Arab Academy for Science Technology and Maritime Transport
College of Computing and Information Technology

Course	**Computer System Security**
Course Code	**CS421**
Lecturer	**Prof. Dr Ayman Adel**
TA	**Maram Shouman, Menna Elmasry**

Sheet 5

Review Questions: (2 marks per each question)

1. What is a public key certificate?
2. What are the roles of the public and private key?

Problems: (5 marks per each question)

1. Perform encryption and decryption using the RSA algorithm, as in Figure 9.5, for the Following:
   a. p = 3; q = 7, e = 5; M = 1 0
   b. p = 5; q = 13, e = 5; M = 8
   c. p = 7; q = 17, e = 11; M = 1 1
   d. p = 7; q = 13, e = 11; M = 2
   e. p = 17; q = 23, e = 9; M = 7

   Hint: Decryption is not as hard as you think; use some finesse.

2. In a public-key system using RSA, you intercept the cipher text C = 2 0 sent to a user whose public key is e = 13, n = 7 7. What is the plaintext M?

3. In an RSA system, the public key of a given user is e = 65, n = 2881. What is the private key of this user? Hint: First use trial-and-error to determine p and q; then use the extended Euclidean algorithm to find the multiplicative inverse of 31 modulo f(n).

4. Suppose we have a set of blocks encoded with the RSA algorithm and we don’t have the private key. Assume n = pq, e is the public key. Suppose also someone tells us they know one of the plaintext blocks has a common factor with n. Does this help us in any way?

5. In the RSA public-key encryption scheme, each user has a public key, e, and a private key, d. Suppose Bob leaks his private key. Rather than generating a new modulus, he decides to generate a new public and a new private key. Is this safe?

6. Consider the following scheme:

   1. Pick an odd number, E.
   2. Pick two prime numbers, P and Q, where (P - 1) (Q - 1) - 1 is evenly divisible by E.

3. Multiply P and Q to get N.
4. Calculate D = ((P - 1) (Q - 1) (E - 1) + 1) / E

Is this scheme equivalent to RSA? Show why or why not.

7. Perform the operations described below. Document results of all intermediate modular multiplications. Determine a number of modular multiplications per each major transformation (such as encryption, decryption)
   - ➢ Encrypt the message block M = 2 using RSA with the following parameters:
     e = 23 and n = 233 * 241.
   - ➢ Compute a private key (d, p, q) corresponding to the given above public key (e, n).
   - ➢ Perform the decryption of the obtained cipher text
8. RSA is one of the first public-key cryptosystems and is widely used for secure data transmission this asymmetry is based on the practical difficulty of the factorization of the product of two large prime numbers, the "factoring problem". Using the following number to get its factorization.

RSA-100 = 1522605027922533360535618378132637429718068114961380688657908494580122963258952897654000350692006139