

# Information Security

## CS3002

Lecture 19  
2nd November 2023

Dr. Rana Asif Rehman  
Email: [r.asif@lhr.nu.edu.pk](mailto:r.asif@lhr.nu.edu.pk)



# Secure Socket Layer (SSL)



# SSL what is it?

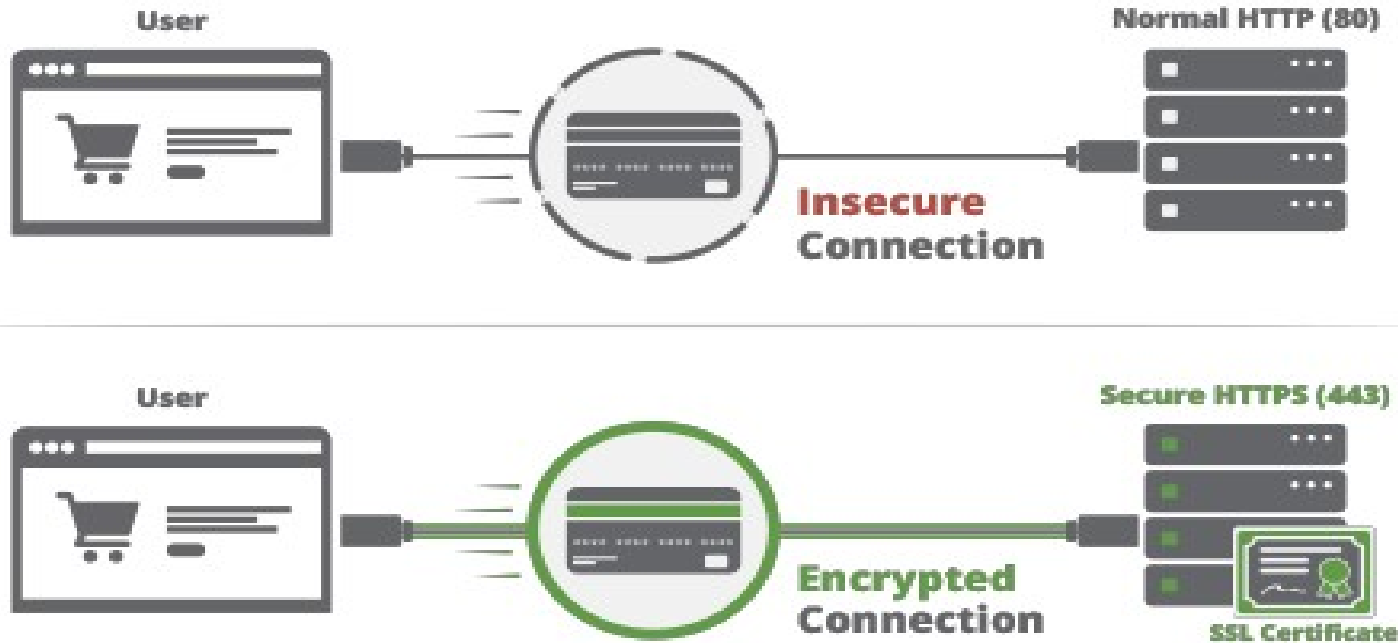


- Security at layer 4 (Transport layer)
- **Secure Sockets Layer (SSL)**
- Secure transport channel (session level):
  - peer authentication (server, server + client)
  - message confidentiality
  - message authentication and integrity
  - protection against replay attacks
- Easily applicable to all protocols based on TCP:
  - HTTP, SMTP, FTP, TELNET, ...
  - e.g. the famous secure HTTP ([https://....](https://...)) = 443/TCP

# SSL/TLS



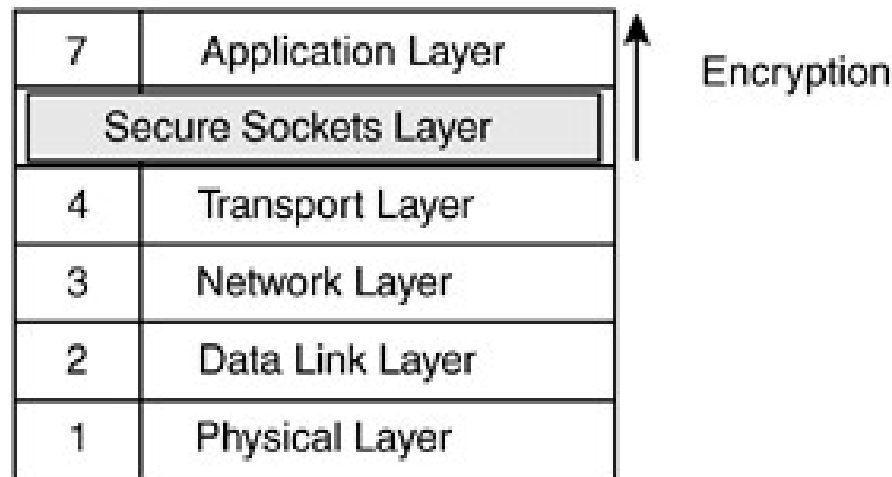
## HTTP VS HTTPS



# SSL/TLS



- Philosophy of SSL: Easier to deploy something if no changes in OS required
- Application's API (Socket) is interface to SSL: Hence secure socket layer
- API to SSL is the superset of API to TCP
- SSL/TLS operate above TCP. OS doesn't change applications do!



# SSL Certificate

An SSL certificate is a data file hosted in a website's origin server.

## SSL certificates include:

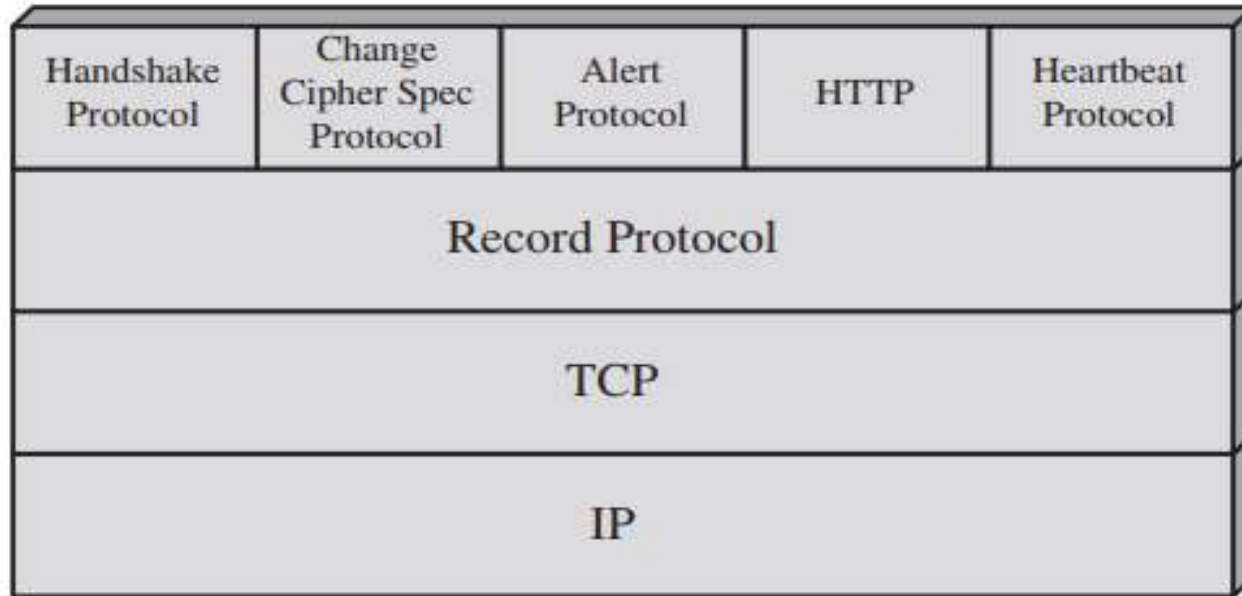
- The domain name that the certificate was issued for
- Which person, organization, or device it was issued to
- Which certificate authority issued it
- The certificate authority's **digital signature**
- Associated subdomains
- Issue date of the certificate
- Expiration date of the certificate
- The public key  
(the private key is kept secret)



# SSL/TLS



# SSL V3 Architecture



- Handshake: enables the SSL or TLS client and server to establish the secret keys with which they communicate
- Change cipher spec: indicates the usage of secret key for data communication
- Alert: signal problems with SSL connection, give current status
- Record protocol: permits the encapsulation of higher level protocols

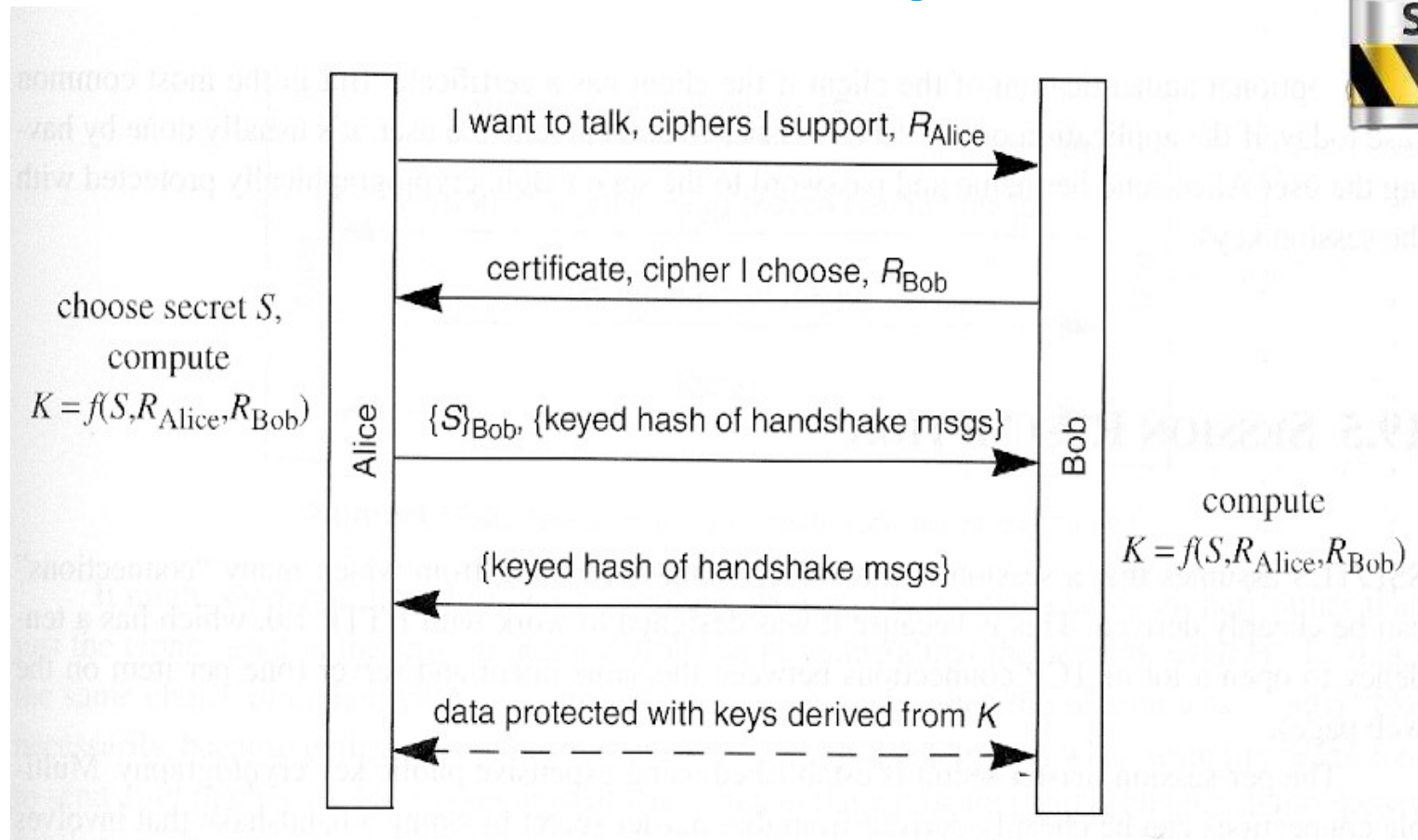


# SSL Handshake



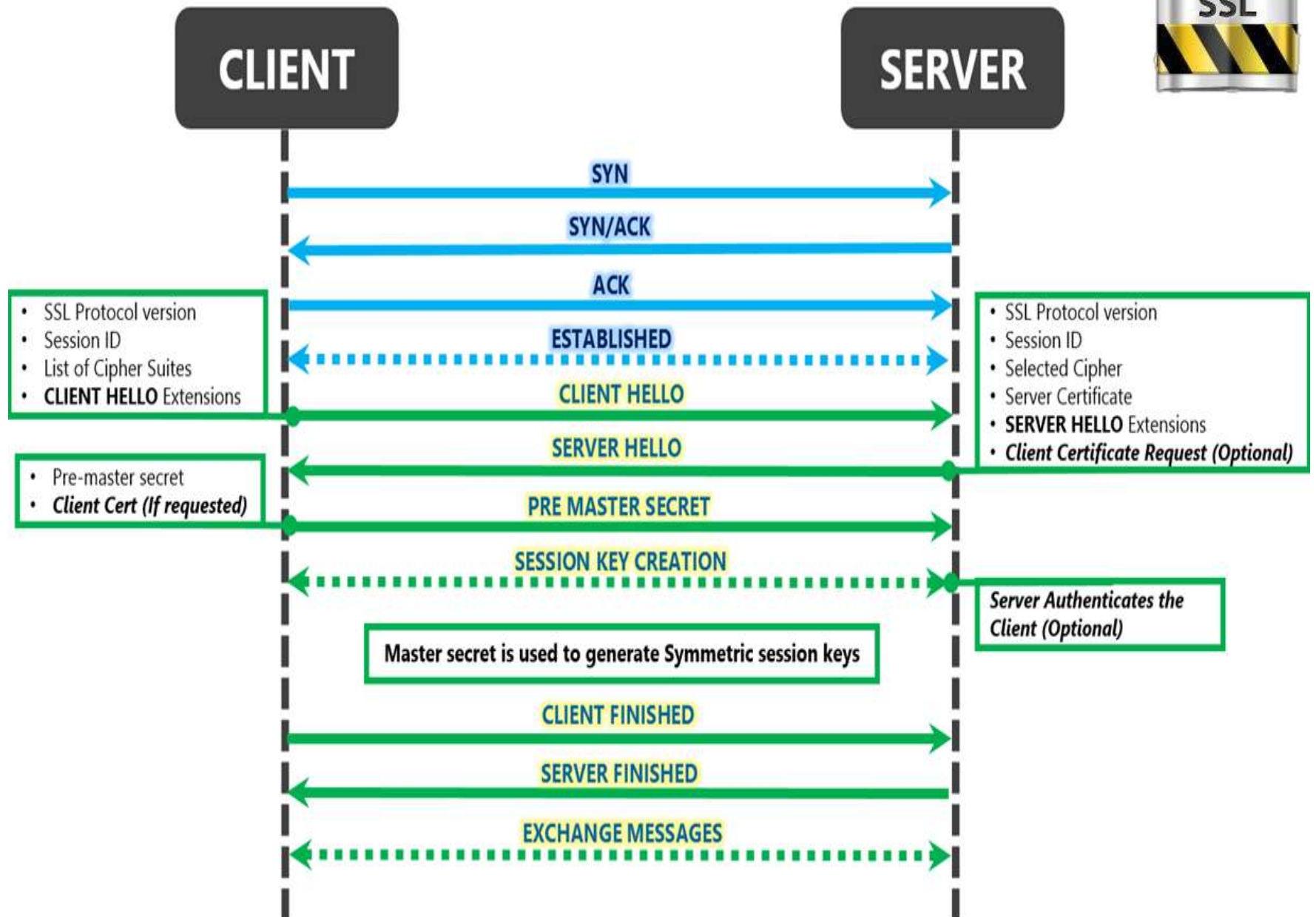
- Agree on a set of algorithms for confidentiality, integrity and authentication
- Exchange random numbers between the client and the server to be used for the subsequent generation of the keys
- Establish a symmetric key by means of public key operations, e.g. RSA
- Negotiate the session-id
- Exchange the necessary certificates

# SSL Handshake Simplified



- Secrets are: Pre-master key  $S$ , Master Key  $K$
- Server authentication
- Client authentication by password (optional)

# SSL Handshake in Detail

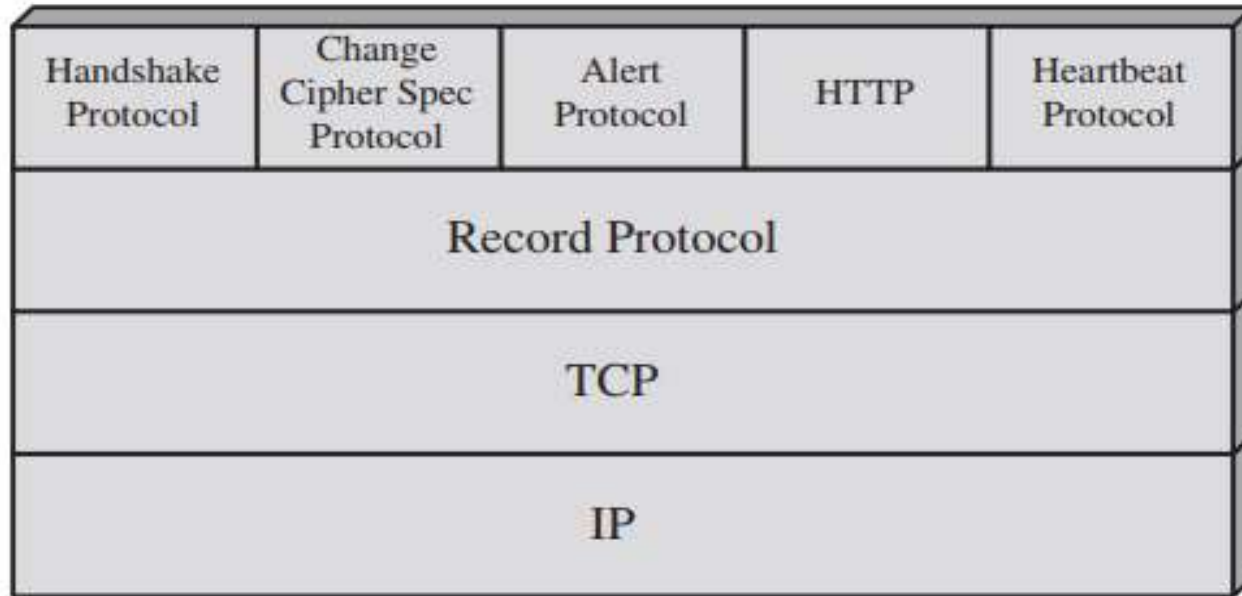


# Key Terms



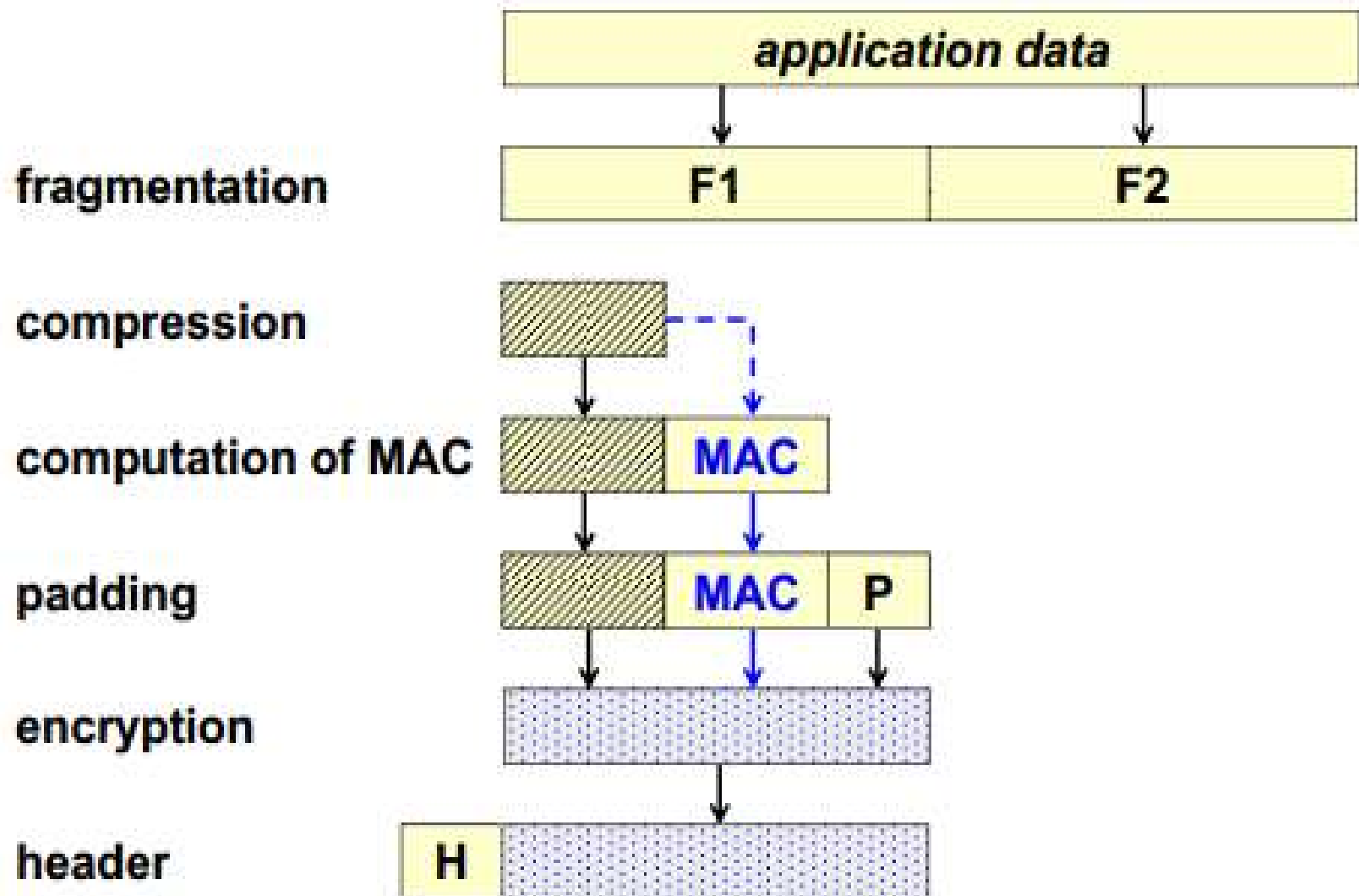
- HELLO Extensions: request extended functionality by sending data in the extensions field.
  - E.g: max\_fragment\_length, status request
  - The server may not oblige
  - Client may abort the handshake
- Pre-shared Secret (key): generated by client OR directly obtained from the key exchange. E.g: (DH:  $g^{ab} \bmod p$ )
- Master keys: generated from the pre-shared secret + random.client + random.server by applying a PRF
- Master key = PRF (pre-shared secret, random.client, random.server)
- PRF = Pseudo Random Function

# SSL V3 Architecture



- Handshake: enables the SSL or TLS client and server to establish the secret keys with which they communicate
- Change cipher spec: indicates the usage of secret key for data communication
- Alert: signal problems with SSL connection, give current status
- Record protocol: permits the encapsulation of higher level protocols

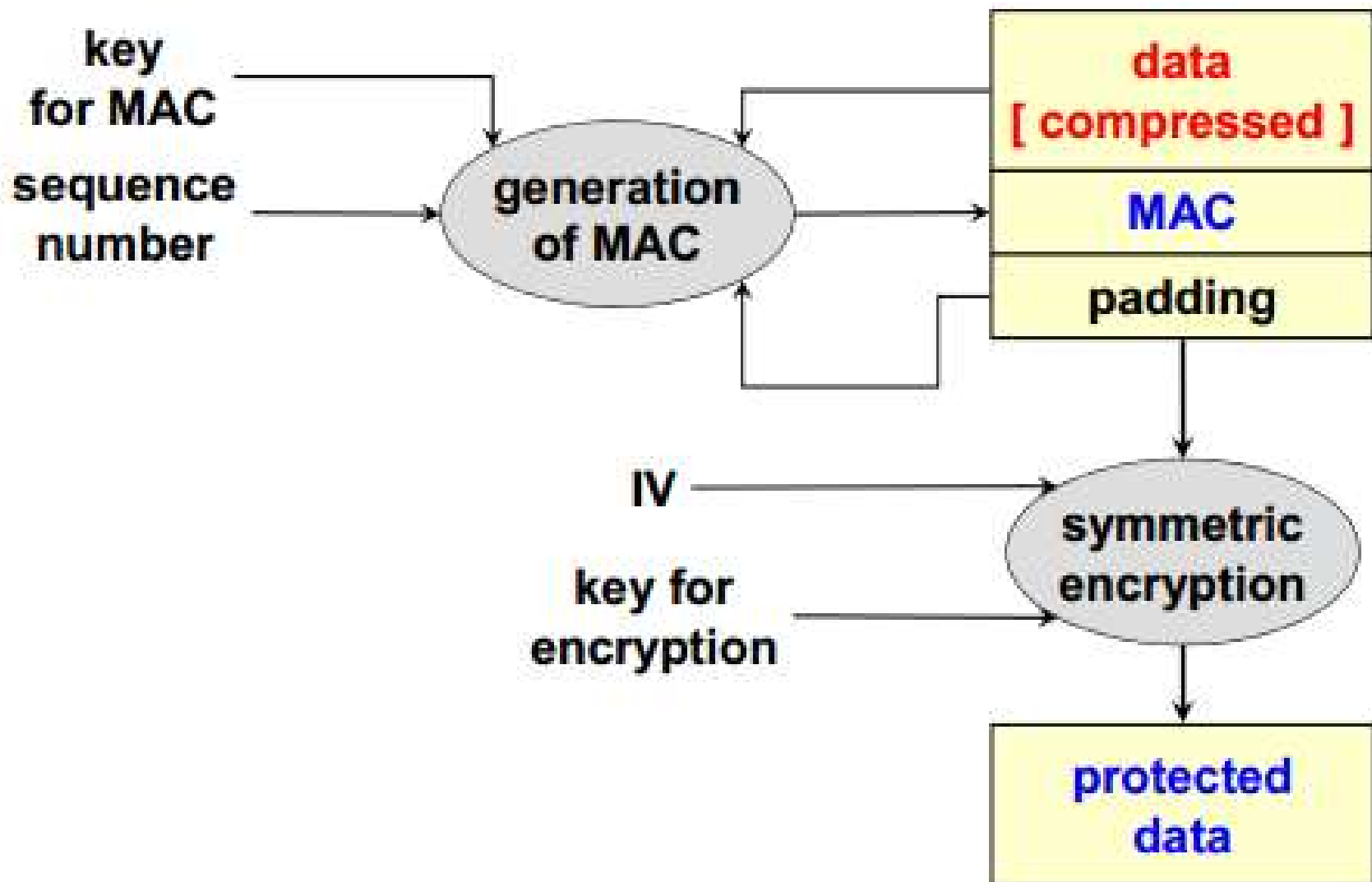
# SSL3/TLS Record Protocol



# SSL MAC Computation

- $MAC = \text{message\_digest} ( \text{key}, \text{seq\_number} \mid \text{type} \mid \text{version} \mid \text{length} \mid \text{fragment} )$
- `message_digest`
  - depends on the chosen algorithm
- `key`
  - sender-write-key or receiver-read-key
- `seq_number`
  - 32-bit integer
- `Type`
  - Type of record
    - change cipher spec (20)
    - alert (21)
    - Handshake (22)
    - Application data (23)
- `length`
  - length of the fragment/plaintext

# Data Protection in SSL





## SSL-3 New Features with Respect to SSL-2

- data compression:
  - optional
  - Done before encryption
- data encryption is optional: in order to have only authentication and integrity
- possibility to re-negotiate the SSL connection:
  - periodical change of keys
  - change of the algorithms