EXERCISE #1

If a user (sender) encrypts a message using a private (secret) key and sends the encrypted message to a remote user, who will decrypt the message using the public key, which of the following security threats (from the view point of the receiver) can be prevented? Explain for each.

The message consists only of:

- the sender’s address (network address)
- the receiver’s address (network address)
- the text message
- The message size (in # of bytes)

(a) Replay

(b) Man-in-middle

(c) Masquerading

EXERCISE #2

If a user (sender) encrypts a message using a public key and sends the encrypted message to the remote user, who owns the private key. The remote user will decrypt the message using the private key, which of the following security threats (from the view point of the receiver) can be prevented? Explain for each.

The message consists only of:

- the sender’s address (network address)
- the receiver’s address (network address)
- the text message
- The message size (in # of bytes)

(d) Replay

(e) Man-in-middle

(f) Masquerading