

# COM-402 exercises 2025, session 2:

## Crypto and Trust in the Internet

### Exercise 2.1

- Why can't you use a message authentication code (e.g. HMAC-SHA2) to sign a contract between a buyer and a seller ?

### Exercise 2.2

- If asymmetric crypto is really more useful than symmetric, why are we still using AES ?

### Exercise 2.3

- Explain why using the same initialization vector (IV) multiple times with a stream cipher is more dangerous than with a block cipher.

### Exercise 2.4

- Explain why AEAD is not malleable.

### Exercise 2.5

- Describe an attack that would work if it was possible to find second pre-images for a hash function.

### Exercise 2.6

- How can you find out all cipher suites supported by a TLS server?

### Exercise 2.7

- Why is perfect forward secrecy important?

### Exercise 2.8

To be sure that your customers connect to your website with https instead of http, you configure your web server to answer requests on the http port with a redirection to the https port.

- Why does this not guarantee that all customers will end up using https?
- Why does closing the http port still not guarantee that customers will use https?
- What would be a working solution?

### Exercise 2.9

Most mobile e-banking applications use certificate pinning to validate the certificates of the servers they connect to.

- Describe an attack that can be prevented by using a pinned certificate.

### Exercise 2.10

- Which certificate authorities have been used to sign the certificate of the `www.epfl.ch` web server?