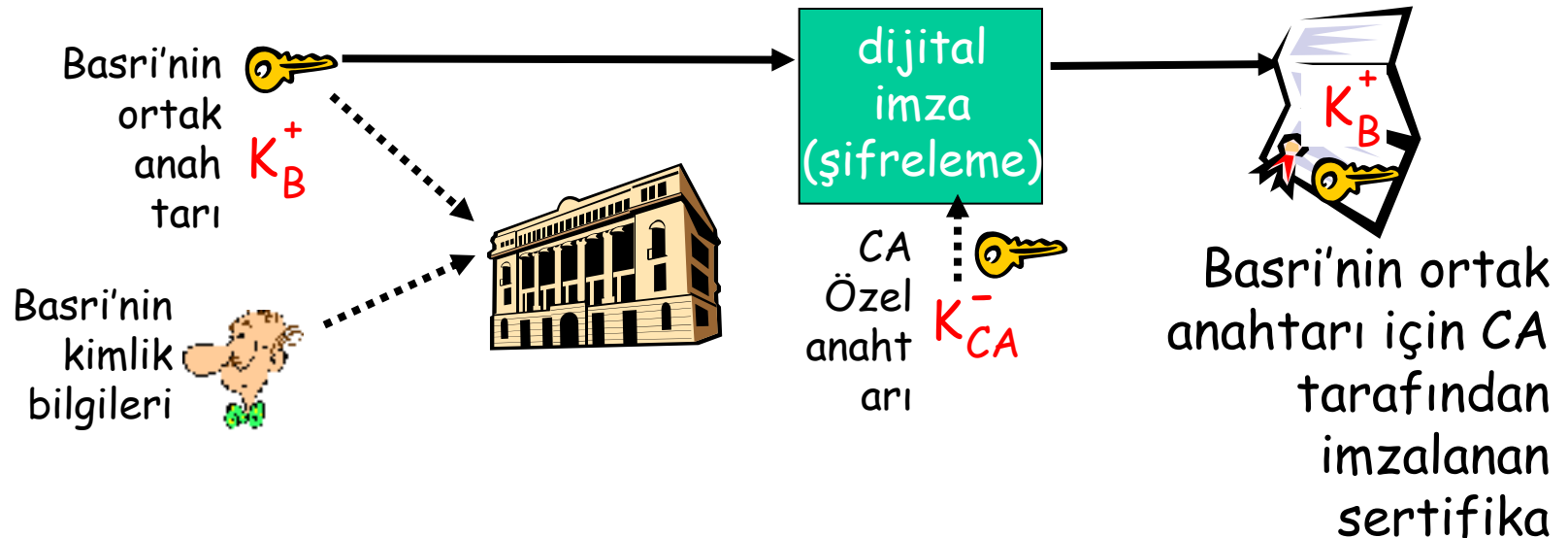


Ayşe, imzanın ve mesajın bütünlüğünü doğrular



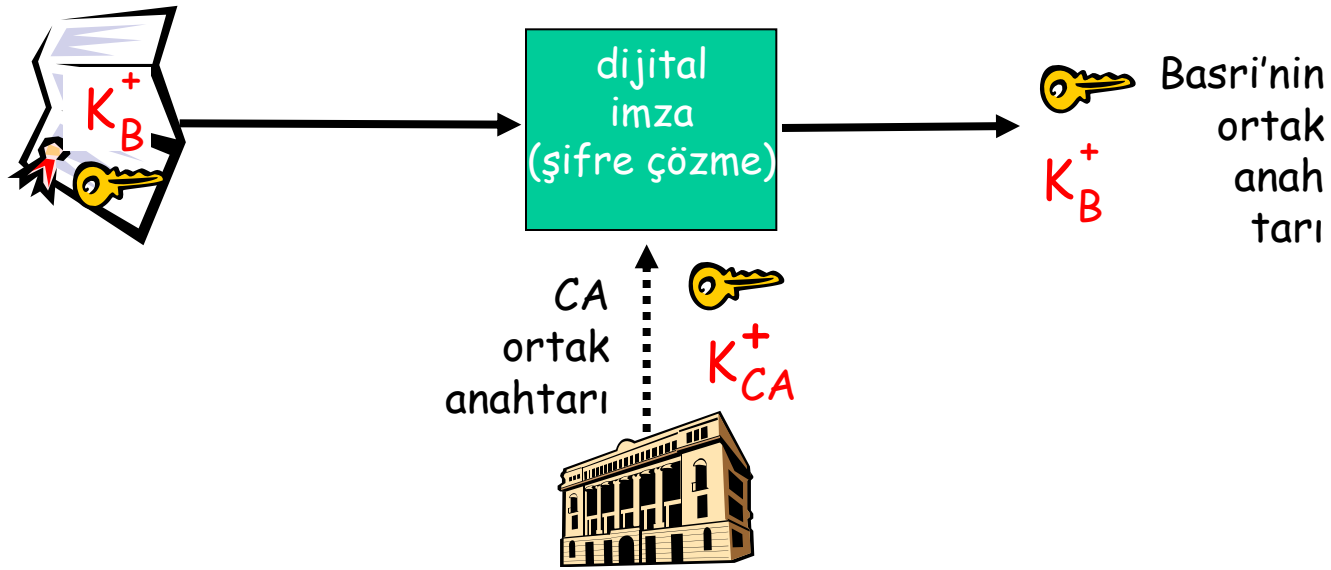
Sertifika yetkilileri (Certification Authorities-CA)

- Ortak anahtarı belli bir varlığa bağlar, E.
- E (kişi, router) ortak anahtarını CA'e kayıt eder
 - E varlığı kendini CA'e tanıtır
 - CA, E varlığını ortak anahtarına bağlayan sertifika oluşturur
 - Sertifika, E varlığının ortak anahtarı yerine geçer



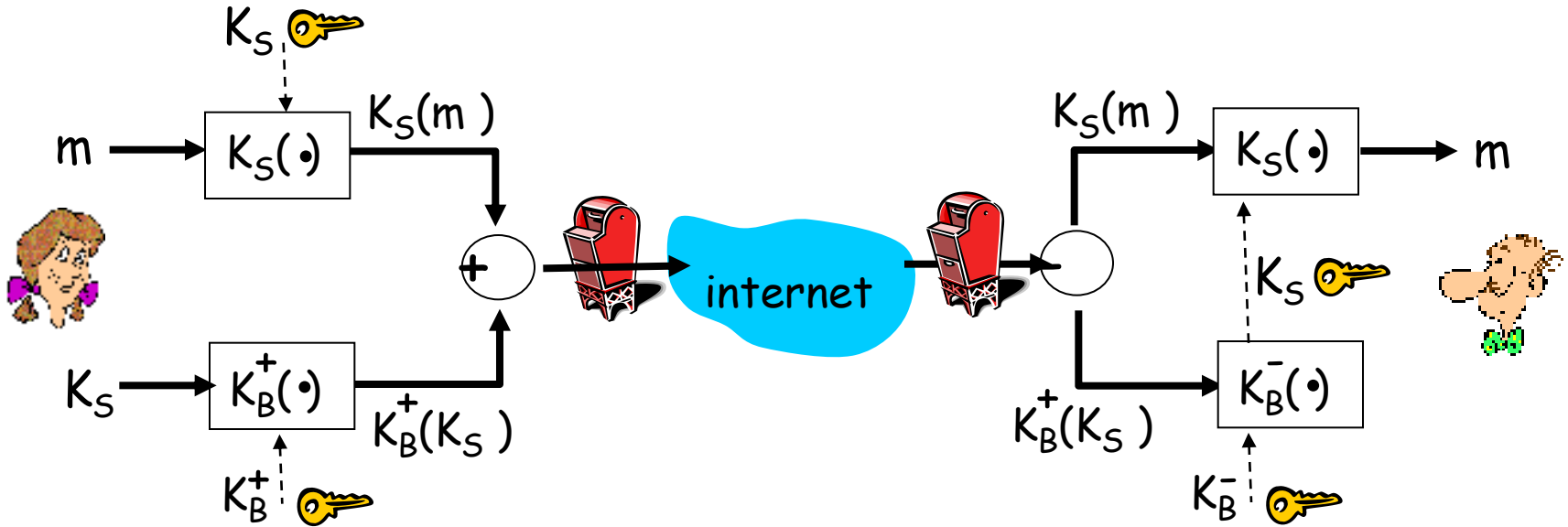
Sertifika yetkilileri

- Ayşe, Basri'nin ortak anahtarını istediğinde:
 - Basri'nin sertifikasını elde eder
 - CA ortak anahtarını Basri'nin sertifikasına uygulayarak Basri'nin ortak anahtarını elde eder



8.4 Güvenli e-posta

- Ayşe, gizli m e-postasını Basri'ye göndermek istiyor

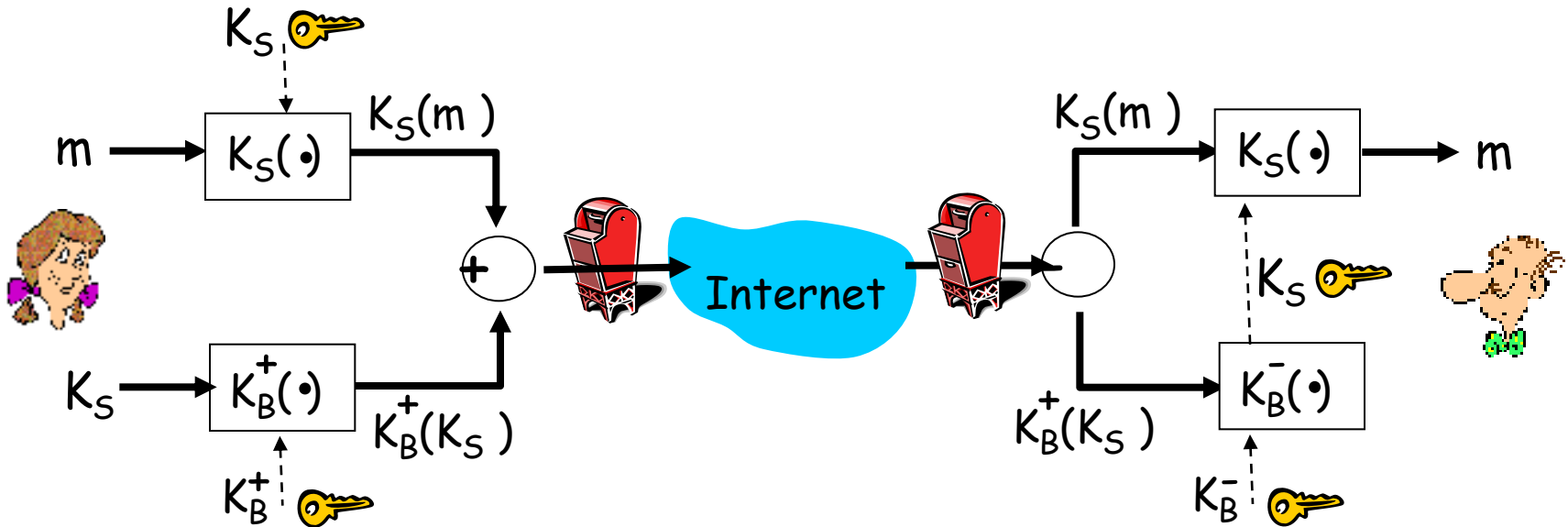


Ayşe:

- Rasgele simetrik özel anahtar üretir, K_S .
- Mesajı K_S ile şifreler
- Ayrıca K_S 'yi Basri'nin ortak anahtarı ile şifreler
- Hem $K_S(m)$ hem de $K_B(K_S)$ 'yi Basri'ye gönderir

Güvenli e-posta

- Ayşe, gizli m e-postasını Basri'ye göndermek istiyor



Basri:

- Özel anahtarı ile K_S şifresini çözer ve elde eder
- K_S 'yi kullanarak $K_S(m)$ 'yi çözer, m mesajını elde eder