# Review Questions

1. Why public-key cryptography is needed? Why symmetric encryption is insufficient for these purposes?

2. What is the strength of the RSA algorithm? Why it is difficult to break?

3. How can public-key encryption be used to provide authentication/signature?

# Problems

1. If the RSA private key of Ahmed has been leaked. Instead of generating a new value of *n*, Ahmed only generated new values of *e* and *d*. Explain if this is sufficient or not.

2. Perform encryption and decryption using the RSA algorithm, for the following
a. *p* = 3; *q* = 11, *e* = 7; *M* = 5
b. *p* = 11; *q* = 13, *e* = 11; *M* = 7
c. *p* = 17; *q* = 31, *e* = 7; *M* = 2
Note: **You must use modular exponentiation** for mod calculations.

3. In a public-key system using RSA, you intercept the ciphertext *C* = 58 sent to a user whose public key is *e* = 43, *n* = 221. What is the plaintext *M*? **Show all steps**.