Department of Computer Systems Engineering,
University of Engineering and Technology, Peshawar,
Pakistan

Finalterm Exam (Fall 2023) **Time:** 2 Hours
Paper: CSE-425 Computer Security **Marks:** 50

Note: Attempt all questions on answer sheet. Write short and precise answers.

Question No. 1 **(Marks=3+3+3+3+3) (CLO-2)**

Solve the following using RSA algorithm.

a) p = 3, q = 11 and e = 7, encrypt the Message (M) = "AC"
b) p = 7, q = 11 and e = 3, encrypt the Message (M) $=(32)_{16}$
c) p = 23, q=19, e=283, Find d?
d) Ciphertext C = $(1010)_2$, e = 5, n = 35, what is plaintext M?
e) Find the *ciphertext* (C) where *plaintext* (M) = $(14)_8$, and Public key (3, 187).

Note: Alphabets are coded by numbers from 0 to 25 before encryption.

Question No. 2 **(Marks=3+3) (CLO-3)**

a) What is IT Security Management? Describe its main functions?
b) What is the relationship between Risk, Threat and Vulnerability and how Security Controls can affect them?

Question No. 3 **(Marks=3+3+3+3)**

a) How is hash function different from Digital Signatures? How they can be combined?
b) Describe a scenario in computer security where the use of hash function is preferred instead of MAC?
c) Is it possible to use Hash function where both confidentiality and integrity of messages is important? Justify your answer.
d) Ali has an account with a server. The server makes her change her password every few months, to which Ali just increments a number in her password, e.g., pak1, pak2, · · ·. Why does the server not complain that the new password is very much like her old one?

Question No. 4 **(Marks=3+3+3+3)**

In the Diffie-Hellman Key Exchange, let the public keys be p = 43, g = 26, and the secret keys be a = 13 and b = 22, where a is Alice's secret key and b is Bob's secret key.

a) What value does Alice send Bob?
b) What value does Bob send Alice?
c) What is the secret key they share?
d) Unknown to Alice and Bob, Eve is listening and is able to intercept their messages as well as inject her own messages. Suppose Eve chooses an secret key e = 7. Explain how Eve can use e to perform the Intruder-in-the-Middle attack on the Alice-Bob Diffie-Hellman key exchange.

Question No. 5 **(Marks=2.5+2.5)**

a) What are the major vulnerability points of the RSA algorithm?
b) In what scenarios would you advise against using RSA and why?