16-124-836
Marcel Matti ZAUDER

2.1 Question 1

2.1.A Provide a quick explanation why the following statements are True or False:

Symmetric encryption is a crypto-mechanism where encryption and decryption are performed using different keys.

False, in symmetric encryption only one key is used for both encrypting and decrypting a message.

With the use of symmetric encryption, the principal security problem is maintaining the secrecy of the key.

True, in symmetric encryption only one key is used and therefore it must be only available only to the communcating parties as every procedure for encryption/decryption can be performed with this single key.

The process of converting from plaintext to ciphertext is known as deciphering or decryption.

False, it is called enciphering or encryption. The process of converting from ciphertext to plaintext is known as deciphering or decryption.

The algorithm will produce a different output depending on the specific secret key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

True, as a simple example, the output of an encryption step using the CESAR CIPHER, will produce a different output depending on how much the alphabet was shifted.

When using symmetric encryption it is very important to keep the algorithm secret.

False, the algorithm itself can be publicly known, however, the key to encrypt and decrypt messages must be kept secret at all time.

Ciphertext generated using a computationally secure encryption scheme is impossible for an opponent to decrypt simply because the required information is not there.

False, unconditionally secure encryption schemes are impossible to decrypt because the required information is not there.