

## Question 1:

- Provide a quick explanation why the following statements are **True** or **False**:
  1. Asymmetric encryption can be used for confidentiality but not for authentication.
  2. In asymmetric encryption, plaintext is transformed into ciphertext using two keys and a decryption algorithm.
  3. Much of the theory of public-key cryptosystems is based on number theory.
  4. A public-key encryption scheme is not vulnerable to a brute-force attack.
  5. The defense against the brute-force approach for RSA is to use a large key space.