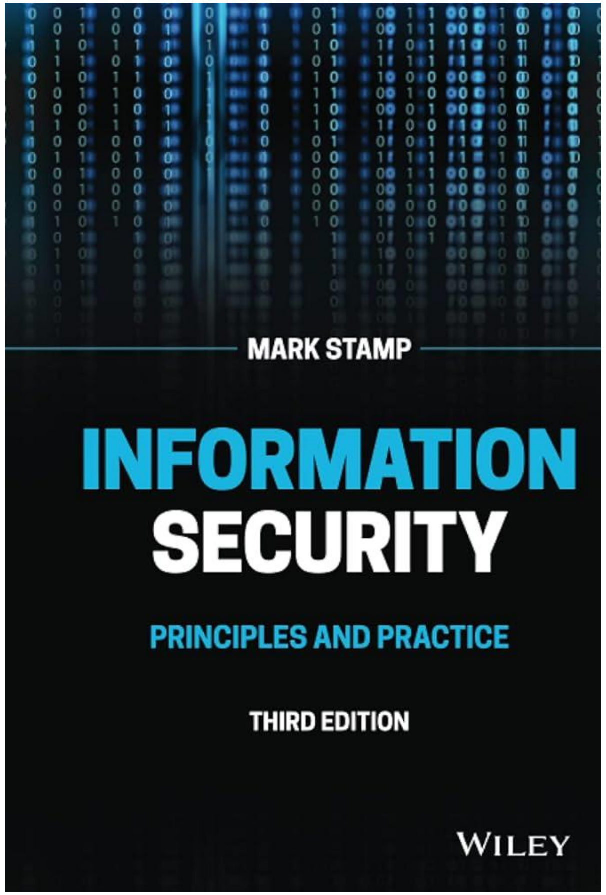
بسم الله الرحمن الرحیم

مبانی رایانش امن

جلسه ۱۱

مجتبی خلیلی
دانشکده برق و کامپیوتر
دانشگاه صنعتی اصفهان

- فصل ۲۲ و ۲۳ استالینگ
- فصل ۱۰ استمپ



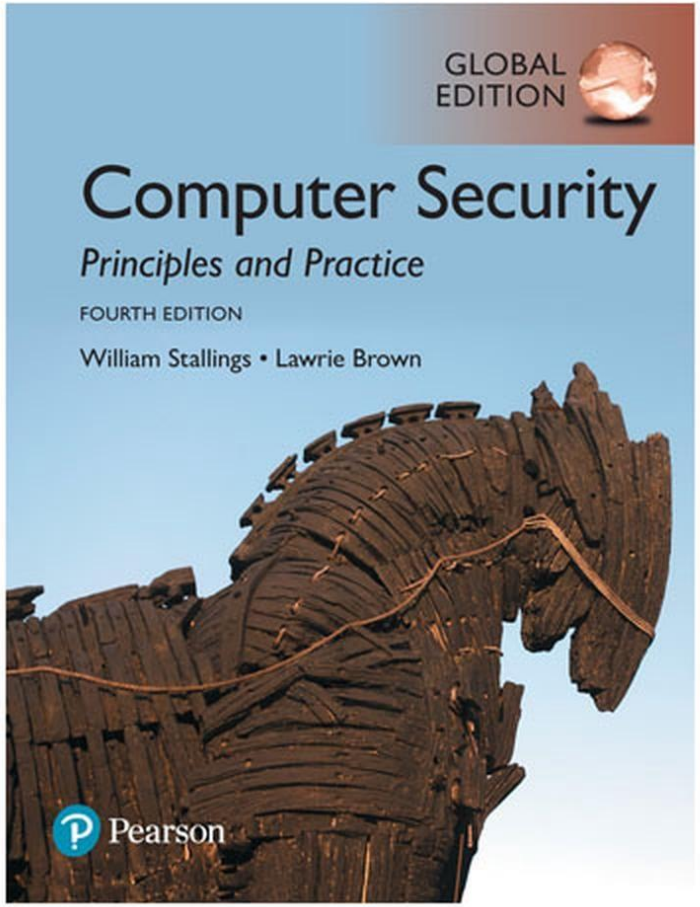
MARK STAMP

INFORMATION SECURITY

PRINCIPLES AND PRACTICE

THIRD EDITION

WILEY



GLOBAL EDITION

Computer Security

Principles and Practice

FOURTH EDITION

William Stallings • Lawrie Brown

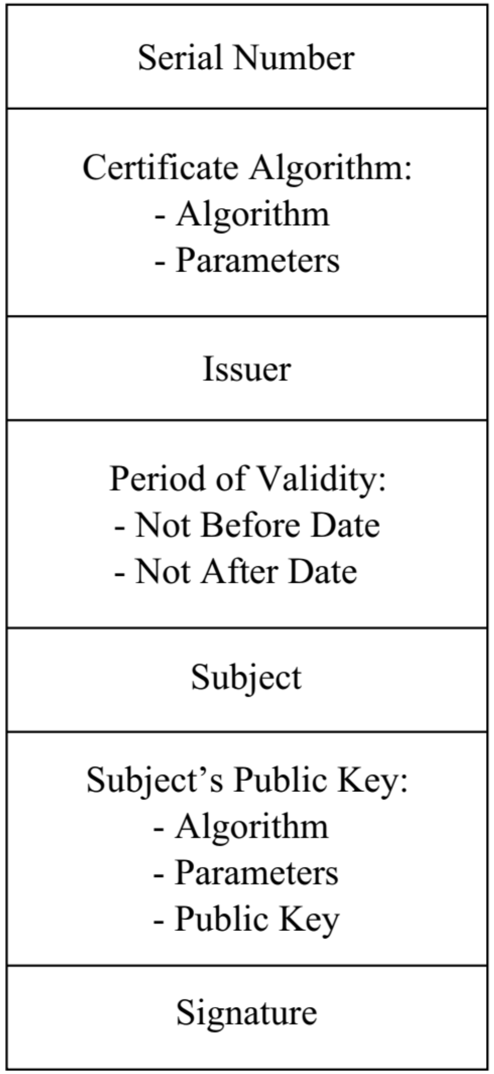
Pearson

public-key infrastructure

The entire system that is formed by CAs together with the necessary support mechanisms is called a *public-key infrastructure*, usually referred to as *PKI*.

Certificate

- In practice, certificates not only include the ID and the public key of a user, they tend to be quite complex structures with many additional fields. As an example, we look at the a X.509 certificate in Fig. 13.4. X.509 is an important standard for network authentication services, and the corresponding certificates are widely used for Internet communication.



Serial Number

Certificate Algorithm:
- Algorithm
- Parameters

Issuer

Period of Validity:
- Not Before Date
- Not After Date

Subject

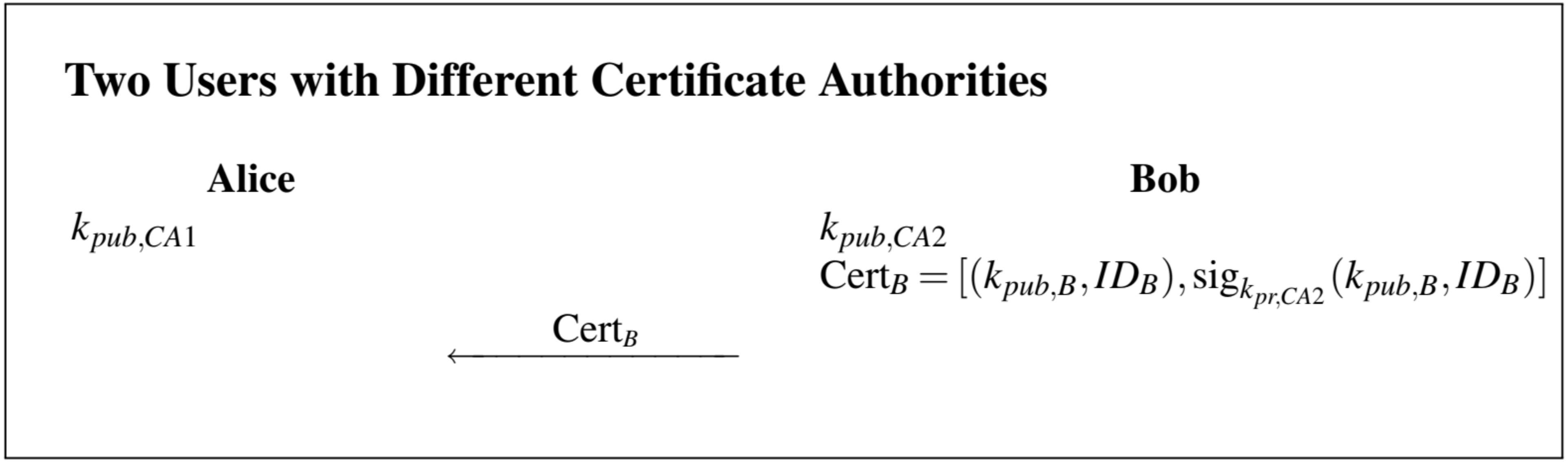
Subject’s Public Key:
- Algorithm
- Parameters
- Public Key

Signature

Fig. 13.4 Detailed structure of an X.509 certificate

public-key infrastructure

Let's look at an example where Alice's certificate is issued by CA1 and Bob's by CA2. At the moment, Alice is only in possession of the public key of "her" CA1, and Bob has only $k_{pub,CA2}$. If Bob sends his certificate to Alice, she cannot verify Bob's public key. This situation looks like this:



Two Users with Different Certificate Authorities

Alice | **Bob**

$k_{pub,CA1}$

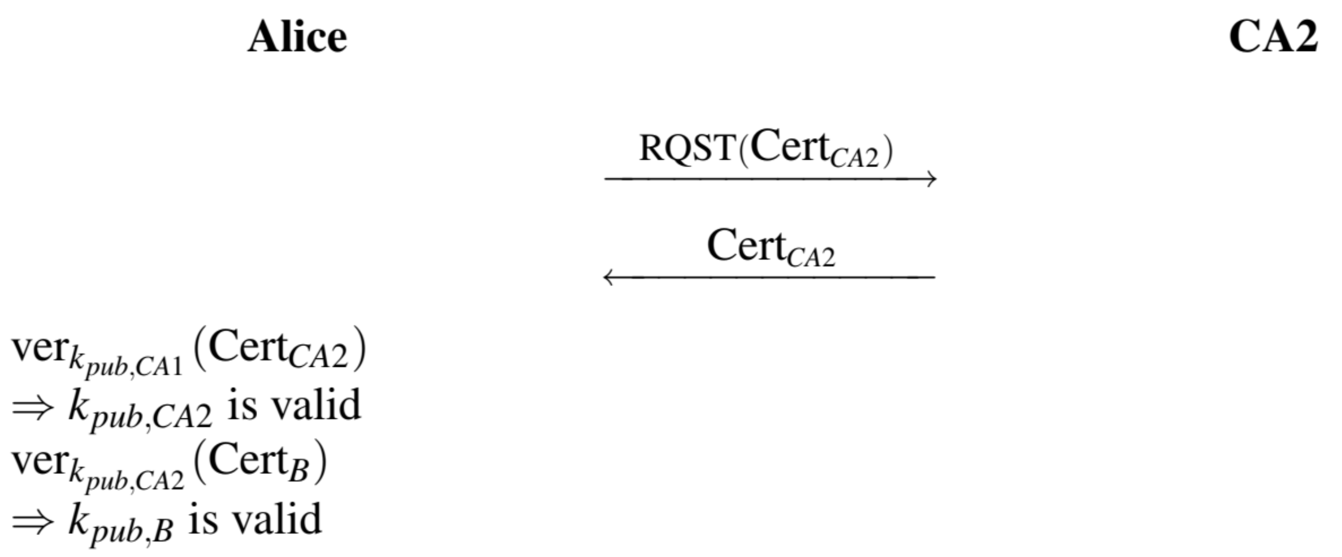
$k_{pub,CA2}$

$\mathrm{Cert}_B = [(k_{pub,B}, ID_B), \mathrm{sig}_{k_{pr,CA2}}(k_{pub,B}, ID_B)]$

$\xleftarrow{\quad\mathrm{Cert}_B\quad}$

Alice can now request CA2's public key, which is itself contained in a certificate that was signed by Alice's CA1:

Verification of a CA Public Key

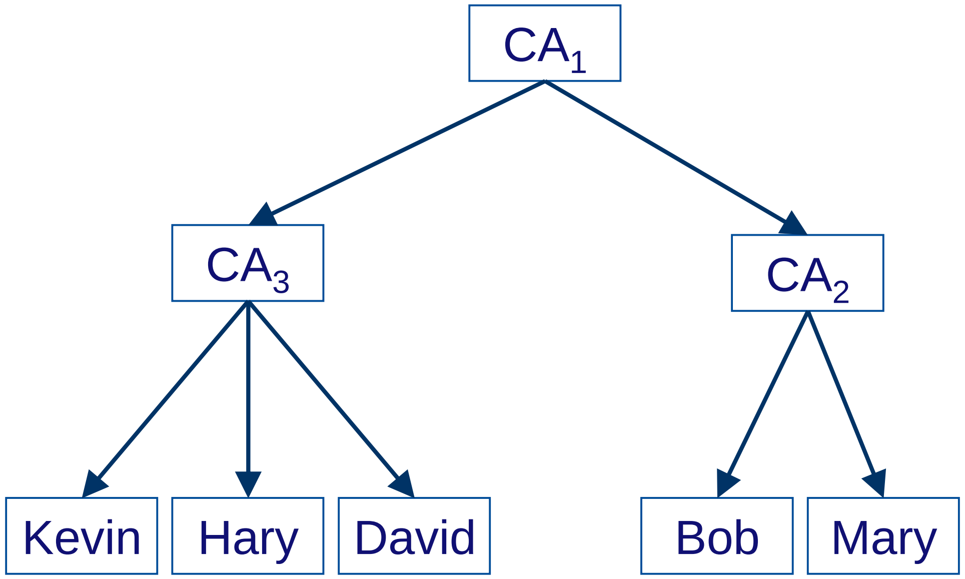


$\mathrm{ver}_{k_{pub,CA1}}(\mathrm{Cert}_{CA2})$
$\Rightarrow k_{pub,CA2}$ is valid
$\mathrm{ver}_{k_{pub,CA2}}(\mathrm{Cert}_{B})$
$\Rightarrow k_{pub,B}$ is valid

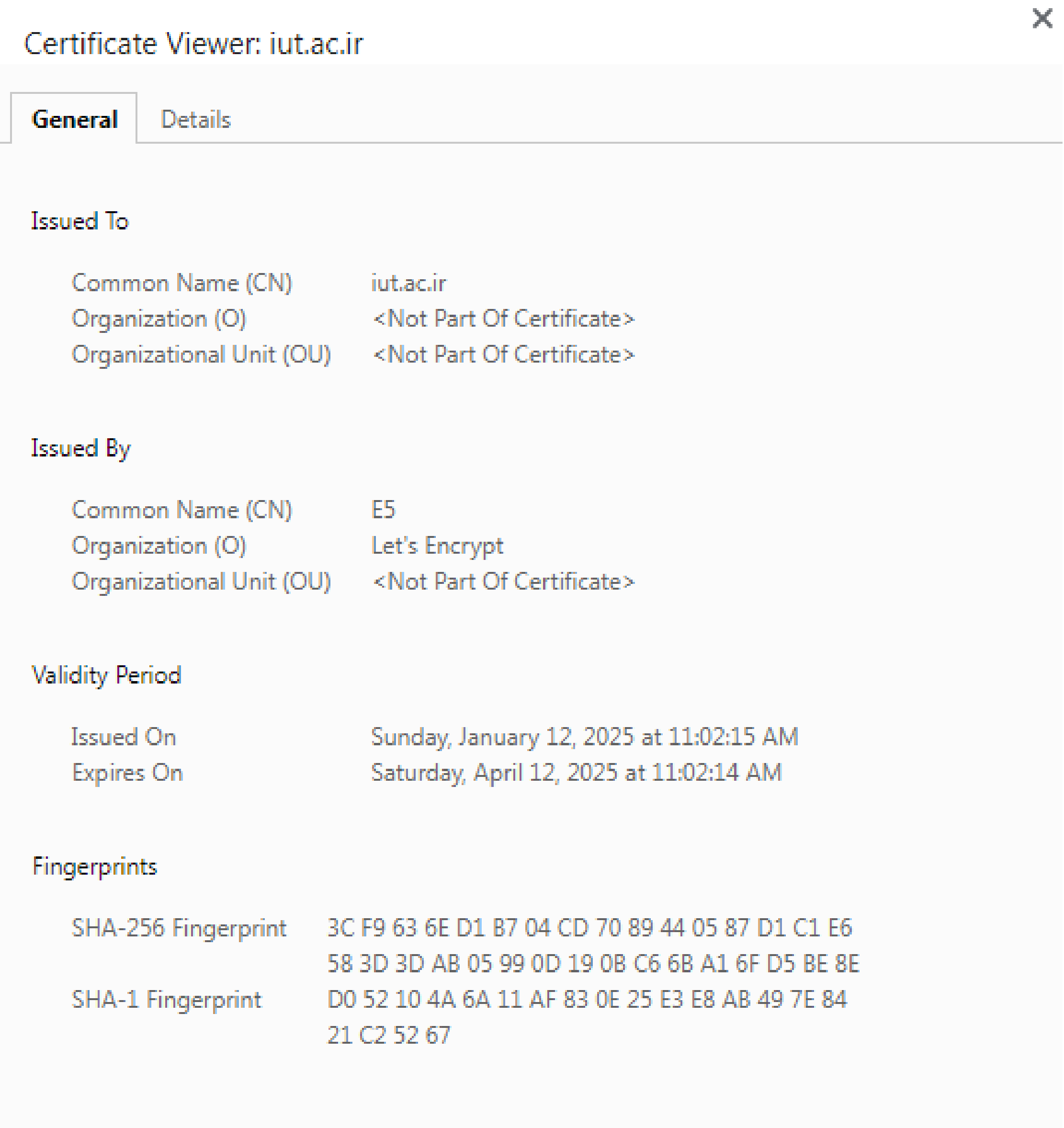
The structure Cert_{CA2} contains the public key of CA2 signed by CA1, which looks like this:

$$\mathrm{Cert}_{CA2} = [(k_{pub,CA2}, ID_{CA2}), \mathrm{sig}_{k_{pr,CA1}}(k_{pub,CA2}, ID_{CA2})]$$

Certificate



Certificate



Certificate Viewer: iut.ac.ir

Issued To

Common Name (CN)	iut.ac.ir
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

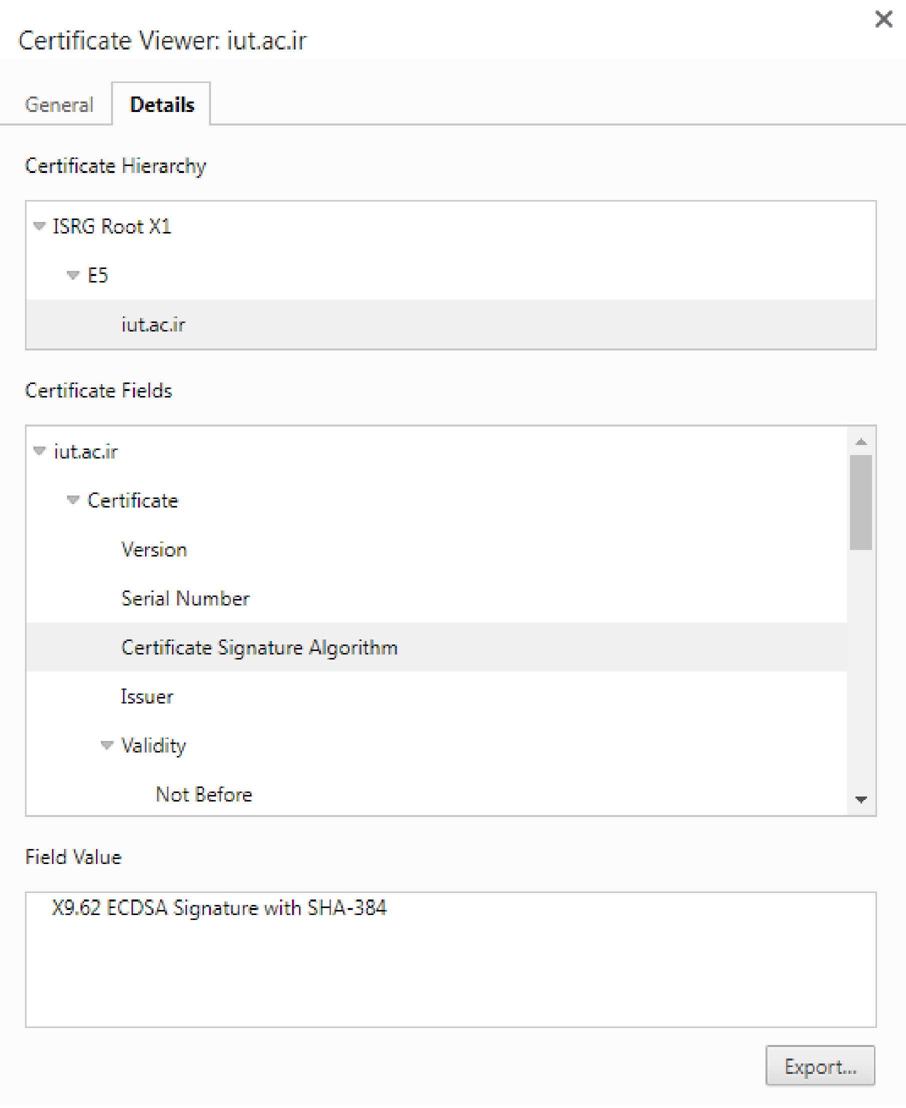
Common Name (CN)	E5
Organization (O)	Let's Encrypt
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period

Issued On	Sunday, January 12, 2025 at 11:02:15 AM
Expires On	Saturday, April 12, 2025 at 11:02:14 AM

Fingerprints

SHA-256 Fingerprint	3C F9 63 6E D1 B7 04 CD 70 89 44 05 87 D1 C1 E6 58 3D 3D AB 05 99 0D 19 0B C6 6B A1 6F D5 BE 8E
SHA-1 Fingerprint	D0 52 10 4A 6A 11 AF 83 0E 25 E3 E8 AB 49 7E 84 21 C2 52 67



Certificate Viewer: iut.ac.ir

Certificate Hierarchy

```
▾ ISRG Root X1
    ▾ E5
        iut.ac.ir
```

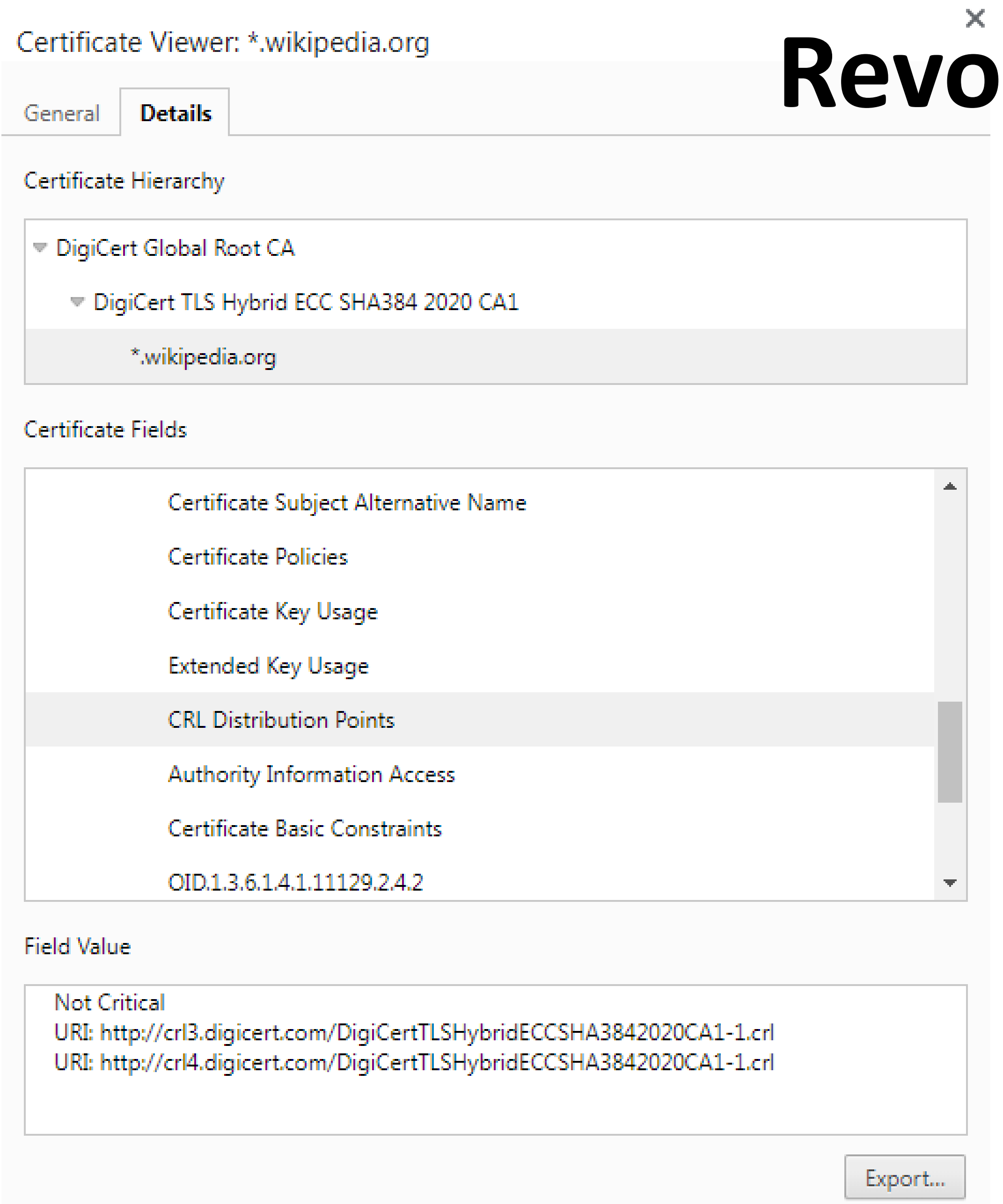
Certificate Fields

```
▾ iut.ac.ir
    ▾ Certificate
        Version
        Serial Number
        Certificate Signature Algorithm
        Issuer
        ▾ Validity
            Not Before
```

Field Value

X9.62 ECDSA Signature with SHA-384

Revocation



Certificate Viewer: *.wikipedia.org

Certificate Hierarchy

- DigiCert Global Root CA
  - DigiCert TLS Hybrid ECC SHA384 2020 CA1
    - *.wikipedia.org

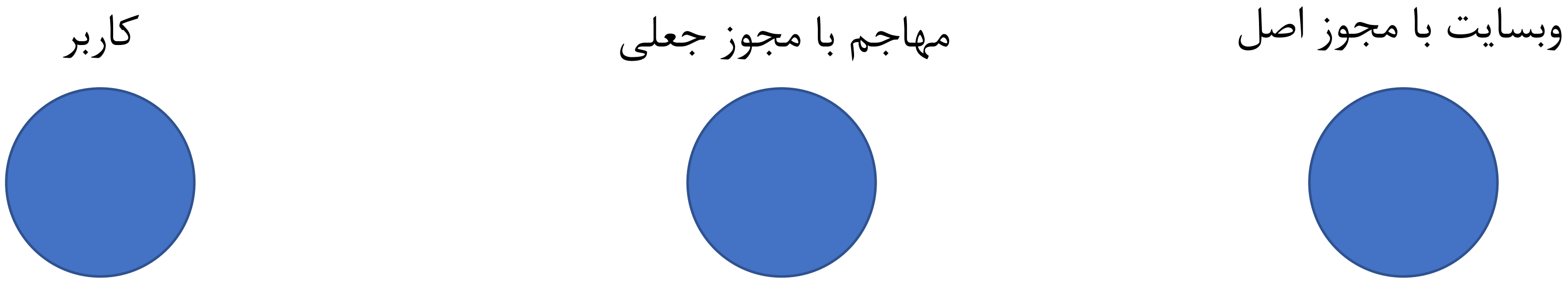
Certificate Fields

- Certificate Subject Alternative Name
- Certificate Policies
- Certificate Key Usage
- Extended Key Usage
- CRL Distribution Points
- Authority Information Access
- Certificate Basic Constraints
- OID.1.3.6.1.4.1.11129.2.4.2

Field Value

```
Not Critical
URI: http://crl3.digicert.com/DigiCertTLSHybridECCSHA3842020CA1-1.crl
URI: http://crl4.digicert.com/DigiCertTLSHybridECCSHA3842020CA1-1.crl
```

MITM



وبسایت با مجوز اصل

مهاجم با مجوز جعلی

کاربر

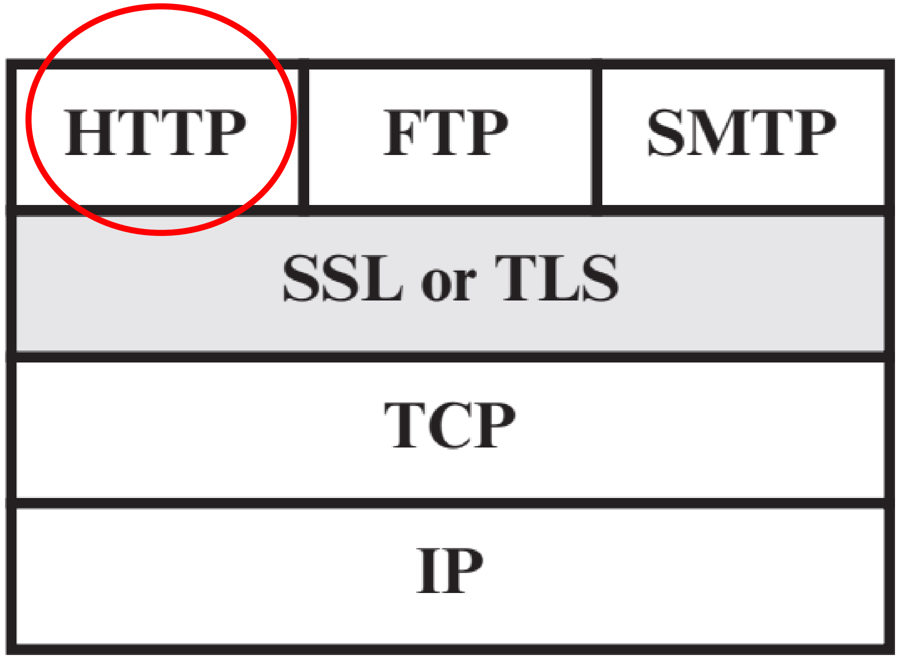
What is TLS/SSL?

- SSL is the protocol used for majority of secure Internet transactions today
- For example, if you want to buy a book at amazon.com…
  - You want to be sure you are dealing with Amazon (**authentication**)
  - Your credit card information must be protected when sent (**confidentiality** and **integrity**)
  - As long as you have money, Amazon does not really care who you are…
  - …so, no need for mutual authentication

TLS/SSL

- Secure Socket Layer (SSL)
- Transport Layer Security (TLS)

HTTP (**Hypertext Transfer Protocol**) is an application layer protocol in the Internet protocol suite model for distributed, collaborative, hypermedia information systems.

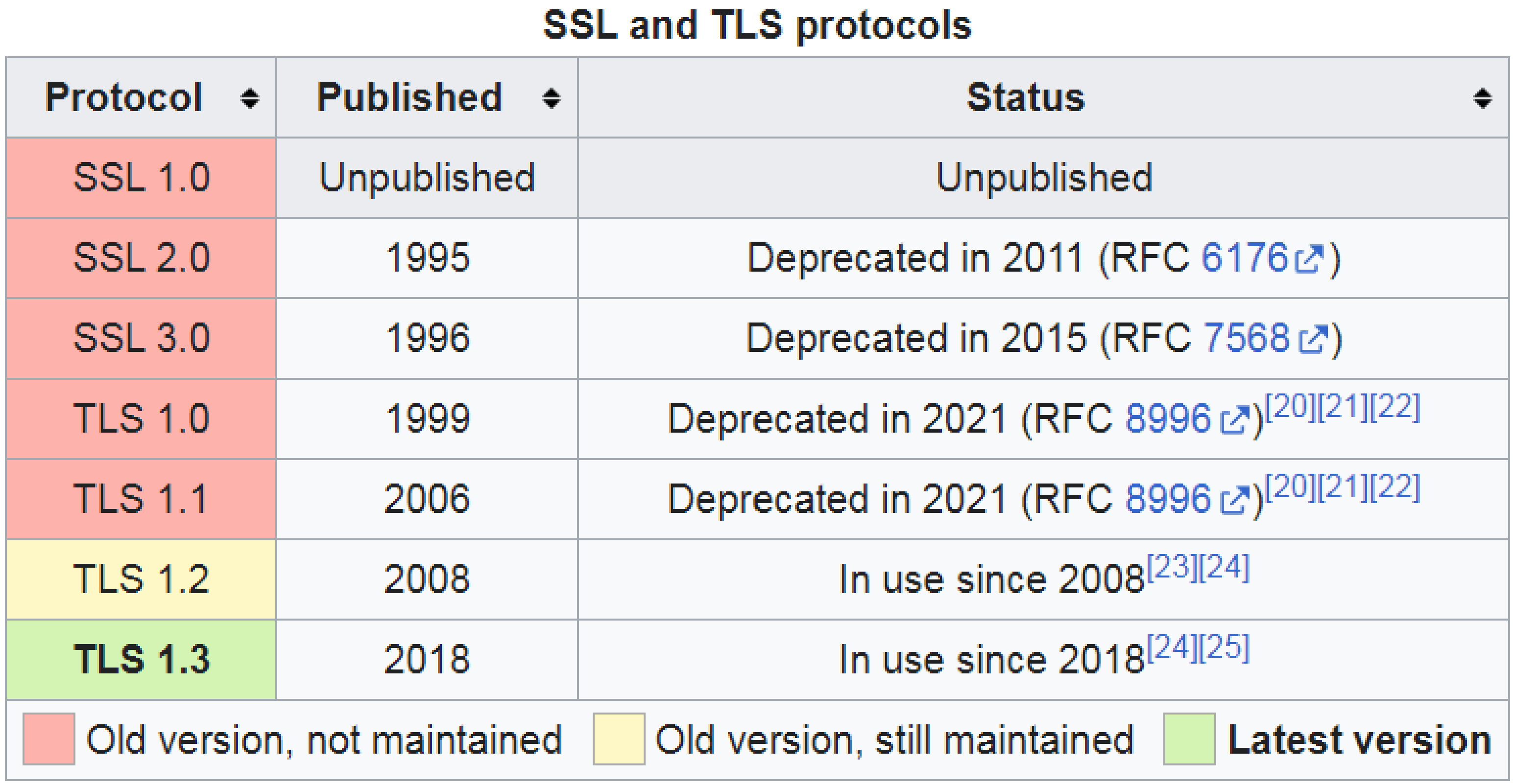


HTTPS

- Hypertext Transfer Protocol Secure (HTTPS) is an extension of the Hypertext Transfer Protocol (HTTP). It uses encryption for secure communication over a computer network, and is widely used on the Internet. In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS) or, formerly, Secure Sockets Layer (SSL). The protocol is therefore also referred to as HTTP over TLS, or HTTP over SSL.

TLS/SSL

- Secure Socket Layer (SSL)
- Transport Layer Security (TLS)



SSL and TLS protocols

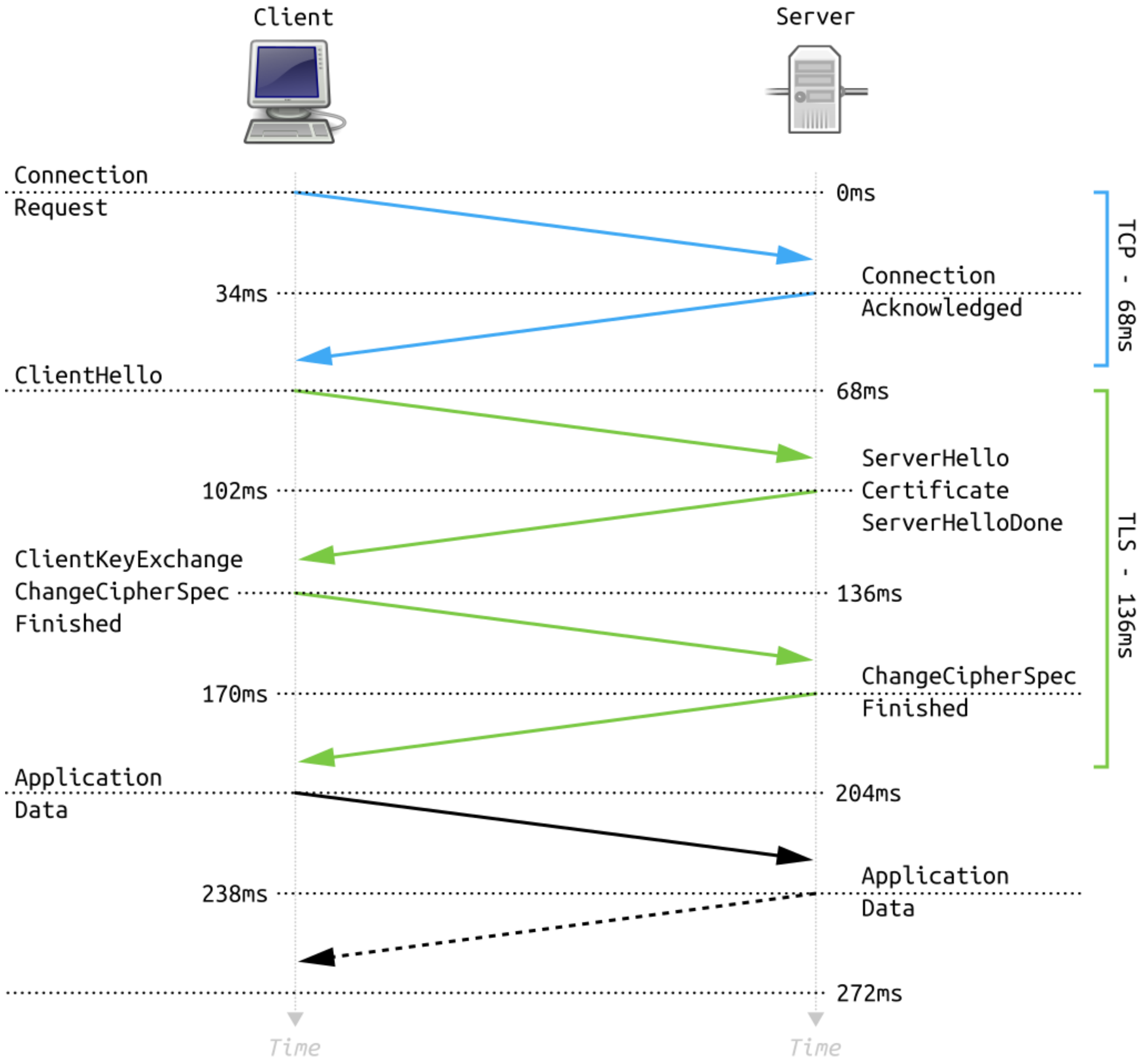
Protocol	Published	Status
SSL 1.0	Unpublished	Unpublished
SSL 2.0	1995	Deprecated in 2011 (RFC 6176)
SSL 3.0	1996	Deprecated in 2015 (RFC 7568)
TLS 1.0	1999	Deprecated in 2021 (RFC 8996)[20][21][22]
TLS 1.1	2006	Deprecated in 2021 (RFC 8996)[20][21][22]
TLS 1.2	2008	In use since 2008[23][24]
TLS 1.3	2018	In use since 2018[24][25]

🟥 Old version, not maintained 🟨 Old version, still maintained 🟩 **Latest version**

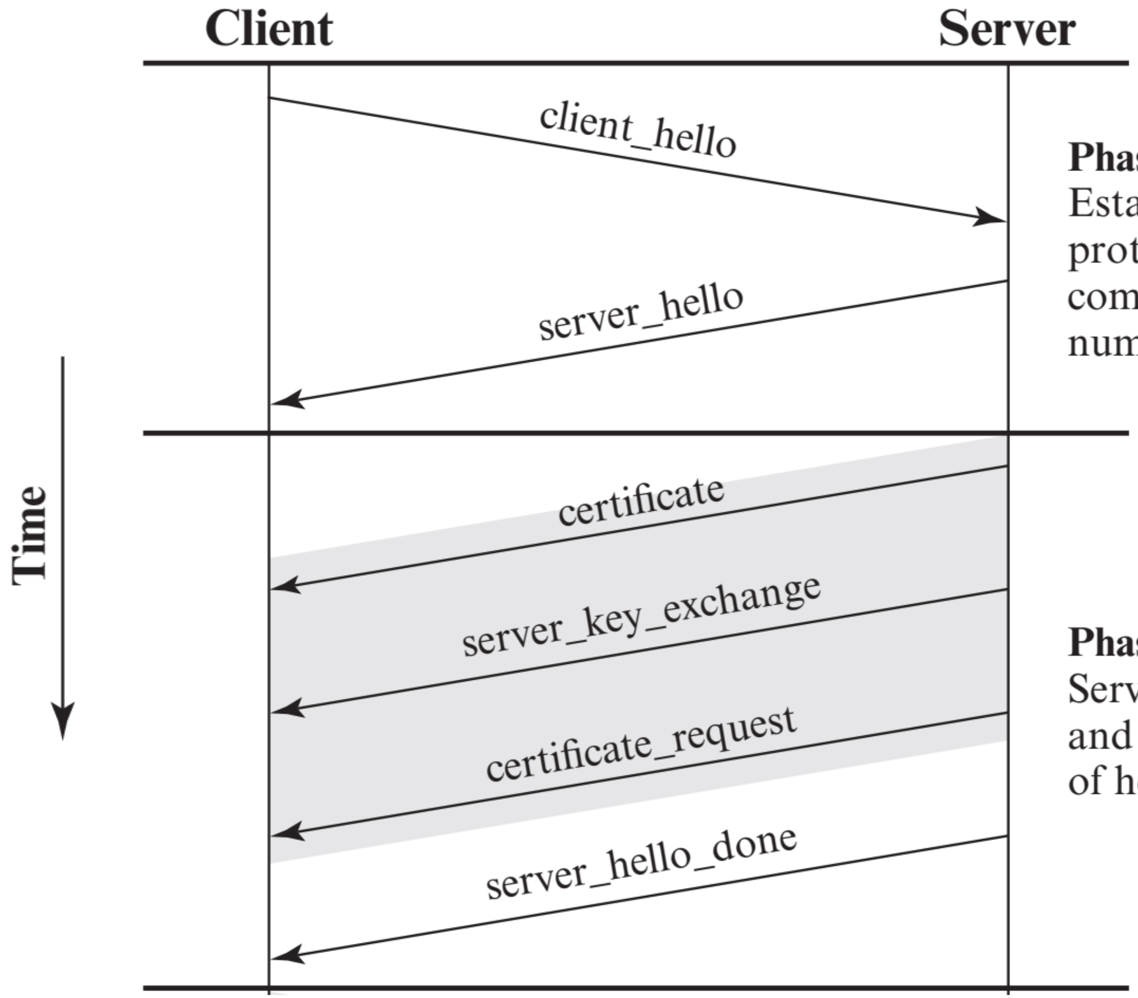
TLS

- پروتکل های موجود در TLS:
  - ❑ Handshake: احراز اصالت و ایجاد کلید
  - ❑ Record: انتقال داده (رمز شده و MAC)
  - ❑ Alert: هشدار به طرف مقابل در صورت بروز خطا

TLS handshake



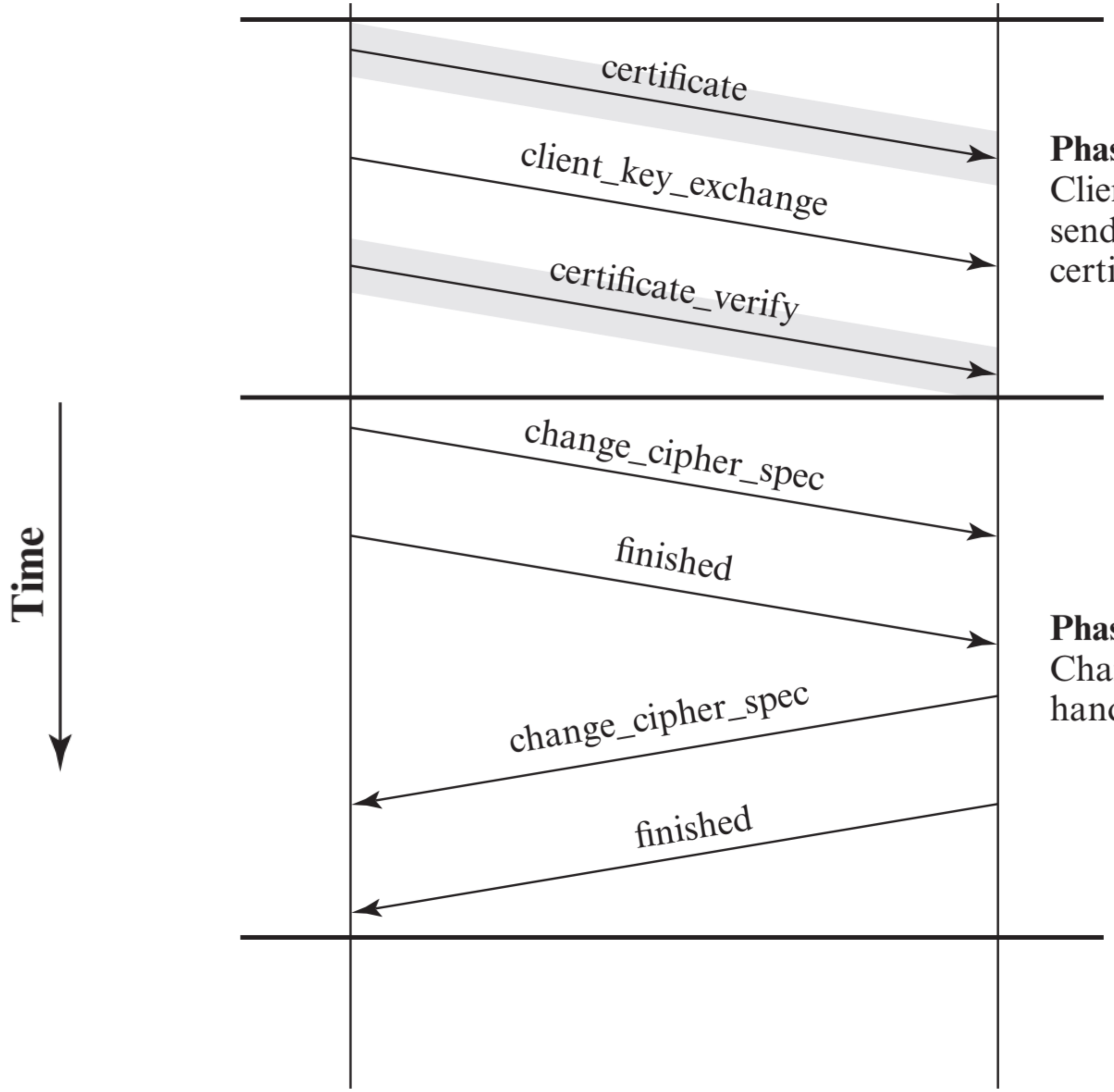
TLS handshake



Phase 1
Establish security capabilities, including protocol version, session ID, cipher suite, compression method, and initial random numbers.

Phase 2
Server may send certificate, key exchange, and request certificate. Server signals end of hello message phase.

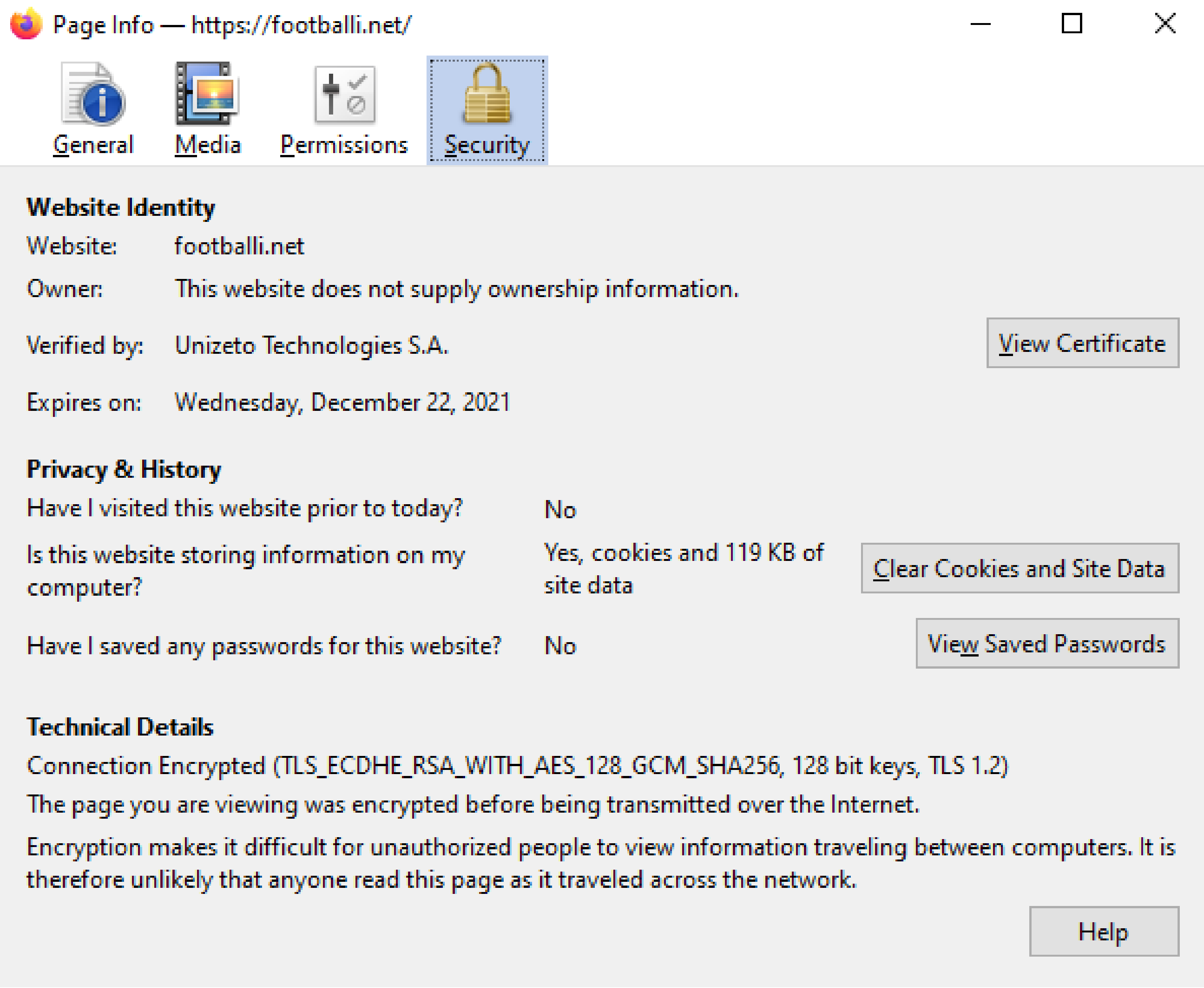
TLS handshake



Phase 3
Client sends certificate if requested. Client sends key exchange. Client may send certificate verification.

Phase 4
Change cipher suite and finish handshake protocol.

Note: Shaded transfers are optional or situation-dependent messages that are not always sent.



Page Info — https://footballi.net/

Website Identity

Website: footballi.net

Owner: This website does not supply ownership information.

Verified by: Unizeto Technologies S.A.

Expires on: Wednesday, December 22, 2021

Privacy & History

Have I visited this website prior to today? No

Is this website storing information on my computer? Yes, cookies and 119 KB of site data

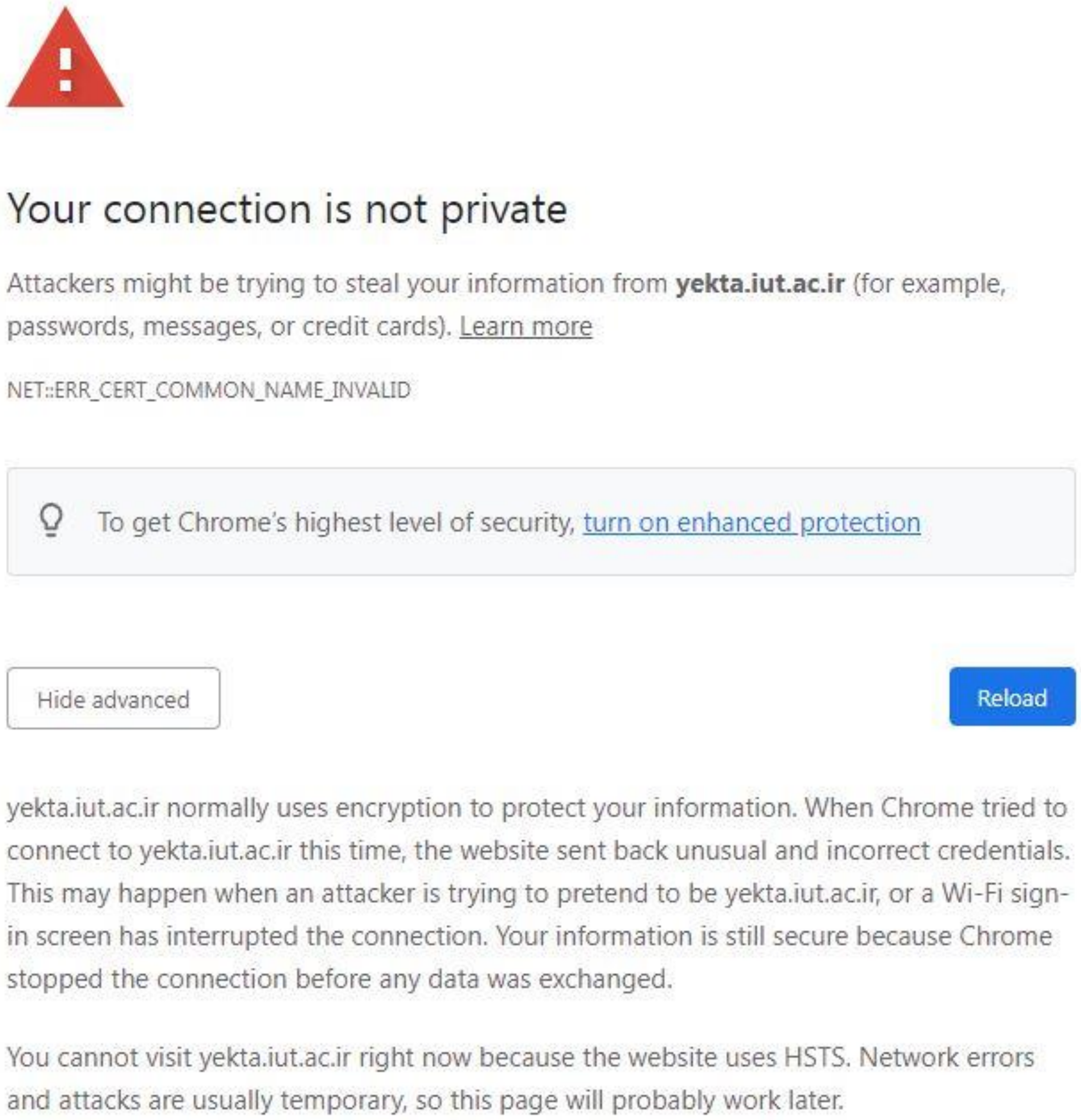
Have I saved any passwords for this website? No

Technical Details

Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128 bit keys, TLS 1.2)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.



Your connection is not private

Attackers might be trying to steal your information from **yekta.iut.ac.ir** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_COMMON_NAME_INVALID

To get Chrome's highest level of security, turn on enhanced protection

yekta.iut.ac.ir normally uses encryption to protect your information. When Chrome tried to connect to yekta.iut.ac.ir this time, the website sent back unusual and incorrect credentials. This may happen when an attacker is trying to pretend to be yekta.iut.ac.ir, or a Wi-Fi sign-in screen has interrupted the connection. Your information is still secure because Chrome stopped the connection before any data was exchanged.

You cannot visit yekta.iut.ac.ir right now because the website uses HSTS. Network errors and attacks are usually temporary, so this page will probably work later.

TLS Record

IUT-ECE

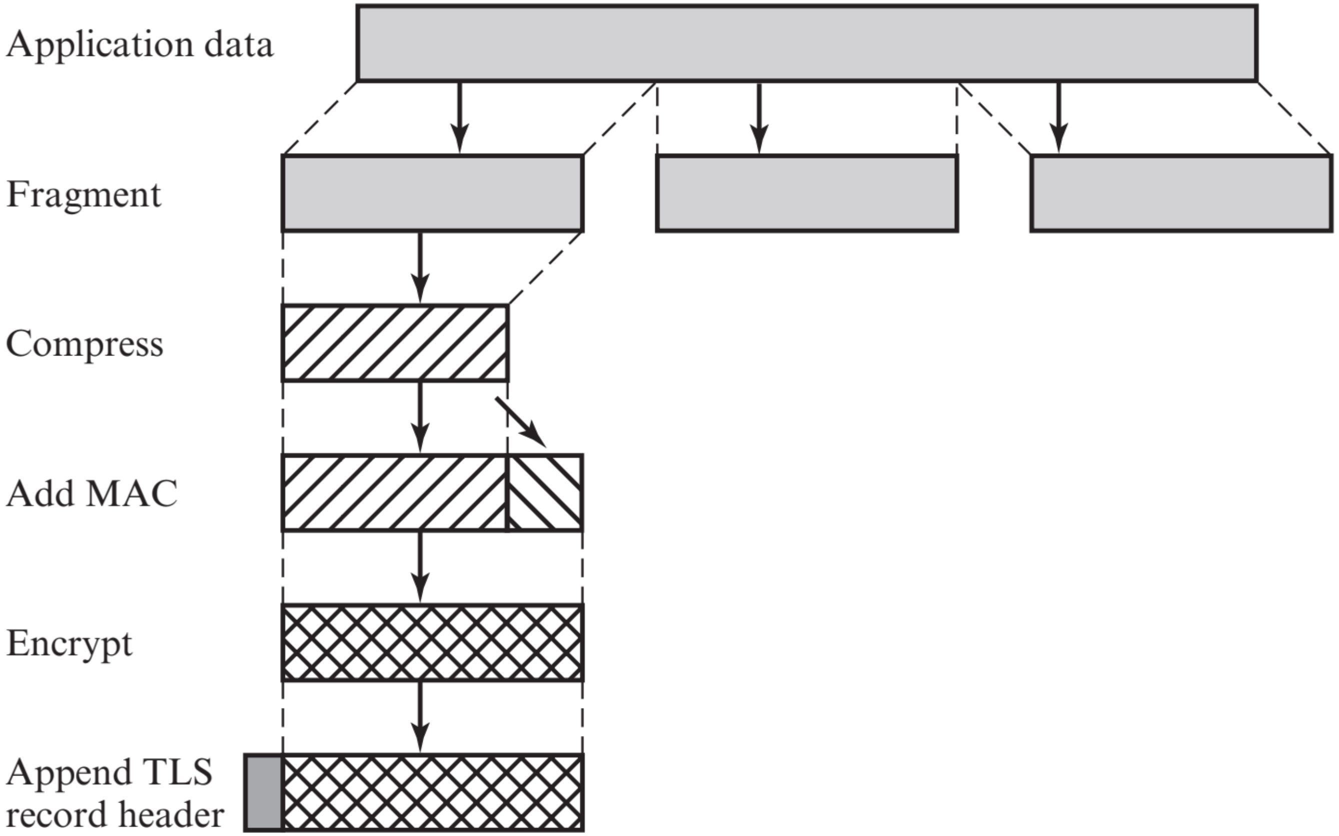


Figure 6.3 TLS Record Protocol Operation

TLS Record

- ❑ قطعه بندی: تولید قطعاتی به طول محدود.
- ❑ فشرده سازی: اختیاری و بدون از دست دادن داده.
- ❑ تولید MAC: اضافه کردن آن به داده
- ❑ رمزگذاری: استفاده از رمز قطعه ای در یک مد
- ❑ اضافه کردن سرآیند: اضافه کردن به ابتدای قطعه رمز شده.
  - ▪ نوع محتوا، طول داده فشرده شده و...

TLS 1.3

- حذف تبادل کلید RSA.

- رمز handshake پس از توافق روی کلید.