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

False, if one uses the private key for encryption - or the private key to create a signature - authenticity can also be ensured.

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

False, one key is used for encryption and a different but related key is used for decryption.

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

True, especially modulo operations are often used in creating the key, enciphering and deciphering.

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

False, as the public key and the private key are mathematically related it might be easier to find this relation than brute-forcing all different keys.

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

True, as brute-forcing is a "viable" option the prime numbers must be very large - making also the key space very large - in order to have the same level of security as symmetric encryption.