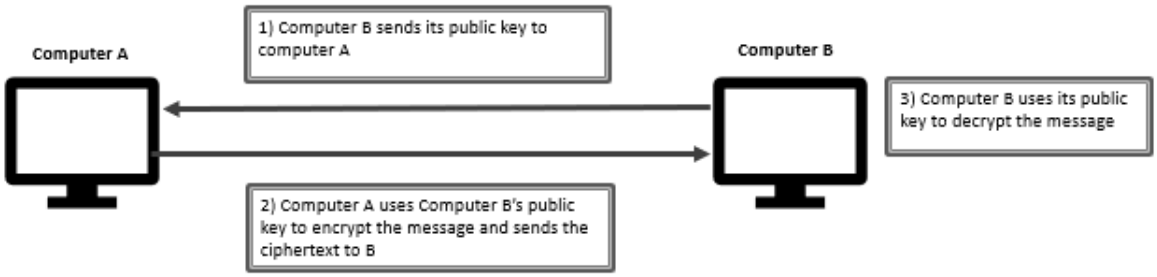
1.3.1 Encryption

Symmetric Encryption

Encryption is the act of encoding a plaintext message into and unreadable format (ciphertext). This stops intercepted messages from being understood if they are intercepted during transmission.

Symmetric encryption uses one key, the same key to encrypt and the decrypt the data being transferred.



The main problem is securely exchanging the shared key. If the key is sent over an insecure network, an attacker could intercept it and decrypt the messages.

Asymmetric Encryption

Asymmetric encryption uses two separate keys, a public key to encrypt data and private key to decrypt data.

The public key can be sent openly over the network because it does not need to be kept secret.

As the private key is never transmitted over the network it cannot be intercepted and an attacker cannot decrypt the intercepted message without the recipient's private key.