CIS 658 Web Architectures

HTTP

Lecturer: Dr. Yong Zhuang

Based on the original version by Professor Hans Dulimarta.

Secure HTTP ➡ HTTPS

HTTPS

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

- PKI (Public Key Infrastructure)

HTTPS

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

- PKI (Public Key Infrastructure)

private key

public key

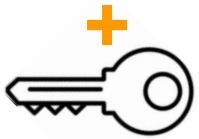
Encrypted Message (with public+private key pair)

Encrypted Message (with public+private key pair)

Client

Server

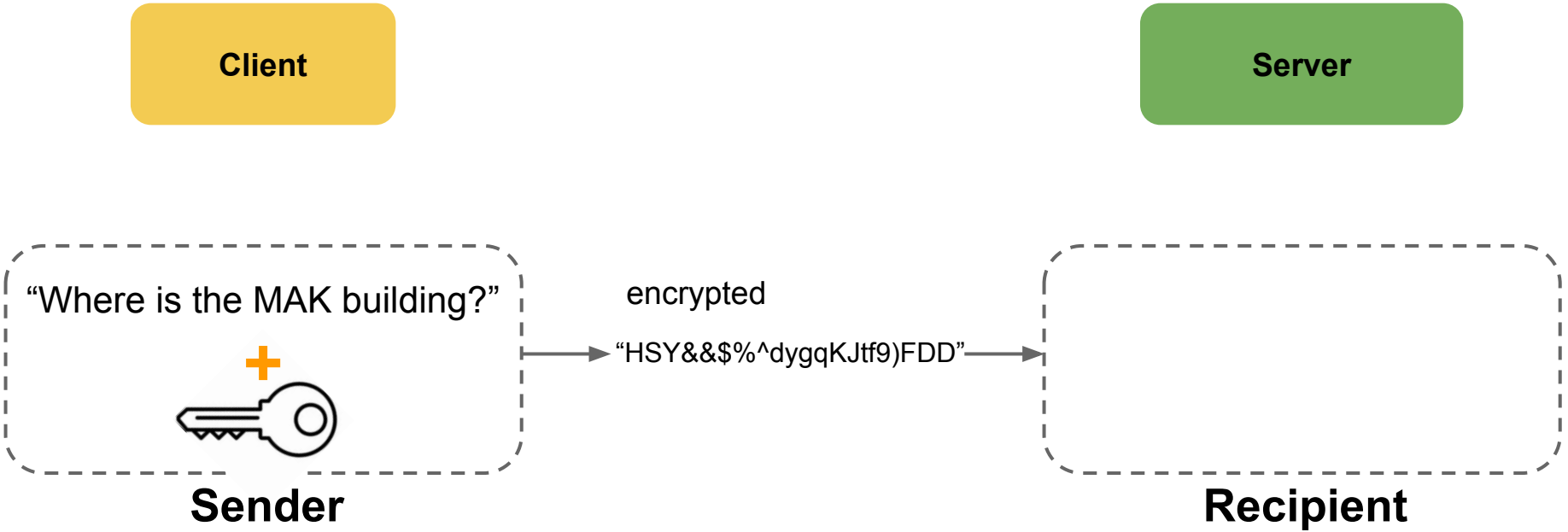
"Where is the MAK building?"



Sender

Recipient

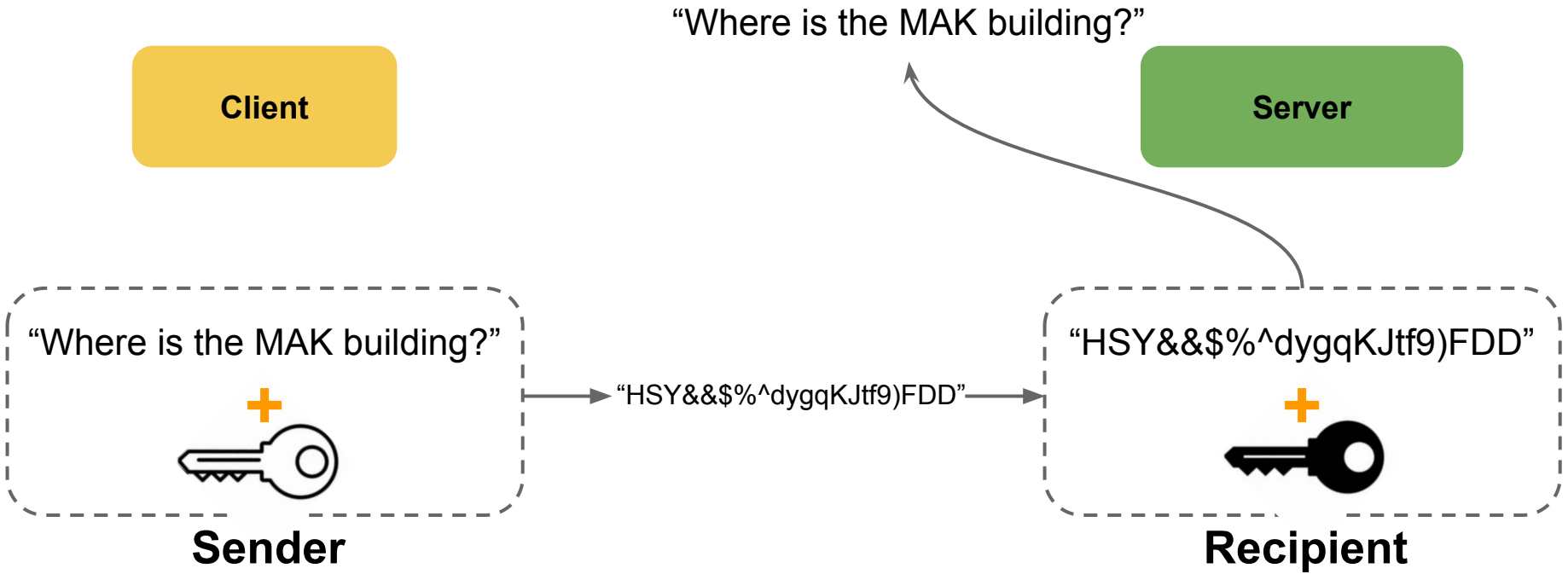
Encrypted Message (with public+private key pair)



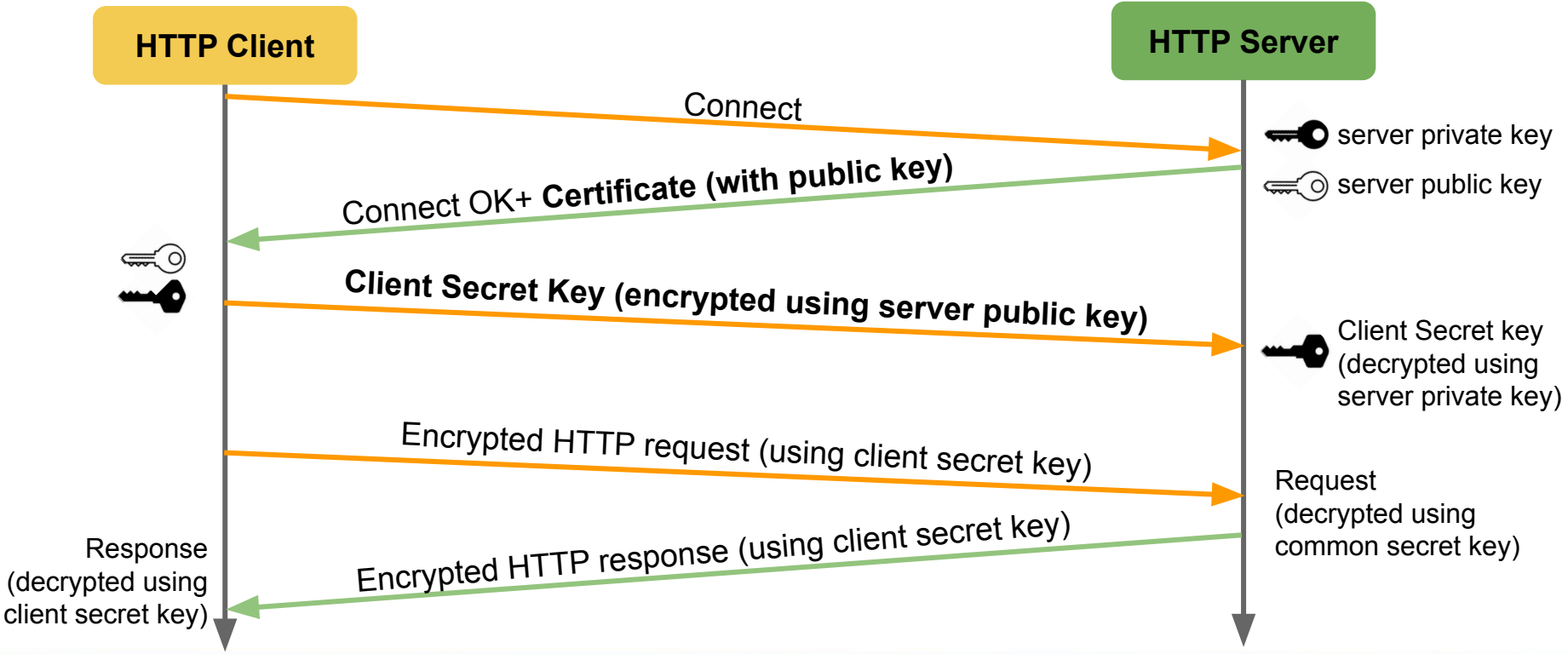
Encrypted Message (with public+private key pair)

Encrypted Message (with public+private key pair)

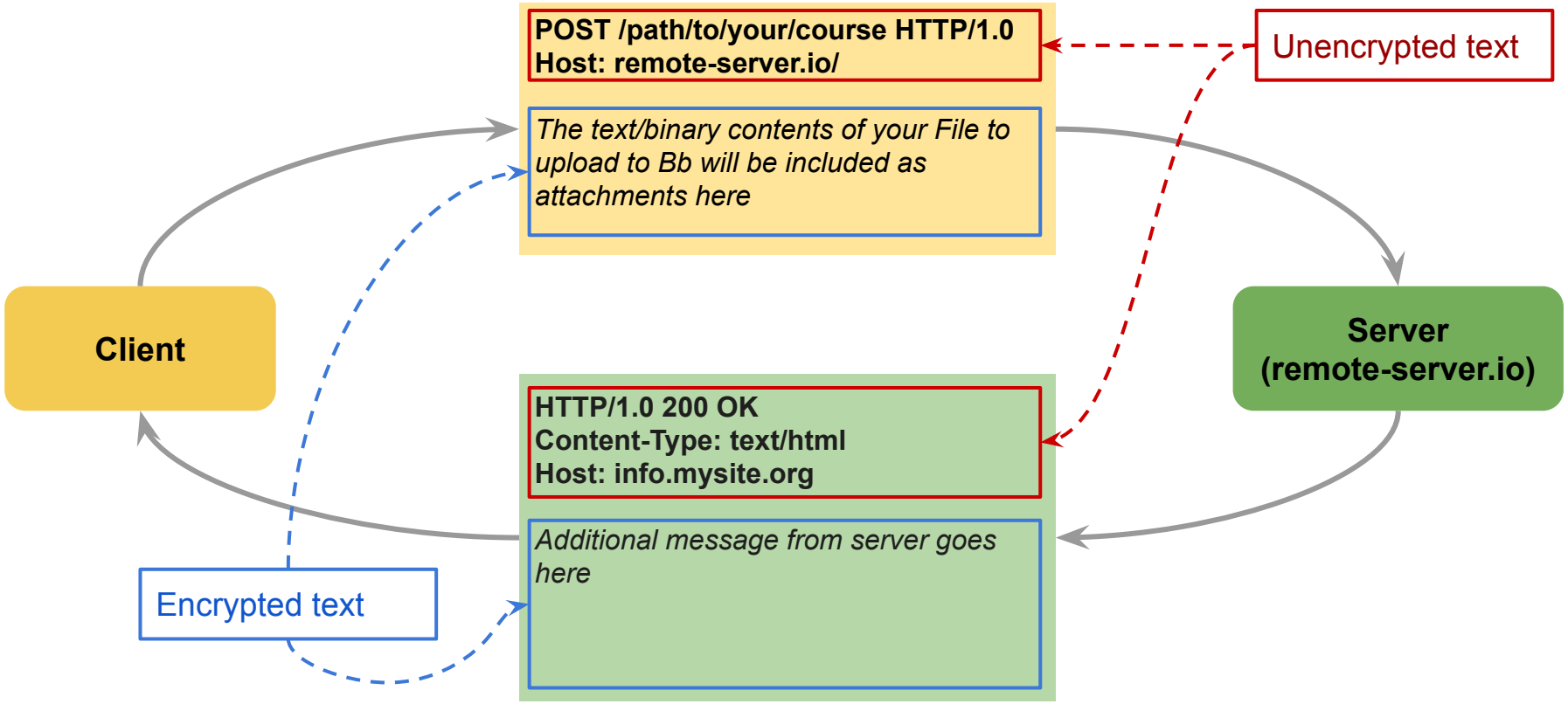
Encrypted Message (with public+private key pair)



Secure Message Exchange (over Persistent Connection)



GET or POST over secure connections



Uploading Sensitive Data over Encrypted Channel

- Embed the sensitive data in a GET request query string

  GET /place/my/order/?creditcard=xxxxyyyyzzzzuuuu&zip=12345 HTTP/1.0
  Host: www.amazon.co.uk

- Embed the sensitive data in a POST message payload

  POST /place/my/order HTTP/1.0
  Host: www.amazon.co.uk

  creditcard=xxxxyyyyzzzzuuuu
  zip=12345

Uploading Sensitive Data over Encrypted Channel

- Embed the sensitive data in a GET request query string

```
GET /place/my/order/?creditcard=xxxxyyyyzzzzuuuu&zip=12345 HTTP/1.0
Host: www.amazon.co.uk
```

Unencrypted

- Embed the sensitive data in a POST message payload

```
POST /place/my/order HTTP/1.0
Host: www.amazon.co.uk
```

Unencrypted

```
creditcard=xxxxyyyyzzzzuuuu
zip=12345
```

Encrypted

Certificate and Certificate Authority (CA)

Certificate: Proof of Your Identity

Certificate Authority:
Trusted Organizations who issue certificates

Michigan IDs vs. Browser Certificates

Michigan IDs	(Browser) Certificates
A formal proof of your identity	A formal proof of the web server identity
Issued and signed by Secretary of State	Issued and signed by Certificate Authority
Provide other proof of identity (birth certificate, passport) to apply for Michigan ID to the SoS	Certificate Signing Request: server request a CA to sign the server's identity (public key) using the CA key
The SoS is a trusted government body	Trusted CAs

Obtaining Web Certificates ("Web ID Cards")

Proof of identity (passport, GOV ids, birth certificates)

Certificate (signed by CA)

Private+Public Key Pair

Certificate Authority (CA)
Known to Browsers

Web Certificate
(signed by CA's private key)

Watch:
http://www.youtube.com/watch?v=iQsKdtjwtYI