**2.1 What are the essential ingredients of a symmetric cipher?**

The plaintext to be translated into ciphertext, the algorithm to translate the plaintext into ciphertext, the algorithm to translate the ciphertext back into plaintext, and a key that is paired with the two algorithms so only those with access to the key can decipher the ciphertext.

**2.3 What are the two principal requirements for the secure use of symmetric encryption?**

The ciphertext produced by the encryption algorithm should not be possible to decrypt, and the key involved in creating and reading the ciphertext should be kept secure so that only the sender and receiver have access to the key.

**2.5 What is a message authentication code?**

A message authentication code is a code appended to a message that is the hash of that message using some key. When the recipient receives the message, they can use the same hash and key on the message to ensure that the message came from the proper sender and that the message is unaltered.

**2.7 What properties must a hash function have to be useful for message authentication?**

A hash function for message authentication should make it impossible to generate collisions using two different inputs and it should also be impossible to generate a specific hash value if you don’t know the input that was used to generate the hash.

**2.9 List and briefly define three uses of a public-key cryptosystem.**

A public-key cryptosystem can be used to provide digital signatures, can help distribute symmetric keys by keeping them secure while they are distributed, and can be used for the encryption of secret one use keys.

**2.11 What is a digital signature?**

A digital signature is a value associated with a message that helps the recipient verify that the message came from the person they think it did.

**2.13 How can public-key encryption be used to distribute a secret key?**

A secret key can be encrypted just like any other plaintext. So, when someone wishes to send a message, they can encrypt the message using a temporary secret key, and then encrypt that secret key with the recipient's public key. The recipient can then decrypt the secret key with their private key, and use the secret key to decrypt the message.