Hybrid Encryption and SSL/TLS

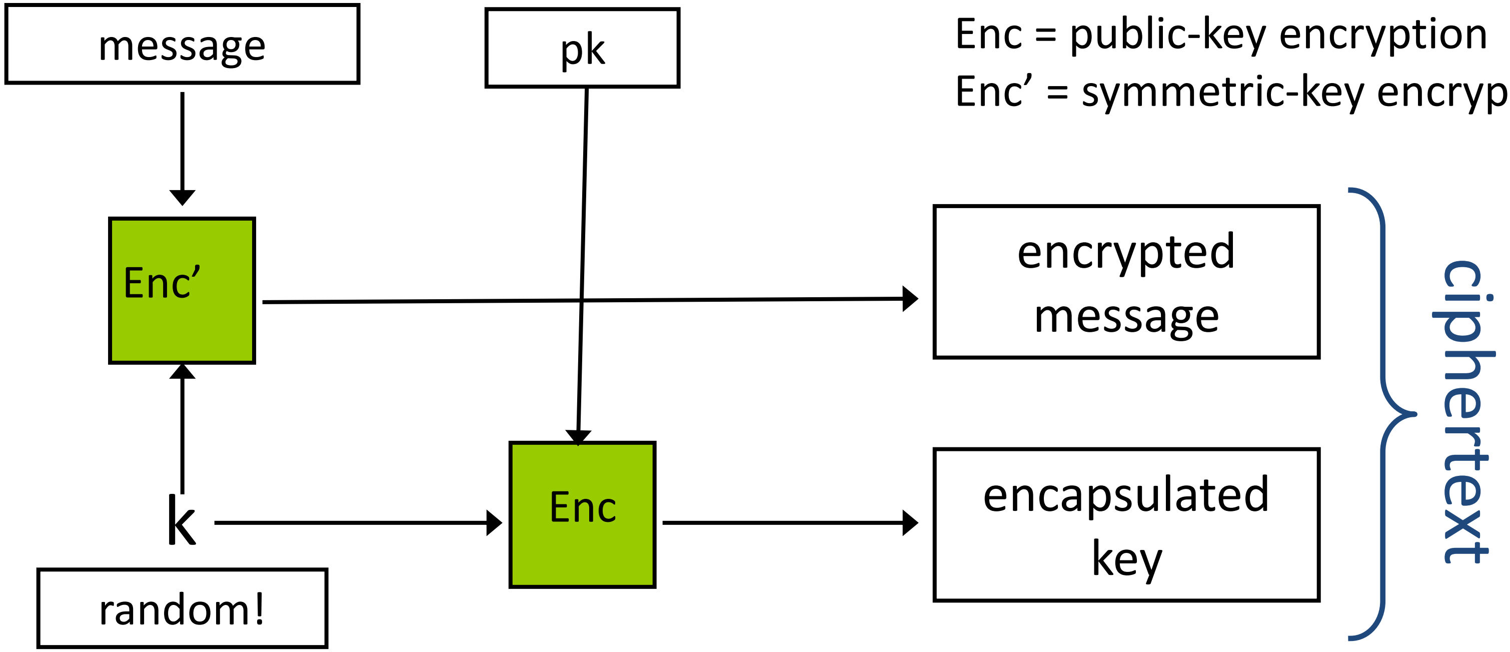
Dr. Chen Zhang

Department of Computer Science
The Hang Seng University of Hong Kong

Hybrid Encryption

- Problem of symmetric-key encryption & public-key encryption
  - Symmetric-key encryption:
    - Secure key exchange
  - Public-key encryption:
    - Slow in speed
- Hybrid encryption: combines the convenience of a public-key cryptosystem with the efficiency of a symmetric-key cryptosystem

Hybrid Encryption



Enc = public-key encryption
Enc' = symmetric-key encryption

- Think: How should hybrid encryption be done when sending the same message to multiple recipients?

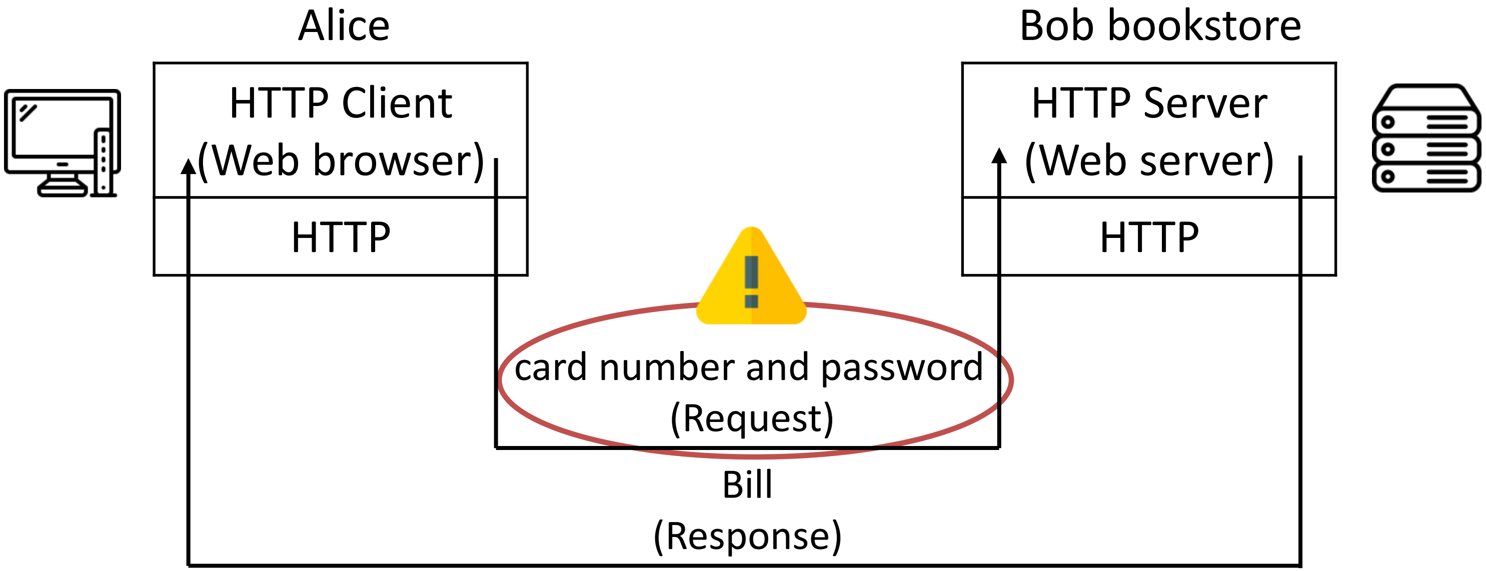
SSL/TLS – For Secure communication

- Scenario: Alice wants to buy a book from Bob bookstore’s online store. To complete the order, Alice needs to enter her card number and password.

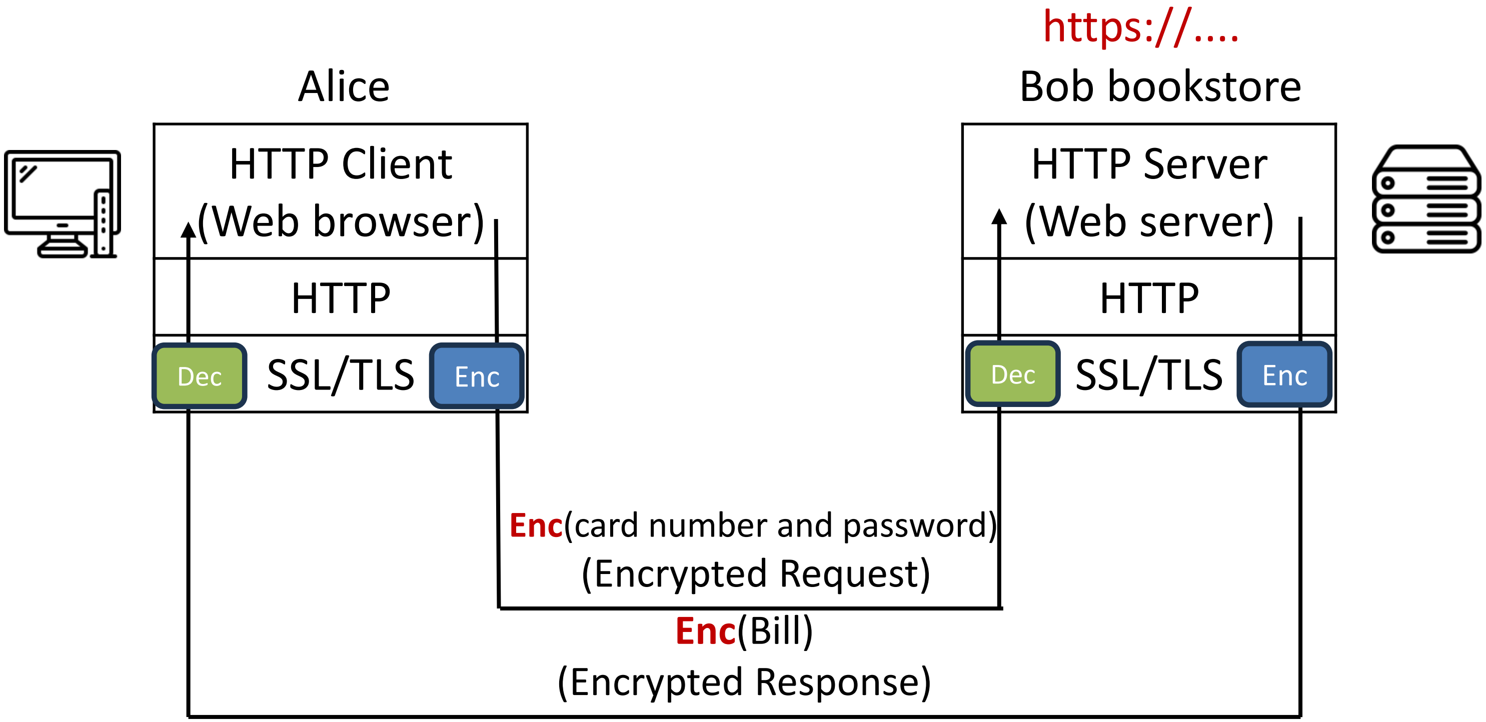
Alice is worried that her card number and password will be eavesdropped.

The communication between Alice and Bob bookstore without SSL/TLS

http://....



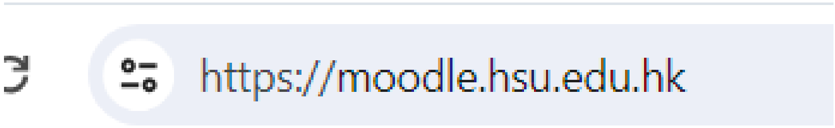
The communication between Alice and Bob bookstore without SSL/TLS



- Task of SSL/TLS:
  - The data cannot be eavesdropped when sent to Bob - **Confidentiality**
  - The data cannot be altered when sent to Bob - **Integrity**
  - Ensure the web server communicating with Alice is real Bob bookstore - **Authenticity**

SSL/TLS

- The tools can be used
  - Confidentiality: Hybrid encryption
  - Integrity: MAC
  - Authenticity: Digital signature



https://moodle.hsu.edu.hk

- SSL/TLS provides a **framework** for cryptographic communication. It establishes an encrypted connection between a client and a server, ensuring the confidentiality, integrity, and authenticity of the data transmitted.

- SSL/TLS can also be used to protect other protocols such as simple mail transfer protocol (SMTP), post office protocol (POP3)

Development of SSL/TLS

- SSL (Secure Socket Layer)
  - SSL 1.0
    - Internal Netscape design, early 1994
    - Lost in the mists of time
  - SSL 2.0
    - Published by Netscape, November 1994
  - SSL 3.0
    - Designed by Netscape and Paul Kocher, November 1996
- TLS (Transport Layer Security)
  - TLS 1.0
    - Internet standard based on SSL 3.0, 1999
    - Not interoperable with SSL 3.0
  - TLS 1.1
    - Add AES, 2006
  - TLS 1.2
    - Add HMAC-SHA256 and delete DES, 2008
  - TLS 1.3
    - Remove MD5 and SHA-1, 2018

TLS Basics

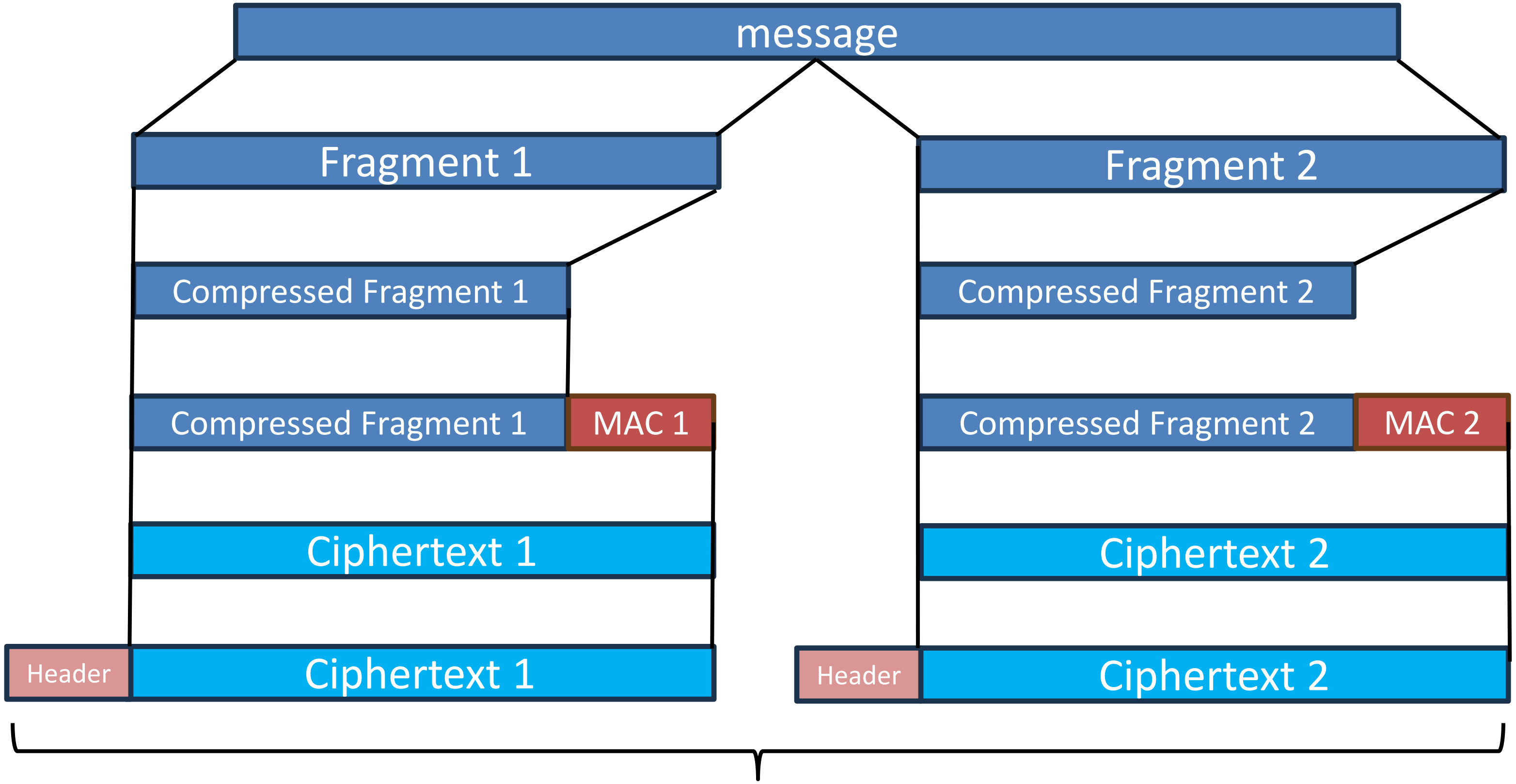
- TLS consists of two protocols
  - TLS Handshake protocol
    - Use public-key cryptography to establish a shared secret key between the client and the server
    - Exchange digital certificates for authentication (optional)
  - TLS Record protocol
    - Use the secret key established in the handshake protocol to protect communication between the client and the server

TLS Handshake Protocol

- Two parties: client and server
- Negotiate version of the protocol and the set of cryptographic algorithms to be used
- Authenticate client and server (optional)
  - Use digital certificates to learn each other’s public keys and verify each other’s identity
- Use public keys to establish a shared secret

TLS Record Protocol

- Response for message compression, encryption, and authentication



Message to be sent