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 7

Review Questions: (2 marks per each question)

1. Briefly explain Diffie–Hellman key exchange.

Problems: (5 marks per each question)

1. Alice and Bob use the Diffie–Hellman key exchange technique with a common prime q = 157 and a primitive root a = 5.
    a. If Alice has a private key $X_A = 15$, find her public key Y_A.
    b. If Bob has a private key $X_B = 27$, find his public key Y_B.
    c. What is the shared secret key between Alice and Bob?
2. Alice and Bob use the Diffie-Hellman key exchange technique with a common prime q = 23 and a primitive root a = 5.
    a. If Bob has a public key $Y_B = 10$, what is Bob's private key Y_B?
    b. If Alice has a public key $Y_A = 8$, what is the shared key K with Bob?
    c. Show that 5 is a primitive root of 23.
3. In the Diffie–Hellman protocol, each participant selects a secret number x and sends the other participant a x mod q for some public number a. What would happen if the participants sent each other x a for some public number a instead? Give at least one method Alice and Bob could use to agree on a key. Can Eve break your system with-out finding the secret numbers? Can Eve find the secret numbers?