16-124-836
Marcel Matti ZAUDER

3.1 Question 1

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

Asymmetric encryption can be used for confidentiality but not for authentication

In asymmetric encryption, plaintext is transformed into ciphertext using two keys and a decryption algorithm.

Much of the theory of public-key cryptosystems is based on number theory.

A public-key encryption scheme is not vulnerable to a brute-force attack.

The defense against the brute-force approach for RSA is to use a large key space.