# SSL/TLS

Halil Kemal TAŞKIN

Orta Doğu Teknik Üniversitesi
Uygulamalı Matematik Enstitüsü
Kriptografi Bölümü

# İçerik

# Açık Anahtar Altyapısı (AAA)

Veri iletişiminde açık anahtarlı kriptografinin yaygın ve güvenli olarak kullanılabilmesini sağlayan hizmetler bütünüdür.

- Gizlilik (confidentiality),
- Bütünlük (integrity),
- Kimlik Doğrulama (authentication),
- Reddedememe (non-repudiation)

fonksiyonlarını kullanıcıların dijital sertifika kullanması yolu ile sağlar.

- Sertifika, dijital bir kimlik olduğu gibi aynı zamanda sahibine ait bilgiler ile gerekli algoritma anahtarlarını üzerinde bulundurur.

# ESHS nedir?

**Elektronik İmza Kanunu Madde 8**

Elektronik sertifika hizmet sağlayıcısı, elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişilerdir.

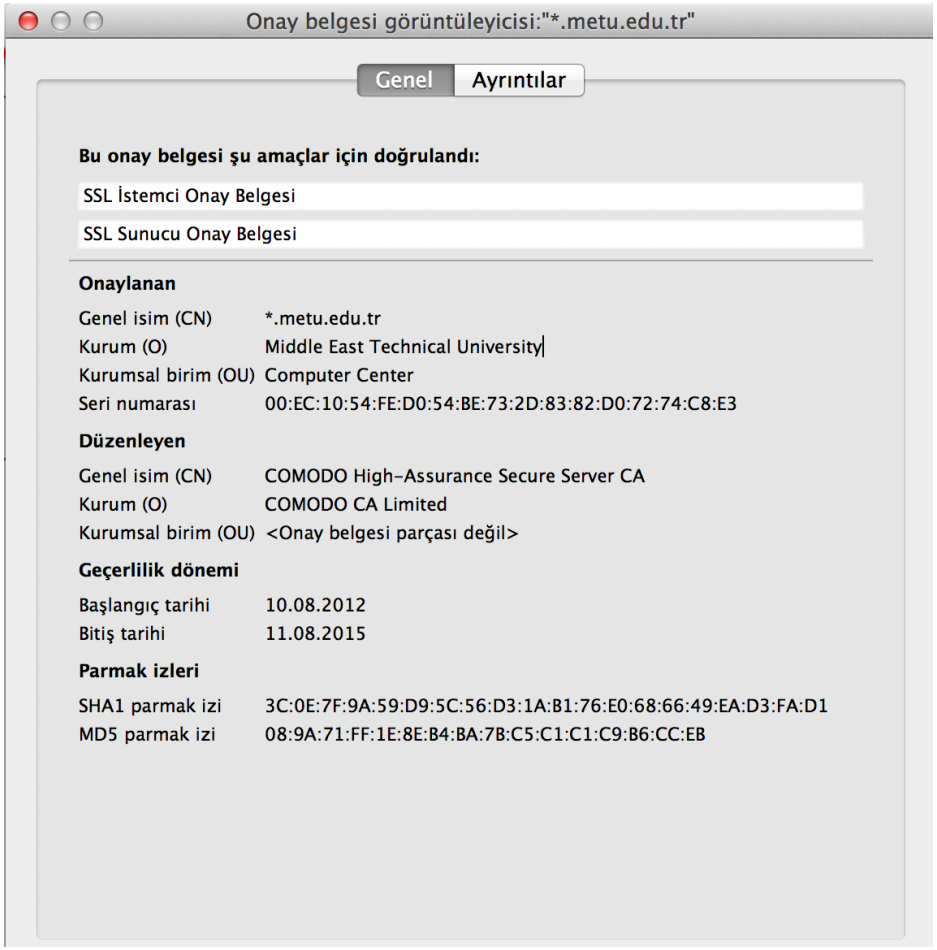
- ESHS: Elektronik Sertifika Hizmet Sağlayıcı
- CA: Certification Authority
- Güvenilir 3. Taraf! (Trusted 3rd Party)

# ESHS

- Güven sağlar.
- Güvenilir olmalıdır.
- Alanında yetkin ve uzman olmalıdır.
- İstikrarlı ve kesintisiz olmalıdır.
- Tarafsız olmalıdır.
- Teknik altyapısı güçlü olmalıdır.

# Elektronik Sertifikalar

- Bütünlüğü korunan bilgileri ve elektronik imzasını içeren dosyalardır.
- Sertifika bilgi içeriği ihtiyaca göre değişebilir.
- X.509v3 standardı kullanılmaktadır.



# Sertifika Sınıfları (Classes)

- **Class 0**: Test amaçlıdır ve herhangi bir kontrol yoktur.
- **Class 1**: Kişsel kullanım içindir.
- **Class 2**: Firmalar içindir ve kimlik denetimi için kullanılır.
- **Class 3**: Sunucular ve yazılım imzalama amaçlı kullanılır.
- **Class 4**: Şirketler arasındaki online işlemler için kullanılır.
- **Class 5**: Çok gizli dökümanlar ve devlet güvenliği seviyesinde kullanılır.

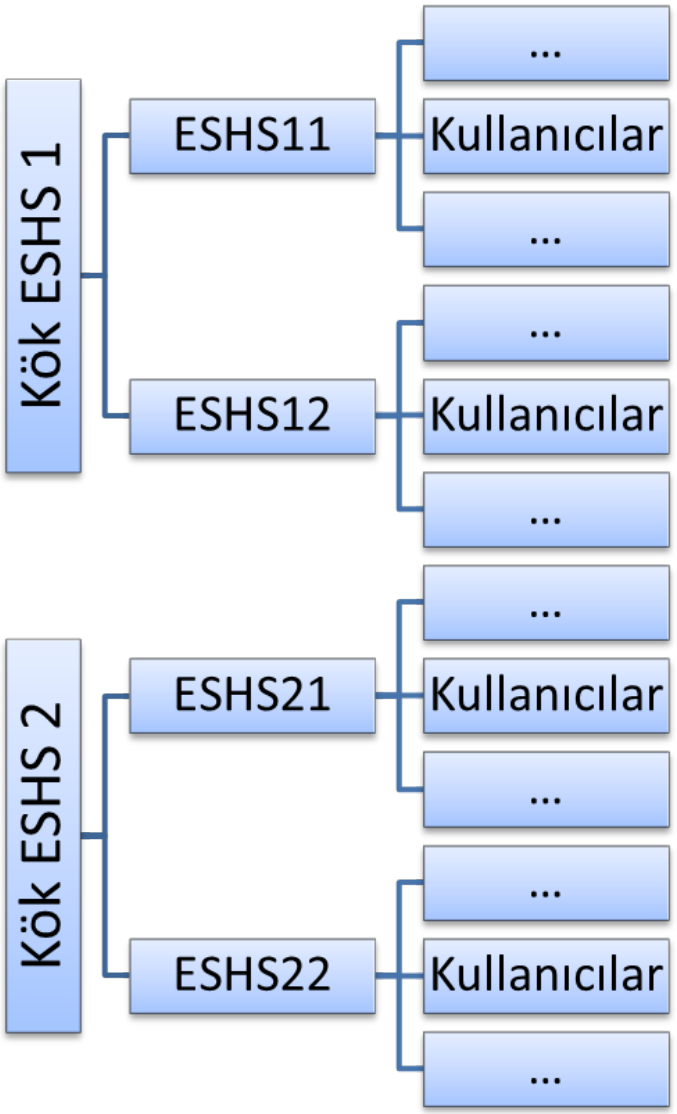
# X.509 İçeriği

- Seri No
- Düzenlenen Kurum
- Düzenleyen Kurum
- Başlangıç Tarihi
- Bitiş Tarihi
- Kullanım Yerleri
- Düzenlenen Kurumun Açık Anahtarı
- İmza Algoritması (Örnek: SHA1withRSA)
- Sertifika İmza Bilgisi
- Parmakizi Algoritması
- Parmak İzi Bilgisi

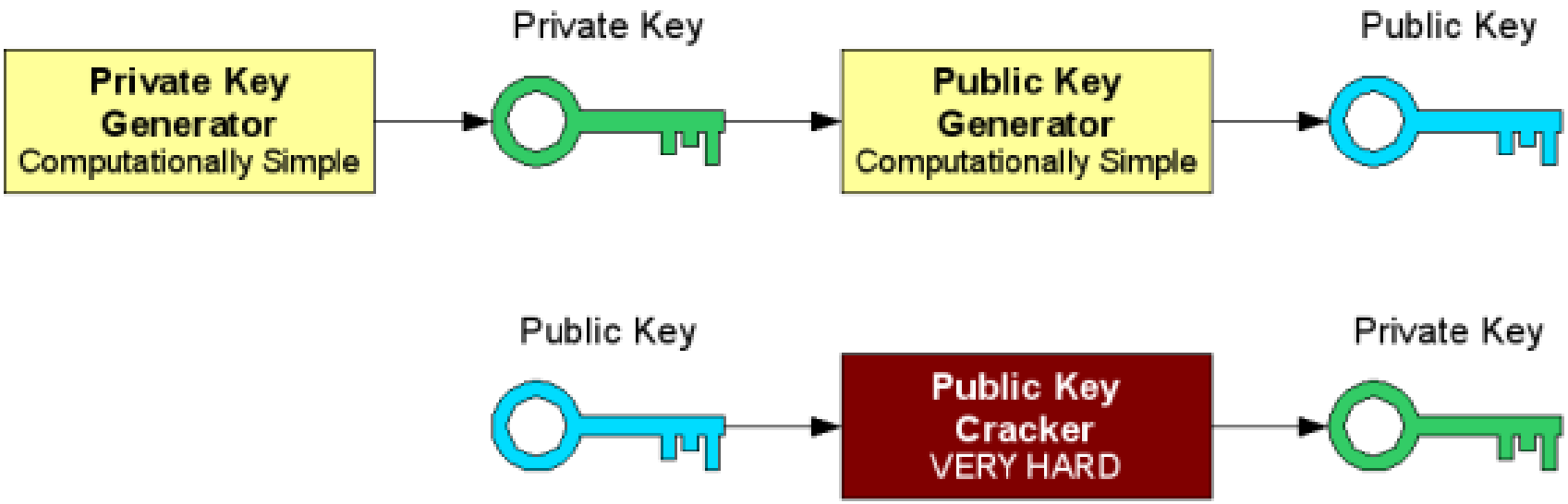
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            ec:10:54:fe:d0:54:be:73:2d:83:82:d0:72:74:c8:e3
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO High-Assurance Secure
        Validity
            Not Before: Aug 10 00:00:00 2012 GMT
            Not After : Aug 10 23:59:59 2015 GMT
        Subject: C=TR/postalCode=06800, ST=Ankara, L=Ankara/street=Universiteler Mah.Dumlupinar Bulvari.No:1,
 Technical University, OU=Computer Center, OU=Hosted by Turk of America, OU=PremiumSSL Wildcard, CN=*.metu.ed
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:df:8b:91:2b:88:16:0c:f4:61:c0:f8:cc:e9:43:
                    09:5e:29:67:1c:ee:5a:71:a3:ca:df:d2:31:16:d0:
                    f5:f9:1f:76:13:68:04:9d:f6:52:c3:c7:5d:32:24:
                    a8:21:c3:71:59:58:c7:2d:62:69:b2:c9:79:93:e4:
                    12:eb:a0:4d:a6:fb:08:4e:64:b1:ed:4a:da:05:12:
                    3c:de:7c:f0:b3:af:9d:76:7c:65:39:80:4d:a0:7e:
                    6a:10:27:f9:f7:c3:38:e4:13:48:6c:97:e6:8d:61:
                    75:9e:56:46:c4:db:43:58:d3:ee:ce:e9:4e:f4:5c:
                    41:e5:aa:b2:a3:be:03:c8:ce:90:64:1b:e4:98:2e:
                    db:96:56:d8:a4:11:ee:98:25:3b:1b:73:31:d8:d4:
                    c7:bb:6a:ba:71:1e:82:0d:16:7c:dd:c1:85:d2:a4:
                    44:41:0c:25:28:4b:4d:42:d2:eb:b1:2a:c8:84:88:
                    f8:ea:54:0c:14:bc:78:b0:7f:7f:44:b9:8e:5c:d8:
                    52:f4:b5:7d:42:3a:65:8b:da:e4:51:67:ad:a3:6d:
                    d2:75:35:8b:49:83:d3:90:5c:df:4d:39:18:99:8a:
                    5c:85:91:e9:5d:08:0b:91:de:7e:6b:8a:4f:fe:d4:
                    d1:6f:08:6a:4e:82:62:94:35:3a:17:a8:fd:d8:90:
                    5d:09
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:3F:D5:B5:D0:D6:44:79:50:4A:17:A3:9B:8C:4A:DC:B8:B0:22:64:6B
```

```
            X509v3 Subject Key Identifier:
                93:2E:1F:E5:5E:41:46:D6:95:69:48:06:44:4A:B4:16:F3:51:DB:35
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.6449.1.2.1.3.4
                  CPS: https://secure.comodo.com/CPS
                Policy: 2.23.140.1.2.2

            X509v3 CRL Distribution Points:
                URI:http://crl.comodoca.com/COMODOHigh-AssuranceSecureServerCA.crl

            Authority Information Access:
                CA Issuers - URI:http://crt.comodoca.com/COMODOHigh-AssuranceSecureServerCA.crt
                OCSP - URI:http://ocsp.comodoca.com

            X509v3 Subject Alternative Name:
                DNS:*.metu.edu.tr, DNS:metu.edu.tr
    Signature Algorithm: sha1WithRSAEncryption
        2e:ae:81:03:b7:84:01:7a:72:0c:fb:e5:9a:de:c0:c0:d0:3a:
        14:6a:59:e8:62:7f:95:9b:9b:dd:7b:ad:04:d3:28:ef:08:3d:
        1d:4c:52:68:4c:af:d9:6a:03:b0:fd:0f:70:83:ae:3a:a2:3a:
        07:1c:d2:fd:18:d5:aa:64:16:fe:6b:33:67:65:22:22:99:e6:
        35:21:41:2e:4e:52:a1:b0:2f:65:b1:c8:bf:76:fe:3e:9a:a6:
        94:43:99:0e:1e:31:92:c0:2f:f3:c3:98:8d:c4:57:3d:5a:97:
        71:82:d7:66:11:c8:14:32:34:7a:40:7d:45:0d:07:10:f3:11:
        a4:16:f7:76:11:06:bc:06:0b:e1:77:12:ce:b5:cc:99:2c:df:
        eb:e6:d7:99:6a:90:f6:60:27:44:02:df:48:bf:7d:90:5d:9c:
        9b:40:17:d1:ab:fc:a3:50:85:42:5c:f5:15:65:fb:92:79:c1:
        7d:48:65:65:88:0e:b2:e4:b9:9d:f2:8f:e9:7f:59:1a:f5:dd:
        82:c0:f5:42:b5:6c:fc:38:de:9f:cb:ee:1e:27:23:98:18:59:
        c5:53:a3:c0:b2:f4:22:a1:0d:3d:e1:b3:a2:e0:c5:37:19:db:
        7d:8e:fc:c0:c2:c1:a9:95:1e:26:7e:e6:87:c4:53:63:04:37:
        1b:09:60:91
```

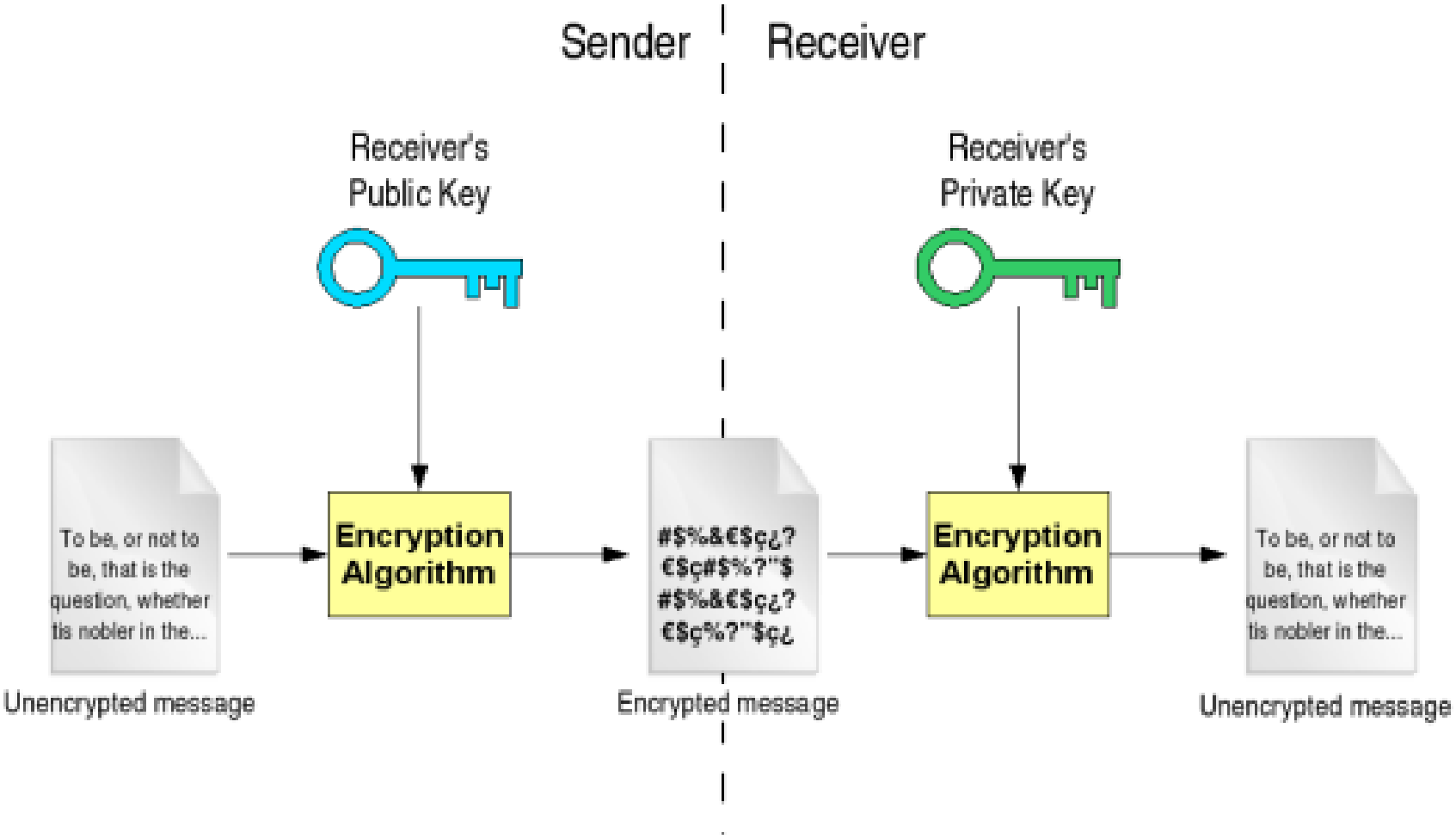
# Sertifikasyon Hiyerarşisi



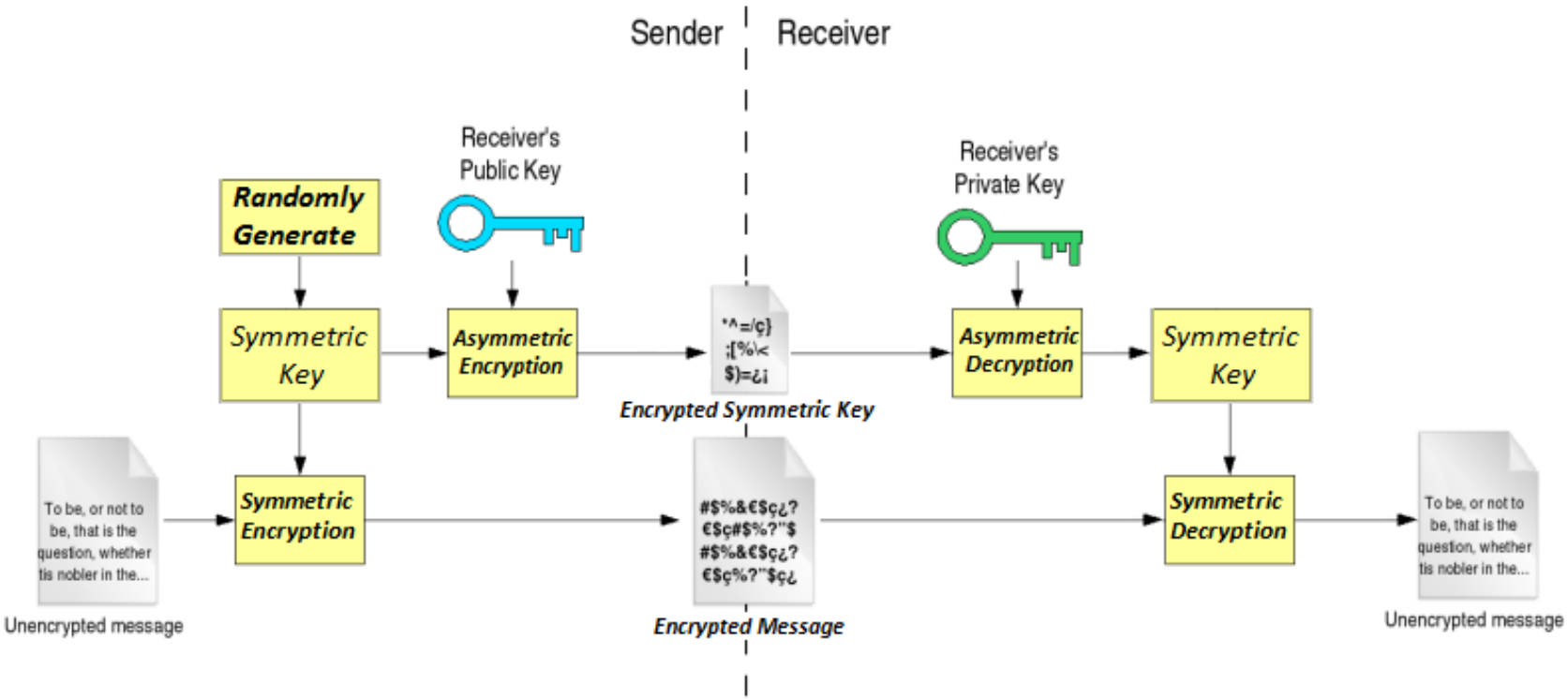
# Anahtar Çifti Üretimi



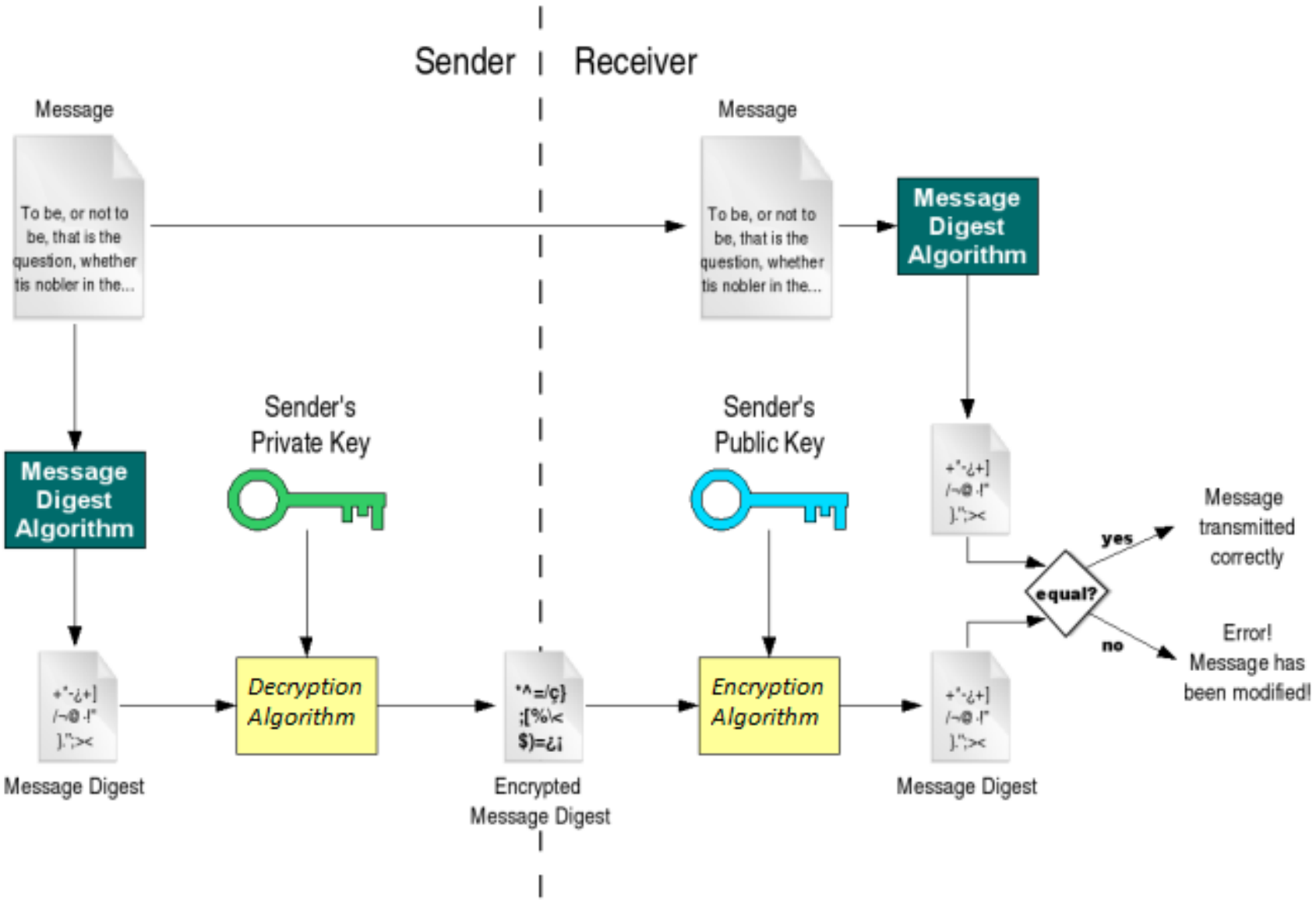
# Açık Anahtarlı Şifreleme



# Melez (Hybrid) Şifreleme



# Elektronik İmza



# SSL/TLS Protokolü

- Internet iletişimini şifrelemek için geliştirilmiştir.
- Web siteleri, E-Posta, anlık mesajlaşma ve VoIP güvenliği için kullanılabilir.
- Açık Anahtar Altyapısını kullanarak çalışır.
- İlk olarak 1995 yılında Netscape tarafından geliştirilmiştir.
- Son versiyonu TLS 1.2 RFC 5246 ile standartlaştırılmıştır.

# SSL/TLS Tarihçe

- **SSL 1.0**: Hiç kullanılmamıştır.
- **SSL 2.0**: 1995'de açıklandı ancak kritik zayıflıkları vardı.
- **SSL 3.0 (TLS 0.9)**: 1996'da tamamen yeni bir tasarım yapılarak yayınlandı. Günümüzdeki sistemlerin altyapısını oluşturmaktadır. RFC 6101.
- **TLS 1.0 (SSL 3.1)**: 1999'da yayınlanmıştır. SSL 3.0 ile benzer yapıdadır. RFC 2246.
- **TLS 1.1**:
  - 2006'da yayınlanmıştır. RFC 4346.
  - Eski sürümlerde bulunan ciddi zayıflıkları gidermektedir.
  - CBC Çalışma kipine yapılan ataklara karşı düzeltmeler vardır.
  - İlklendirme Vektörü (IV) kullanımı ile ilgili yenilikler vardır.
  - Tamamlama (Padding) hataları ile ilgili düzeltmeler yapılmıştır.

# SSL/TLS Tarihçe

- **TLS 1.2**:
  - 2008'de yayınlanmıştır. RFC 5246.
  - SHA-256 desteği eklenmiştir.
  - "Cipher Suite" genişletilmiştir.
  - AES ile şifreleme desteği gelmiştir.
  - Doğrulamalı Şifreleme (Authenticated Encryption) desteği gelmiştir.
  - AES-GCM ve AES-CCM çalışma kipleri eklenmiştir.
- 2011 yılında RFC 6176 ile TLS'in tüm sürümlerinin SSL kullanımı için geriye uyumluluğu kaldırılmıştır.

# SSL/TLS Yapısı

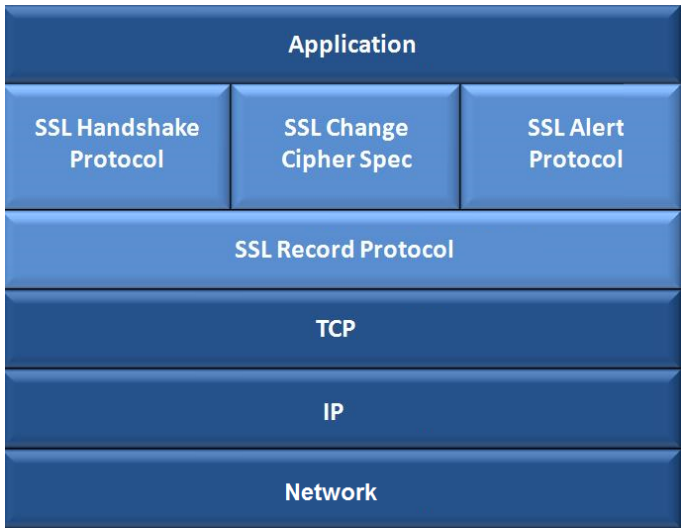
- Taşıma ve Uygulama katmanları arasında 3,5. katman olarak çalışır.
- HTTP+TLS=HTTPS (TCP 443)
- Protokol Katmanları:

  **Handshake**: İstemci ve sunucu arası oturum başlatma

  **Change CipherSpec**: Şifreleme üzerinde anlaşma

  **Alert**: Hata durumunda bildirim katmanı

  **Record**: Şifreli veriye doğrulama kodu ekleyip taşıma katmanına iletim katmanı

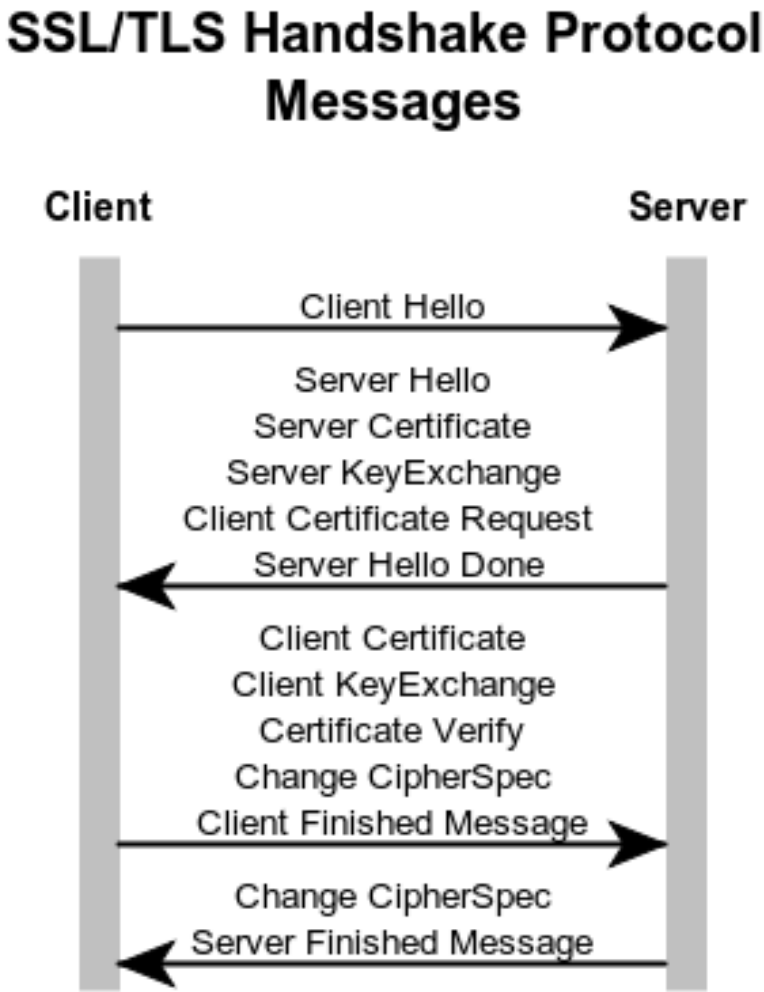


# SSL/TLS El Sıkışma Protokolü Adımları

1. SSL/TLS oturumunu başlatmak için senkronizasyon başlatma
2. Kullanılacak Algoritmalar Üzerinde Anlaşma
3. Sunucu ve İstemcilerin sertifika değişimi ve doğrulama
4. Oturum anahtarının oluşturulması ve doğrulama
5. Kayıt katmanında oturumun başlatılması
6. Sunucu ve istemcinin iletişim başlamaadn önce doğrulama yapmaları

# SSL/TLS El Sıkışma Protokolü

- İstemci protokolü başlatır.
- Server sertifikasını ve bilgilerini gönderir.
- İstemci sertifikayı doğrular ve rastgele bir simetrik anahtar oluşturup, sunucuya şifreli gönderir.
- Sunucu anahtarı doğrulayıp, algoritmalarda anlaşma yapar.
- Şifreli iletişim başlar.



# SSL/TLS Algoritmaları

- **Asimetrik Algoritmalar**

  RSA, DH, ECC
- **Simetrik Algoritmalar**

  AES, 3DES, RC4, Bölgesel (Camellia (Japon), SEED (Kore), GOST (Rus))
- **Özet Fonksiyonları**
- SHA-1, SHA-256

# Tarayıcı SSL/TLS Destek Durumu

| Tarayıcı | TLS 1.2 | TLS 1.1 | TLS 1.0 | SSL 3.0 | SSL 2.0 |
|---|---|---|---|---|---|
| Safari | Evet | Evet | Evet | Evet | Hayır |
| Opera 16.0 | Evet | Evet | Evet | Evet | Hayır |
| Chrome 36.0 | Evet | Evet | Evet | Evet | Hayır |
| Firefox 31.0 | Evet | Hayır | Evet | Evet | Hayır |
| Yandex 1.7 | Evet | Hayır | Evet | Evet | Hayır |
| IE 10.0 | Hayır | Hayır | Evet | Evet | Hayır |

- Test Sitesi: `https://www.ssllabs.com/projects/`

# Dünya'daki Önemli ESHS Olayları

- RealTek
- TrustWave
- DigiNotar ve Comodo
- Microsoft
- TürkTrust
- OpenSSL: Heartbleed

# RealTek

- 2010 yılında Stuxnet'in keşfinden sonra yapılan incelemeler sonucu bazı geçerli kod sertifikaları bulunmuştur.

# RealTek

- 2010 yılında Stuxnet'in keşfinden sonra yapılan incelemeler sonucu bazı geçerli kod sertifikaları bulunmuştur.
- Sisteme saldırmak için yerleşen DLL dosyalarının geçerli imzaya sahip olması virüsü bu denli güçlü yapmıştır.

# RealTek

- 2010 yılında Stuxnet'in keşfinden sonra yapılan incelemeler sonucu bazı geçerli kod sertifikaları bulunmuştur.
- Sisteme saldırmak için yerleşen DLL dosyalarının geçerli imzaya sahip olması virüsü bu denli güçlü yapmıştır.
- Araştırmalar sonucu geçerli imzanın RealTek firmasının HongKong'taki ofisinden fiziksel yollarla çalındığı anlaşılmıştır.

# RealTek

- 2010 yılında Stuxnet'in keşfinden sonra yapılan incelemeler sonucu bazı geçerli kod sertifikaları bulunmuştur.
- Sisteme saldırmak için yerleşen DLL dosyalarının geçerli imzaya sahip olması virüsü bu denli güçlü yapmıştır.
- Araştırmalar sonucu geçerli imzanın RealTek firmasının HongKong'taki ofisinden fiziksel yollarla çalındığı anlaşılmıştır.
- RealTek Firmasının sürücü imzalamak için kullandığı özel anahtarın bulunduğu odaya hırsızların girerek anahtarı kopyaladığı ya da virüsleri için gerekli imzayı oda içindeki HSM cihazından temin ettikleri tahmin edilmektedir.

# TrustWave

- 2012 yılında TrustWave firması bir firma için normal sertifika üretmek yerine yanlışlıkla SİS üretmiştir.
- Üretilen sertifika firma içinde Gmail ve Hotmail trafiğini izlemek için kullanılmaya çalışılmıştır.
- TrustWave, bu olaydan sonra gönüllü olarak kendi alt güven düzeyini 0'a çekmiş ve tekrar böyle bir olayın olmayacağını ifade etmiştir.

# Microsoft

- 2012 yılında tespit edilen Flame zararlı yazılımında Microsoft kökenli bir sertifikanın ihlali tespit edilmiştir.

# Microsoft

- 2012 yılında tespit edilen Flame zararlı yazılımında Microsoft kökenli bir sertifikanın ihlali tespit edilmiştir.
- Detaylar incelendiğinde, Windows işletim sisteminin güvenlik güncellemeleri için kullandığı bir sertifikanın Flame zararlı yazılımı tarafından da geçerli bir şekilde kullanıldığı tespit edilmiştir.

# Microsoft

- 2012 yılında tespit edilen Flame zararlı yazılımında Microsoft kökenli bir sertifikanın ihlali tespit edilmiştir.
- Detaylar incelendiğinde, Windows işletim sisteminin güvenlik güncellemeleri için kullandığı bir sertifikanın Flame zararlı yazılımı tarafından da geçerli bir şekilde kullanıldığı tespit edilmiştir.
- Teknik detaylara göre, sertifika için kullanılan özet fonksiyonu olan MD5'in bir zayıflığı kullanılarak aynı sertifika için geçerli olan ve zararlı içerik barındıran ikinci bir dosya daha oluşturulmuştur.

# Microsoft

- 2012 yılında tespit edilen Flame zararlı yazılımında Microsoft kökenli bir sertifikanın ihlali tespit edilmiştir.
- Detaylar incelendiğinde, Windows işletim sisteminin güvenlik güncellemeleri için kullandığı bir sertifikanın Flame zararlı yazılımı tarafından da geçerli bir şekilde kullanıldığı tespit edilmiştir.
- Teknik detaylara göre, sertifika için kullanılan özet fonksiyonu olan MD5'in bir zayıflığı kullanılarak aynı sertifika için geçerli olan ve zararlı içerik barındıran ikinci bir dosya daha oluşturulmuştur.
- Bu açıdan bakıldığında, sisteme sızan kötücül yazılımlar arasında kriptografik algoritmaların daha önceden keşfedilmemiş zayıflığını kullanan ilk zararlı yazılımdır.

# Microsoft

- 2012 yılında tespit edilen Flame zararlı yazılımında Microsoft kökenli bir sertifikanın ihlali tespit edilmiştir.
- Detaylar incelendiğinde, Windows işletim sisteminin güvenlik güncellemeleri için kullandığı bir sertifikanın Flame zararlı yazılımı tarafından da geçerli bir şekilde kullanıldığı tespit edilmiştir.
- Teknik detaylara göre, sertifika için kullanılan özet fonksiyonu olan MD5'in bir zayıflığı kullanılarak aynı sertifika için geçerli olan ve zararlı içerik barındıran ikinci bir dosya daha oluşturulmuştur.
- Bu açıdan bakıldığında, sisteme sızan kötücül yazılımlar arasında kriptografik algoritmaların daha önceden keşfedilmemiş zayıflığını kullanan ilk zararlı yazılımdır.
- Microsoft firması gerekli güncellemeleri yayınlayarak ilgili sertifikayı iptal etmiştir.

# DigiNotar ve Comodo

- 2011 yılında Hollanda kökenli DigiNotar firmasının kök sertifikalarının özel anahtarı ele geçirilerek başta Google'a ait sistemlerin web siteleri olmak üzere toplamda 531 sahte SSL sertifikası üretilmiştir.

# DigiNotar ve Comodo

- 2011 yılında Hollanda kökenli DigiNotar firmasının kök sertifikalarının özel anahtarı ele geçirilerek başta Google'a ait sistemlerin web siteleri olmak üzere toplamda 531 sahte SSL sertifikası üretilmiştir.
- Üretilen sertifikalar ile özellikle İran'daki Gmail kullanıcılarının e-postaları okunmuştur. Yaklaşık 300.000 kullanıcının e-posta trafiğinin kaydedildiği tahmin edilmektedir.

# DigiNotar ve Comodo

- 2011 yılında Hollanda kökenli DigiNotar firmasının kök sertifikalarının özel anahtarı ele geçirilerek başta Google'a ait sistemlerin web siteleri olmak üzere toplamda 531 sahte SSL sertifikası üretilmiştir.
- Üretilen sertifikalar ile özellikle İran'daki Gmail kullanıcılarının e-postaları okunmuştur. Yaklaşık 300.000 kullanıcının e-posta trafiğinin kaydedildiği tahmin edilmektedir.
- Her ne kadar zarar görmemiş olsa da Comodo şirketi de aynı saldırganların hedefine alınmıştır. Ancak saldırılar başarısız olmuştur.

# DigiNotar ve Comodo

- 2011 yılında Hollanda kökenli DigiNotar firmasının kök sertifikalarının özel anahtarı ele geçirilerek başta Google'a ait sistemlerin web siteleri olmak üzere toplamda 531 sahte SSL sertifikası üretilmiştir.
- Üretilen sertifikalar ile özellikle İran'daki Gmail kullanıcılarının e-postaları okunmuştur. Yaklaşık 300.000 kullanıcının e-posta trafiğinin kaydedildiği tahmin edilmektedir.
- Her ne kadar zarar görmemiş olsa da Comodo şirketi de aynı saldırganların hedefine alınmıştır. Ancak saldırılar başarısız olmuştur.
- Olay sonucu DigiNotar firması tüm dünyada itibarını ve güvenin kaybetmiştir. Şirket yaşadığı kriz sonucu iflas ederek kapanmıştır.

# TürkTrust

- 2011 yılında yapılan bir hatalı işlem sonucu TürkTrust tarafından KKTC Merkez bankası ve Ankara EGO kurumu için SSL sertifikası yerine Sertifika İmzalayan Sertifika üretilmiştir.

# TürkTrust

- 2011 yılında yapılan bir hatalı işlem sonucu TürkTrust tarafından KKTC Merkez bankası ve Ankara EGO kurumu için SSL sertifikası yerine Sertifika İmzalayan Sertifika üretilmiştir.
- 21 Aralık 2012 tarihine kadar bu durum anlaşılamamıştır.

# TürkTrust

- 2011 yılında yapılan bir hatalı işlem sonucu TürkTrust tarafından KKTC Merkez bankası ve Ankara EGO kurumu için SSL sertifikası yerine Sertifika İmzalayan Sertifika üretilmiştir.
- 21 Aralık 2012 tarihine kadar bu durum anlaşılamamıştır.
- 6 Aralık 2012 tarihinde EGO kurumuna güvenlik duvarı kurularak hatalı üretilen sertifika yüklenmiş ve SSL trafiği izleme özelliği aktif edilmiştir.

# TürkTrust

- 2011 yılında yapılan bir hatalı işlem sonucu TürkTrust tarafından KKTC Merkez bankası ve Ankara EGO kurumu için SSL sertifikası yerine Sertifika İmzalayan Sertifika üretilmiştir.
- 21 Aralık 2012 tarihine kadar bu durum anlaşılamamıştır.
- 6 Aralık 2012 tarihinde EGO kurumuna güvenlik duvarı kurularak hatalı üretilen sertifika yüklenmiş ve SSL trafiği izleme özelliği aktif edilmiştir.
- EGO kurumu içinde kullanılan Google Chrome Internet tarayıcısında bulunan dahili sertifika kontrol özelliği sayesinde Chrome, Google tabanlı sitelere erişim için kullanılan sertifikanın Google tarafından sağlanan sertifikalardan olmadığı tespit ederek durumu Google sunucularına bildirmiştir.

# TürkTrust

- Yapılan incelemenin ardından Google, Gmail posta hesaplarını izlemeyi sağlayan bu SSL sertifika ihlal durumunu hemen diğer tarayıcılara da iletmiştir. Google ve ardından Mozilla, TürkTrust'ın alt güven düzeyini 0'a çekmişlerdir.

# TürkTrust

- Yapılan incelemenin ardından Google, Gmail posta hesaplarını izlemeyi sağlayan bu SSL sertifika ihlal durumunu hemen diğer tarayıcılara da iletmiştir. Google ve ardından Mozilla, TürkTrust'ın alt güven düzeyini 0'a çekmişlerdir.
- Diğer tarayıcılar da önlemlerini almışlar ve iptal için gerekli güncellemeleri yayınlamışlardır. Aynı zamanda TürkTrust firması da web siteleri üzerinden durumu açıklayan teknik bir duyuru yapmışlardır.

# TürkTrust

- Yapılan incelemenin ardından Google, Gmail posta hesaplarını izlemeyi sağlayan bu SSL sertifika ihlal durumunu hemen diğer tarayıcılara da iletmiştir. Google ve ardından Mozilla, TürkTrust'ın alt güven düzeyini 0'a çekmişlerdir.
- Diğer tarayıcılar da önlemlerini almışlar ve iptal için gerekli güncellemeleri yayınlamışlardır. Aynı zamanda TürkTrust firması da web siteleri üzerinden durumu açıklayan teknik bir duyuru yapmışlardır.
- Olay, tüm dünyada oldukça ilgi çekmiş ve TürkTrust'a olan güvenin sorgulanmasına sebep olmuştur.

# TürkTrust

- Olay sonrası başta Mozilla olmak üzere tüm tarayıcılar TürkTrust'ın yeni dönem kök sertifikalarını Internet tarayıcılarına ekleme güncellemesini belirsiz bir süre ertelemişlerdir ve alt güven düzeyini sabit olarak 0'a çekmişlerdir.

# TürkTrust

- Olay sonrası başta Mozilla olmak üzere tüm tarayıcılar TürkTrust'ın yeni dönem kök sertifikalarını Internet tarayıcılarına ekleme güncellemesini belirsiz bir süre ertelemişlerdir ve alt güven düzeyini sabit olarak 0'a çekmişlerdir.
- Durumun ciddiyetini vurgulamak açısından, RSA 2013 konferansında, RSA kriptosisteminin kurucularından olan ve siber güvenlik dünyasının etkili isimlerinden biri olan bilim adımı Adi Shamir'e 2012 yılının en önemli siber güvenlik ihlali olayı sorulduğunda TürkTrust'ın yaptığı hatayı söylemiştir.

# OpenSSL: Heartbleed

- Açık kaynaklı OpenSSL (1.0.1) kütüphanesinde tespit edilen bir yazılım hatasıdır.

# OpenSSL: Heartbleed

- Açık kaynaklı OpenSSL (1.0.1) kütüphanesinde tespit edilen bir yazılım hatasıdır.
- Sunucu üzerindeki hafızadan rastgele veriler okunabilmektedir.

# OpenSSL: Heartbleed

- Açık kaynaklı OpenSSL (1.0.1) kütüphanesinde tespit edilen bir yazılım hatasıdır.
- Sunucu üzerindeki hafızadan rastgele veriler okunabilmektedir.
- Bu verilerin içinde SSL için kullanılan özel anahtarlarda mevcuttur.

# OpenSSL: Heartbleed

- Açık kaynaklı OpenSSL (1.0.1) kütüphanesinde tespit edilen bir yazılım hatasıdır.
- Sunucu üzerindeki hafızadan rastgele veriler okunabilmektedir.
- Bu verilerin içinde SSL için kullanılan özel anahtarlarda mevcuttur.
- SSL sunucusunun kontrolü için gönderilen pakette geri gönderilmesi istenen bilgi ve boyutu gönderilir.

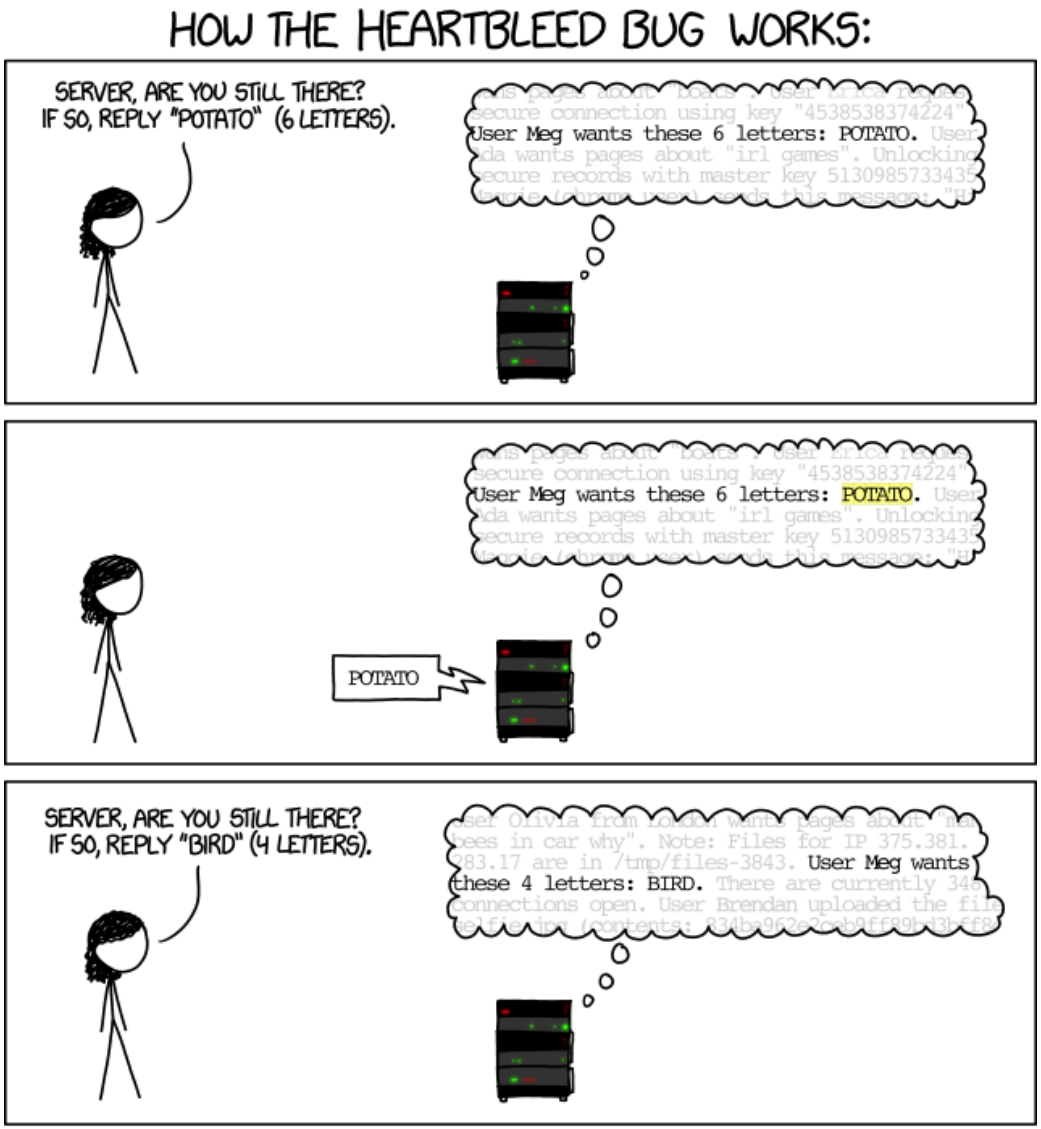
# OpenSSL: Heartbleed

- Açık kaynaklı OpenSSL (1.0.1) kütüphanesinde tespit edilen bir yazılım hatasıdır.
- Sunucu üzerindeki hafızadan rastgele veriler okunabilmektedir.
- Bu verilerin içinde SSL için kullanılan özel anahtarlarda mevcuttur.
- SSL sunucusunun kontrolü için gönderilen pakette geri gönderilmesi istenen bilgi ve boyutu gönderilir.
- Ancak OpenSSL istenen bilginin gerçek boyutuna bakmadan belirtilen boyutta veriyi geri gönderir.

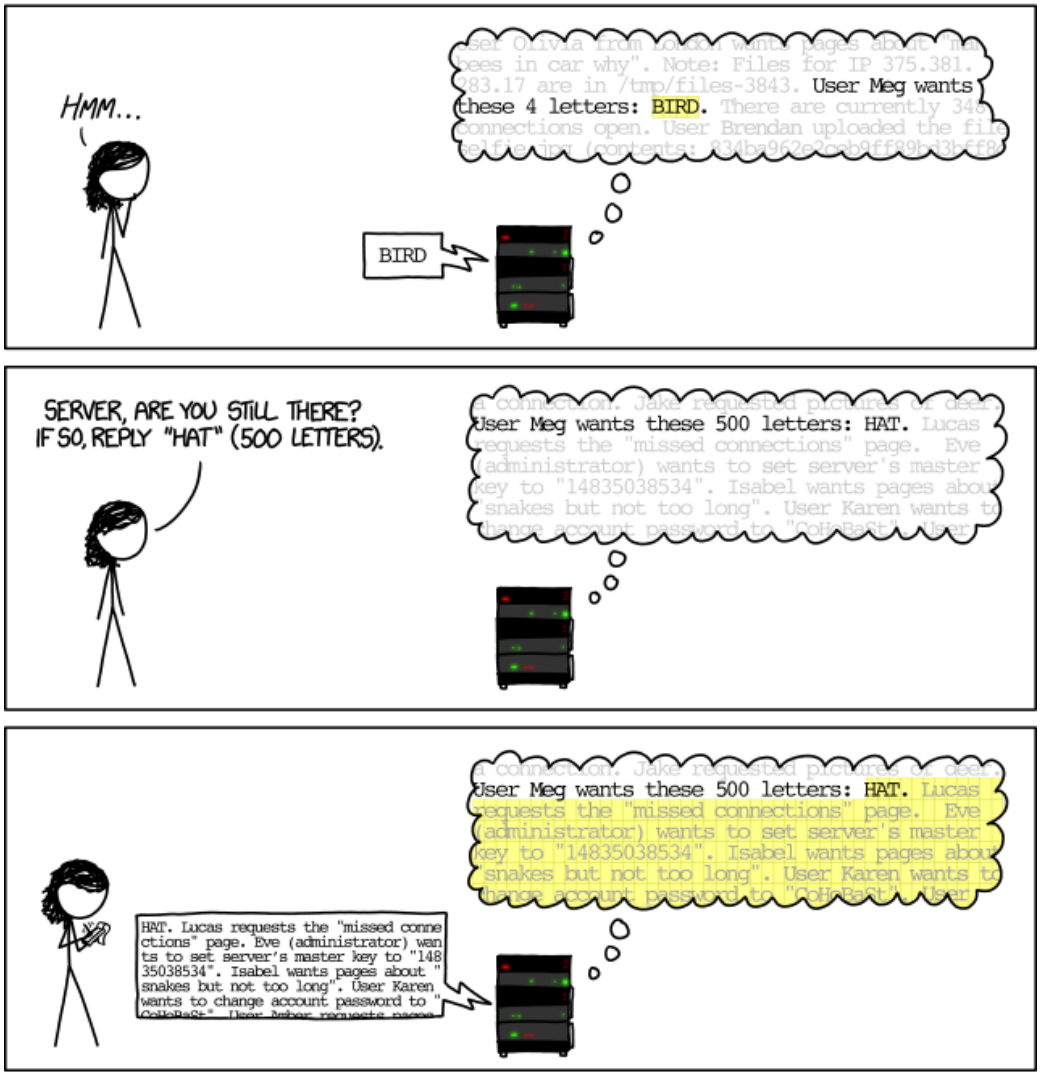
# OpenSSL: Heartbleed

- Açık kaynaklı OpenSSL (1.0.1) kütüphanesinde tespit edilen bir yazılım hatasıdır.
- Sunucu üzerindeki hafızadan rastgele veriler okunabilmektedir.
- Bu verilerin içinde SSL için kullanılan özel anahtarlarda mevcuttur.
- SSL sunucusunun kontrolü için gönderilen pakette geri gönderilmesi istenen bilgi ve boyutu gönderilir.
- Ancak OpenSSL istenen bilginin gerçek boyutuna bakmadan belirtilen boyutta veriyi geri gönderir.
- Bu sayede istenen bilgiden daha büyük boyut belirtildiğince bellekteki rastgele alanlardaki veriler gönderilmektedir.

# xkcd #1354: Heartbleed Explanation



# xkcd #1354: Heartbleed Explanation



# Teşekkürler.
Sorular?