

# Kriptografik Protokoller: Uygulamalar ve Güvenlik

Dr. Hamdi Murat Yıldırım

Bilgisayar Teknolojisi ve Bilişim Sistemleri Bölümü  
Bilkent Üniversitesi

<http://hmurat.bilkent.edu.tr>

hmurat@bilkent.edu.tr

@h\_muratyildirim

Uluslararası Adli Bilişim Sempozyum 2014  
31 Mayıs – 01 Haziran

# Protokol Tanımı (Wikipedia)

- (haberleşme) protokolu bilgisayar içinde ve bilgisayarlar arasında veri değişimi için dijital kurallar sistemidir (wikipedia)
- Kurallar, algoritmalar ve veri yapıları ile ifade edilebilir.
- Bir protokol mutlaka sözdizilimi (syntax), anlamsal ve haberleşmenin eş zamanlığını; belirtilen davranışları, nasıl gerçekleştireceğinden bağımsız tanımlamalıdır.

# Protokol Tanımı

## **Bazı Temel Protokol Gereksinimleri (Wikipedia)**

- Takas edilen verinin formatı
- Alıcı ve gönderinin adresi
- Alındı mesajı
- Akış kontrolü

## **Biçimsel Gösterimleri (Wikipedia)**

- Abstract Syntax Notation One (an ISO standart) veya
- Augmented Backus-Naur form (an IETF standart).
- Biçimsel olarak protokol etkileşimlerinin gösterimi

# Kriptografik Protokoller

- Bir güvenlik (Kriptografik protokol), güvenlik ile ilgili bir işlemi uygulayan, bir dizi kriptografik algoritmaları kullanan bir soyut protokoldür.
  - Böyle bir protokol, bu algoritmaların nasıl kullanılacağını tanımlar.
  - İzleyenlerin bir veya daha fazlasını Kriptografik protokol içerebilir:
    - Gizli anahtar paylaşımı
    - Varlığının (entity) kimlik denetimi
    - Simetrik şifreleme
    - İnkâr edilemezlik metodları
- .... **(Wikipedia)**

# Kriptografik Protokoller, Örnek

Transport Layer Security (TLS), güvenli web (HTTP) bağlantıları kurmak için kullanılan bir kriptografik protokol

- X.509 sertifikaları kullanan (Açık anahtar Altyapısı -PKI- tabanlı)
- Simetrik anahtar oluşturma ve paylaşma - Diffie-Hellman anahtar değişimi protokolü kullanımı-, aşamaları -asimetrik şifreleme kullanılarak.

.... **(Wikipedia)**

## **Diğer Protokol örnekleri:**

**\* Anahtar Değişim Protokolü -  
Internet Key Exchange (IKE or IKEv2) -**

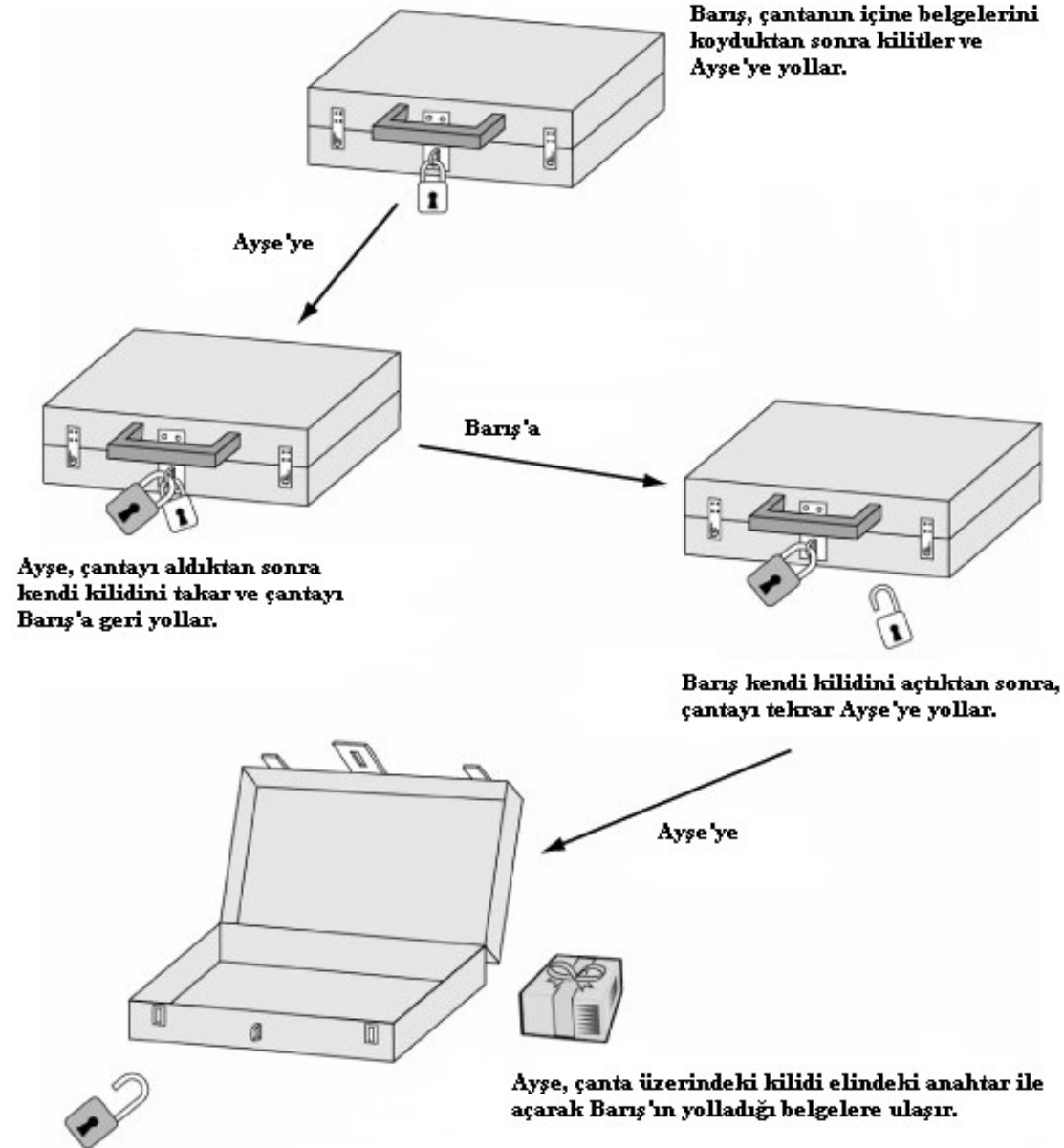
**\* IPSec**

**\* Kerberos**

**\* Point-to-Point Protokol**

# Diffie-Hellman Anahtar Değişimi

- Gizli anahtarlı sistemlerde şifreleme ve şifre çözme için ortak bir anahtar gerekmektedir.
- Diffie-Hellman anahtar değişimi bu anahtarı oluşturmak için kullanılmaktadır
- Sonlu cisimler üzerinde veya eliptik eğri aritmetiğinde bu anahtar değişiminin uygulaması yapılabilmektedir.



# Ayrık Logaritma Problemi

---

$$\triangleright Z_p^* = \{1, 2, \dots, p-1\}$$

$Z_p^*$ 'de  $g$  ve  $y$  verilmiş ve  $g^x = y \pmod{p}$  ise  $x$  kaçtır?

$x = \log_g y$  bulunması zor bir problemdir.

Örnek:  $Z_{17}$ 'de  $g=3$  ve  $y=11$ ,

$$3^x = 11 \pmod{17} \Rightarrow x = ?$$

$$3 \pmod{17} = 3$$

$$3^2 \pmod{17} = 9$$

$$3^3 \pmod{17} = 10$$

$$3^4 \pmod{17} = 13$$

$$3^5 \pmod{17} = 5$$

$$3^6 \pmod{17} = 15$$

$$3^7 \pmod{17} = 11$$

$$3^8 \pmod{17} = 16$$

$$3^9 \pmod{17} = 14$$

$$3^{10} \pmod{17} = 8$$

$$3^{11} \pmod{17} = 7$$

$$3^{12} \pmod{17} = 4$$

$$3^{13} \pmod{17} = 12$$

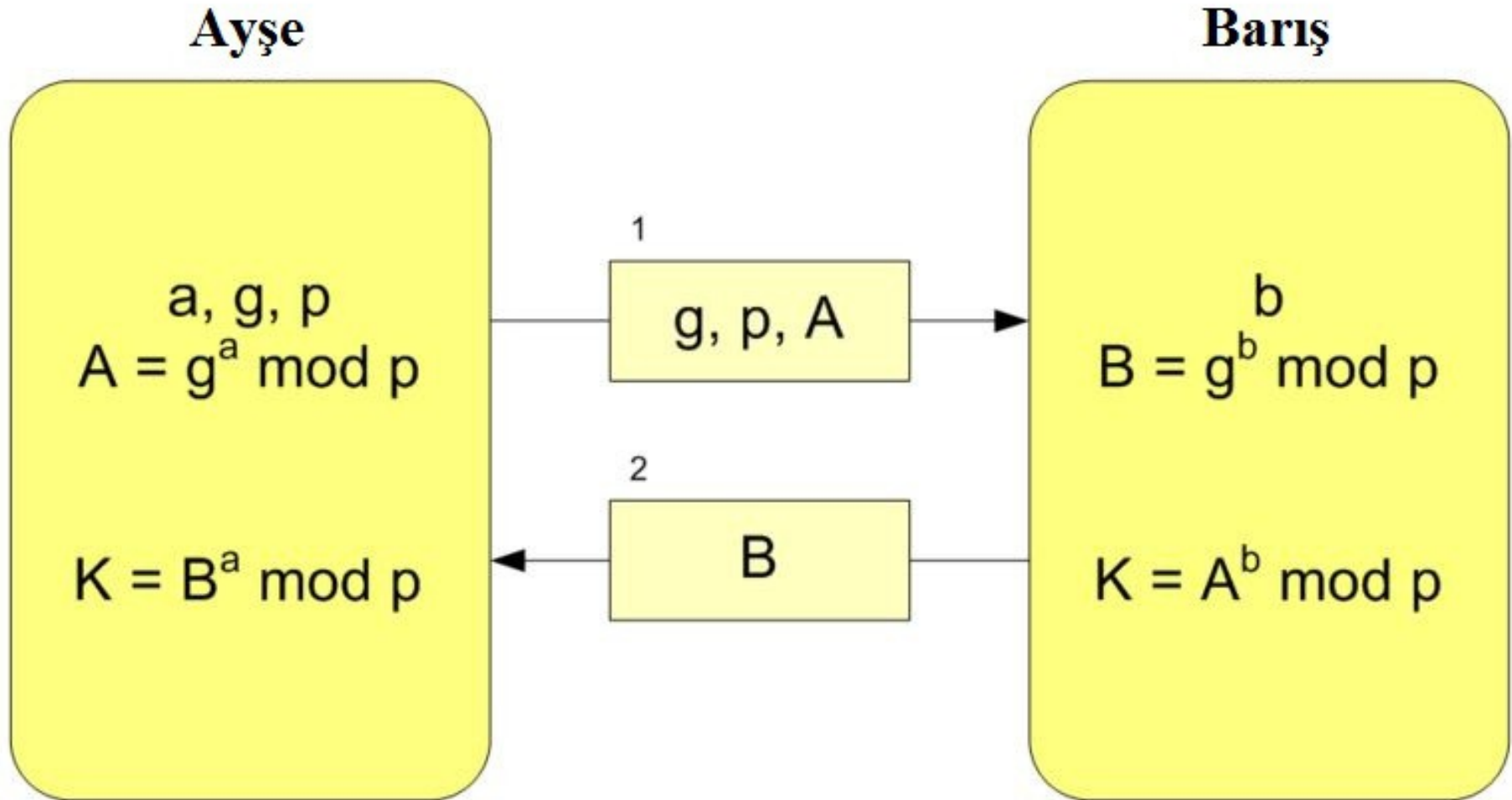
$$3^{14} \pmod{17} = 2$$

$$3^{15} \pmod{17} = 6$$

$$3^{16} \pmod{17} = 1$$

$$3^{17} \pmod{17} = 3$$

# Diffie-Hellman (DH) Anahtar Değişimi



$$K = A^b \text{ mod } p = (g^a \text{ mod } p)^b \text{ mod } p = g^{ab} \text{ mod } p = (g^b \text{ mod } p)^a \text{ mod } p = B^a \text{ mod } p$$

**a: Ayşe'nin kapalı anahtarı; b: Barış'ın kapalı anahtarı**

**A: Ayşe'nin açık anahtarı; B: Barış'ın açık anahtarı**



# DH Anahtar Değişimi protokolüne ortadaki adam saldırısı -man in the middle-

**Ayşe**

$$a, g, p$$
$$A = g^a \text{ mod } p$$

$$S^a \text{ mod } p =$$
$$(g^{sa}) \text{ mod } p = AA$$

**Saldırgan,**  
**Ayşe ile AA**

**gizli anahtarını paylaşır**

**fakat Ayşe, AA'yi Barış ile paylaştığını sanar.**

**Saldırgan**

s ve r seçer.

$$S = g^s \text{ mod } p$$

$$R = g^r \text{ mod } p$$

$$(g^a)^s \text{ mod } p =$$

$$(g^{as}) \text{ mod } p = AA$$

$$(g^b)^r \text{ mod } p =$$

$$(g^{br}) \text{ mod } p = BB$$

**Barış**

$$B = g^b \text{ mod } p$$

$$R^b \text{ mod } p =$$
$$(g^{rb}) \text{ mod } p = BB$$

**Saldırgan,**  
**Barış ile BB**  
**gizli anahtarını**  
**paylaşır**

# DH Anahtar Değişimi protokolüne ortadaki adam saldırısı -man in the middle-

**Ayşe**

$$E(M, AA) = C$$

**Saldırgan,  
Ayşe ile AA  
gizli anahtarını  
paylaştı.**

**Gizlilik İhlali**

**Saldırgan**

$$D(C, AA) = M$$

$$E(M, BB) = C''$$

**M yi  
değiştirme-  
den**

**E: Simetrik Şifreleme; D: Simetrik Deşifreleme**

**Bariş**

$$D(C'', BB) = M$$

**Saldırgan,  
Bariş ile BB  
gizli anahtarını  
paylaştı.**

# DH Anahtar Değişimi protokolüne ortadaki adam saldırısı -man in the middle-

**Ayşe**

$$E(M, AA) = C$$

**Saldırgan,  
Ayşe ile AA  
gizli anahtarını  
paylaştı.**

**Bütünlük İhlali**

**Saldırgan**

$$D(C, AA) = M$$

$$E(M', BB) = X$$

M yi  
değiştirip, M'  
yaratıp

**Barış**

$$D(X, BB) = M'$$

**Saldırgan,  
Barış ile BB  
gizli anahtarını  
paylaştı.**

E: Simetrik Şifreleme; D: Simetrik Deşifreleme

# DH Anahtar Değişimi Protokolüne ortadaki adam saldırısını önlemek

- Kimlik denetimi kullanmak: anahtarı değişinen tarafları, dijital imza kullanarak doğrulamak
- Endüstriyel yaklaşım: X.509 sertifika kullanımı

Ayşe'nin paylaştığı A, DH açık anahtarının, dijital imzası  $\text{Sig}(A)$  oluşturulur ve  $A||\text{Sig}(A)$ , Barış'a gönderilir.

Barış'ın paylaştığı B, DH açık anahtarının, dijital imzası  $\text{Sig}(B)$  oluşturulur ve  $B||\text{Sig}(B)$ , Barış'a gönderilir.

- Diğer yaklaşım: PGP anahtarları ile, DH açık anahtarlarını imzalamak. **GNU PG** ve **bunun kullanan yazılımlar** önerilir.

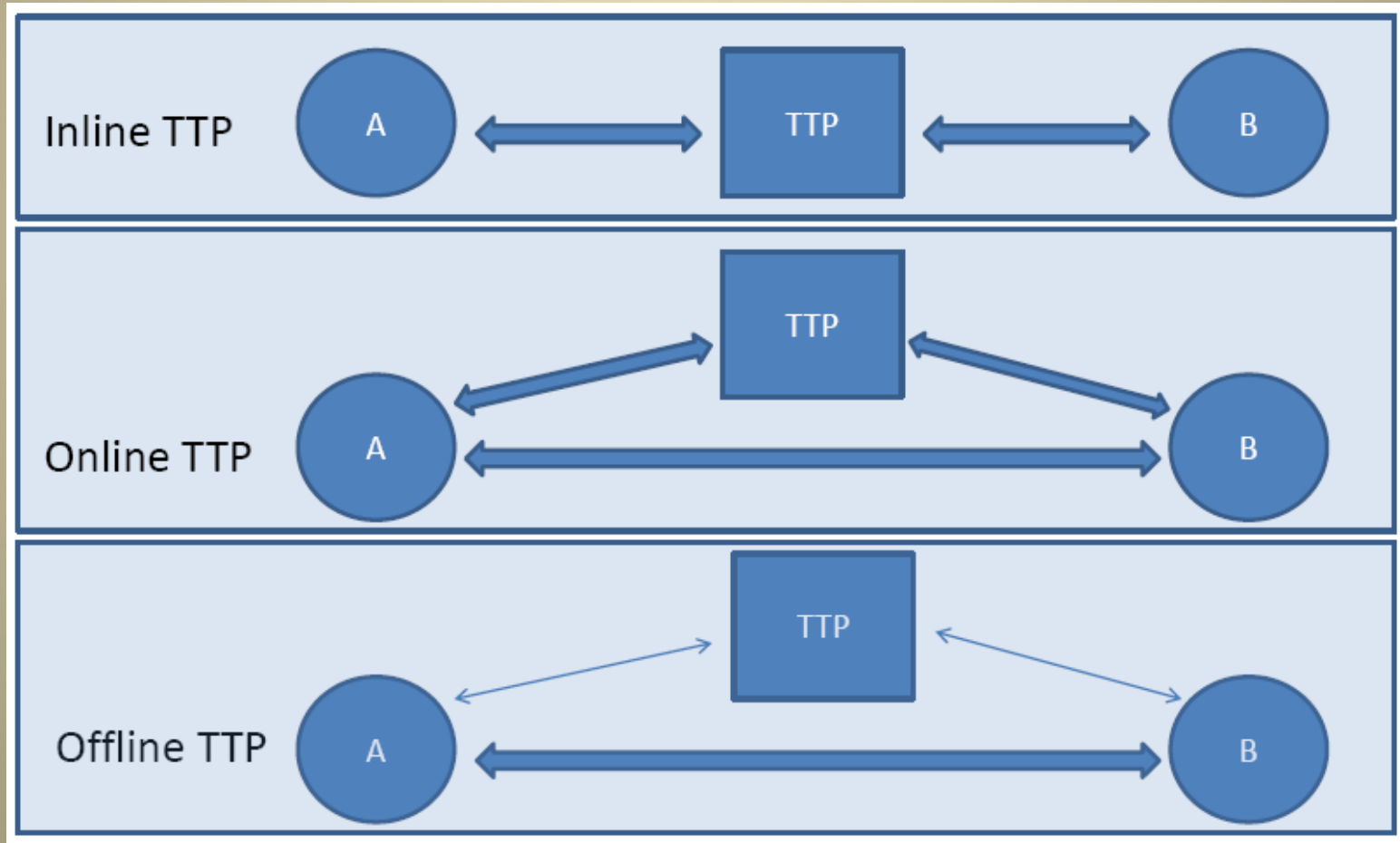
# KEP Protokolü

- E-posta gönderiminin yasal olarakta geçerliliğini sağlayacak, gönderildi ve alındı bildirimleri gibi kanıtları sağlayan temeli kriptografik yapılara dayanan protokol olarak tanımlanabilir.

# KEP Çeşitleri

- Güvenilir Üçüncü Taraf (Trusted Third Party) içeren yöntemler
  - Inline TTP
  - Çevrim dışı (Offline) TTP
  - Çevrim içi (Online) TTP
- Güvenilir Üçüncü Taraf içermeyen yöntemler

# KEP Çeşitleri







# KEP Protokol Özellikleri

- Adillik (Fairness)
- Gönderildi bildirimi (Sending Receipt)
- Kaynağın inkar edilememesi (Non-repudiation of origin)
- Alındı bildiriminin inkar edilememesi (Non-repudiation of receipt)
- Kimlik doğrulama (Authenticity)
- Bütünlük (Integrity)
- Gizlilik (Confidentiality)
- Zaman aralığı/Yerindelilik (Timeliness)
- Zamansal kimlik doğrulama (Temporal Authentication)

# Kaynağın inkar edilememesi (Non-repudiation of origin)

- E-posta gönderimini başlatan taraf mesajın kendisi tarafından gönderildiğini inkar edememeli, alıcı taraf mesajın kaynağına dair kanıta sahip olmalı

# **Alındı bildiriminin inkar edilememesi (Non-repudiation of receipt)**

- Alıcı mesajı aldığını inkar edememeli, protokol sonunda gönderici alıcının mesajı aldığına dair bir kanıta sahip olmalı

# Adillik (Fairness)

- Protokol adil olmalı: her iki tarafta gerekli bilgileri almalı yada hiçbiri yarar sağlayacak bir bilgiyi elde edememeli

# Gönderildi bildirimi (Sending Receipt)

- Gönderici e-posta göndermeyi başlattığına dair kanıt sağlayacak gönderildi bildirimine sahip olmalı

# Kimlik doğrulama (Authenticity)

- Protokole katılan taraflar için kimlik doğrulama sağlanmalı

# Bütünlük (Integrity)

- Protokole katılan taraflar fark ettirmeden gönderilen mesajların bütünlüğünü bozamamalı

# Gizlilik (Confidentiality)

- Sadece gönderici ve alıcı mesaj alışverişleri sonucu orijinal mesaja ulaşabilmeli



# Zaman Aralığı (Timeliness)

- Protokol süresi sonlu bir zaman olmalı, belirlenen zaman zarfında protokol sonlanamıyorsa protokol sonlandırılmalı.

# Zamansal Kimlik Doğrulama (Temporal Authentication)

- Mesaj alışverişinin başlama tarihi sertifikalanmalı ve protokoldeki yer alan taraflarca ulaşılabilmeli  
(Zaman Damgası)

# Bahreman and Tygar Protokolünün Geniřletilmiř Sürümü (Inline TTP)

- Stelvio Cimato, Clemente Galdi, Raffaella Giordano, Barbara Masucci ve Gildo Tomasco tarafından öne sürülmüřtür.
- Bahremen ve Tygar'ın öne sürdüėü protokole ek olarak zaman damgası fonksiyonelitesi eklenmiřtir.
- KEP gereksinimlerinin hepsini karřıladıėı öne sürülmüřtür.

# Protokol Tanımları

$\text{Sig}_A(M)$  : M mesajının A tarafından imzalanmış hali

- $h(.)$  : Özet fonksiyon
- $\text{PK}_B(M)$  : M mesajının B'nin açık anahtarı ile şifrelenmiş hali
- $E_K(M)$ : m mesajının K gizli anahtarı ile şifrelenmiş hali

# In-line TTP CEP by Cimato et al. (2005)

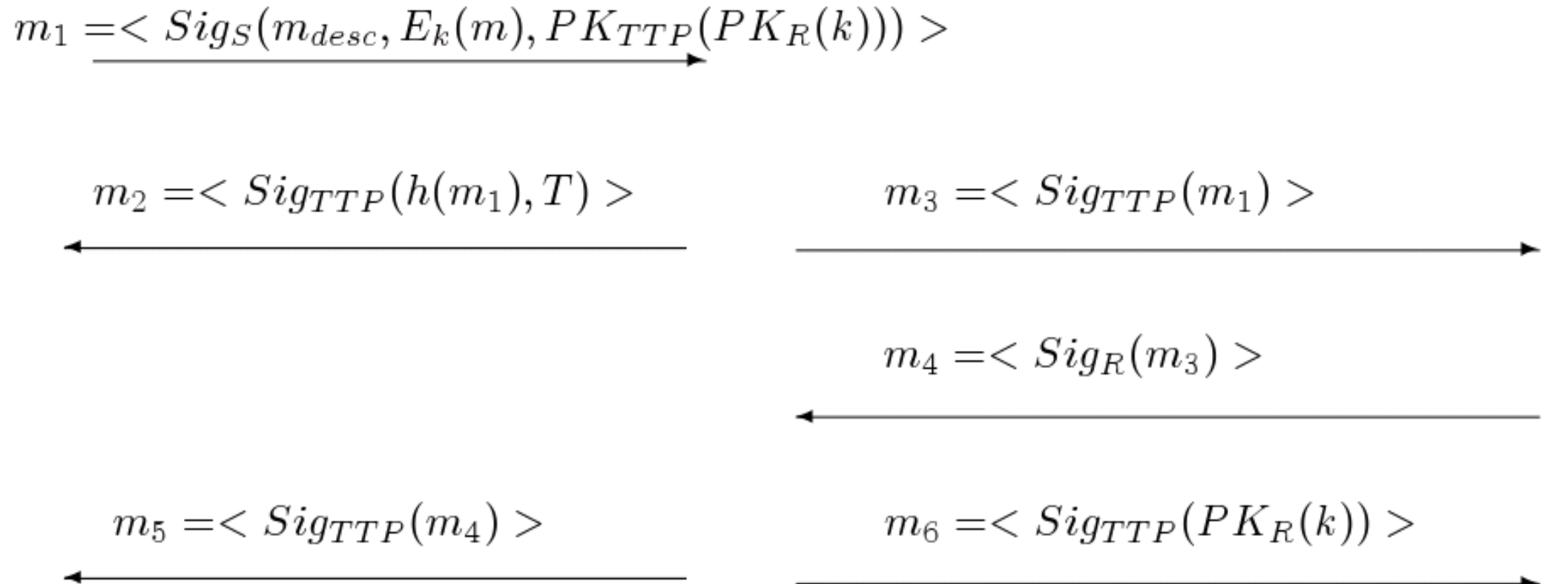
İlk in-line TTP KEP protokolü (Bahreman and Tygar, 1994) üzerine inşa

Sender

Trusted Third Party

Receiver

$m_1 = \langle \text{Sig}_S(m_{desc}, E_k(m), PK_{TTP}(PK_R(k))) \rangle$



$m_2 = \langle \text{Sig}_{TTP}(h(m_1), T) \rangle$

$m_3 = \langle \text{Sig}_{TTP}(m_1) \rangle$

$m_4 = \langle \text{Sig}_R(m_3) \rangle$

$m_5 = \langle \text{Sig}_{TTP}(m_4) \rangle$

$m_6 = \langle \text{Sig}_{TTP}(PK_R(k)) \rangle$

**Özellikler:** Fairness, Sending Receipt, NRO, NRR, Authenticity, Integrity, Confidentiality, Timeliness, Temporal Authentication

# Kayıtlı E-posta Protokolleri

## Saldırıları önlemek için bazı önlem ve tasarım prensipleri

- **Kılavuz #1 (Shao et al, 2005):** İletişim kanalları ile ilgili protokol varsayımlar ve gereksinimler açıkça tanımlanmalı. Böylece, uygulayıcılar da protokolü anlamalı ve rahat bir şekilde gerçekleştirebilmeli
- **Guideline 2 (Shao et al, 2005):** Protokol tasarımdan kullanılan kriptografik algoritmalar, güvenlik seviyeleri ve kullanım yöntemleri belirtilmeli.

# Kayıtlı E-posta Protokolleri

## Saldırıları önlemek için bazı önlem ve tasarım prensipleri

- **Kılavuz #3 (Shao et al, 2005):** Protokol adımını başlatan, alıcı ve belki 3. güvenilir şahış kimlikleri, inkar edilememelik kanıtınıyla ilişkilendirilmeli.
- **Kılavuz #4 (Shao et al, 2005):** Her adil deęişim protokolü dahil olmak üzere, anlaşmazlık çözüm politikalarının detayları, tanımları sunulmalı ve doğrulanmaları sunulmalı.

# Kayıtlı E-posta Protokolleri

## Saldırıları önlemek için bazı önlem ve tasarım prensipleri

- **Tasarım Prensipleri (Gürgens et al. 2005):**
  - Protokol adımlarındaki mesaj kısımları imzanın içinde yer almalı
  - Mesajı alan herkes, mesajının imzasını doğrulayabilmeli
  - Alıcı, mesajın protokolün hangi aşamasına ait olduğunu anlayabilmeli
  - TTP anlamlı kararlar alabilmeli
  - TTP, her isteğe cevap verebilmeli



# Kayıtlı E-posta Protokolleri

## Saldırıları önlemek için bazı önlem ve tasarım prensipleri

- **Tasarım Prensipleri (Kremer et al. 2002)**
  - İnkâr edilememelik (dijital imzalar ve ilgili anahtarlar) kanıtları iyi yönetilmeli
  - Eğer asimetrik sisteminin kullandığı açık anahtarının sertifikası iptal edildiyse, bu anahtar da iptal edilmeli
  - Dijital imzanın ne zaman oluşturulduğu belirlenmeli (sertifika iptalinden önce veya sonra)  
**Çözüm: Zaman Damgası kullanımı**

# Otomatik Protokol Doğrulama

- Protokollerin, güvenlik özelliklerinin sağlayıp, sağlamadıklarını kontrol edilir.
- Scyther (<http://www.cs.ox.ac.uk/people/cas.cremers/scyther/>), otomatik güvenlik protokol doğrulama araçıdır.

Scyther ve birkaç benzeri karşılaştırmalarını içeren ve Scyther kullanılan makaler:

- ASICS: Authenticated Key Exchange Security Incorporating Certification Systems
- Evaluation of ISO/IEC 9798 Protocols
- Provably Repairing the ISO/IEC 9798 Standard for Entity Authentication
- Automated Analysis of Diffie-Hellman Protocols and Advanced Security Properties
- Key Exchange in IPsec revisited: Formal Analysis of IKEv1 and IKEv2  
<http://www.cs.ox.ac.uk/people/cas.cremers/publications/index.html>

# Otomatik Protokol Doğrulama

- ProVerif: Kriptografik protokol doğrulama, biçimsel model ile

<http://prosecco.gforge.inria.fr/personal/bblanche/proverif/>

- “ Birçok farklı kriptografik algoritmayı, DH anahtar değişimi destekleniyor.

Diğer bir araç: AVISPA: Automated Validation of Internet Security Protocols and Applications (<http://www.avispa-project.org/>)

# Protokol Saldırıları

- Gizli Dinleme (pasif saldırı)
- Değiştirme (aktif saldırı)
- Tekrar oynatma -replay- (saldırgan protokoldeki kayıtları aynen ve değiştirilmiş halini, başka bir saldırıya zemin olması adına kullanır)
- Yazma (Typing) saldırısı (saldırgan, şifrelenen kısmı bir başka şifreli kısım ile değiştirebilir)
- Kriptanaliz uygulamak
- .....

# Kaynak Tavsiyesi

- Internet Security Protocols:

<http://www.youtube.com/watch?v=CZzd3i7Bs2o>

- ADVANCING AUTOMATED SECURITY PROTOCOL VERIFICATION (Thesis)

<http://e-collection.library.ethz.ch/eserv/eth:7011/eth-7011-02.pdf>

- Security Protocol Verification: Symbolic and Computational Models

<http://cs.ioc.ee/etaps12/invited/blanchet-slides.pdf>

- SECURE KEY MANAGEMENT PROTOCOL IN WIMAX

[https://www.idc-online.com/technical\\_references/pdfs/data\\_communications/SECURE%20KEY.pdf](https://www.idc-online.com/technical_references/pdfs/data_communications/SECURE%20KEY.pdf)

- Enhanced Mobile SET Protocol with Formal Verification

[http://ieeexplore.ieee.org/xpls/abs\\_all.jsp?arnumber=6394714](http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6394714)