



COMSATS UNIVERSITY ISLAMABAD (CUI)

DEPARTMENT OF COMPUTER SCIENCE
FINAL TERM EXAMINATION SPRING - 2025
BS (CYS) – III SEMESTER

Course: CSC232-Information Security.

Dated: 03-07-2025

Maximum Marks:50

Time Allowed: 180 Minutes

Course Instructor: Dr. Tehsin Kanwal.

- All questions are self-explanatory and require no further explanations during exam time.
- Make sure that you have signed the attendance sheet before leaving the examination room.
- Return the question paper along with the answer sheet.
- Attempt all questions.

CLO-1 Describe fundamental concepts of information security along with classical cryptographic algorithms.

Question 1. Short Question Answers [2+ 2 +2 +2 + 2 = 10 Marks]

- (a) Explain the difference between secret-key encryption and public-key encryption.
- (b) What is Vigenère Cipher, Encrypt and decrypt following message using same Cipher:
Message (M) = "attack at dawn"
Key = "moonlight"
- (c) Considering the amount of left shifts in the DES key schedule by studying Table C.3 (d), Answer following questions.
- Is there a pattern?
 - What could be the reason for the choice of these constants?

Table C.3 DES Key Schedule Calculation

(a) Input Key							
1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

- (d) Describe how the OFB mode can be attacked if the IV is not different for each execution of the encryption operation?

1, 2, 9, 16

- (e) What are different types of Attacks that an adversary can be performed on AES encrypted messages?

CLO-2 Analyze authenticated encryption techniques to secure information in a specific network application.

Question 2. [7 + 3 = 10 Marks]

Q2.1 [7 Marks]

MACs can be used to authenticate messages. Consider two protocols,—one with a MAC, and one with a digital signature. In the two protocols, the sending party performs the following operation:

1. Protocol A:

$$y = e_{k_1} [x || h(k_2 || x)]$$

where x is the message, $h()$ is a hash function such as SHA-1, e is a private-key encryption algorithm, " $||$ " denotes simple concatenation, and k_1, k_2 are secret keys which are only known to the sender and the receiver.

2. Protocol B:

$$y = e_k [x || \text{sig}_{k_{pr}}(h(x))]$$

Provide a step-by-step description (e.g., with an itemized list) of what the receiver does upon receipt of y . You have to differentiate between Protocol A and B, You may draw a block diagram for the process on the receiver's side.

Q2.2 [3 Marks]

Your colleagues urgently need a collision-resistant hash function. Their code contains already an existing implementation of HMAC, using a block cipher with 256-bit block size. Therefore, they suggest to use HMAC with fixed keys $K_1 = K_2 = 0'$ as a hash function. Show that this construction is not even pre-image resistant.



CLO3: Solve cryptographic problems using mathematical foundations of number theory and finite fields.

Question 3 [10+7+5 = 22 Marks]

Q3.1 [10 Marks] With RSA encryption, it is common practice to choose e as a small number

(e.g., 3, 17, $2^{16} + 1$).

(a) How does this affect the speed of encryption?

- (b) If you wanted to make decryption faster, could you simply set d to one of these three values instead?
- (c) How else RSA decryption can be calculated more efficiently using the Chinese Remainder Theorem and Fermat's little theorem?
- (d) Is there any problem if a user of RSA choose the encryption exponent e to be even, e.g. $e = 4$, provide justification of your answer.
- (e) List the different approaches to attack the RSA algorithm.

Q 3.2. [7 Marks]

Consider a variation on Diffie-Hellman that could be used as a digital signature. The proposed digital signature variation is simpler than DSA and that does not require a secret random number in addition to private key.

Public elements:

q prime number ✓

α $\alpha < q$ and α is primitive root of q ✓ p

Private key:

X $X < q$ ✓

Public key:

$Y = \alpha^X \text{ mod } q \text{ mod } q$

hash of message

To sign a message M , compute $h = H(M)$, which is the hash code of the message. We require that $\gcd(h, q - 1) = 1$. If not, append the hash to the message and calculate a new hash. Continue this process until a hash code is produced that is relatively prime to $(q - 1)$. Then, calculate Z to satisfy $Z \equiv X \times h \text{ mod } (q - 1)$. The signature of the message is $\sigma = \alpha^Z$. To verify the signature, a user computes t such that $t \times h \equiv 1 \text{ mod } (q - 1)$ and verifies $Y = \sigma^t \text{ mod } q$.

Show that this scheme works. That is, show that the verification process produce

an equality if signature is valid.

Q3.3 [5 Marks] 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 X_B ? 3
- b. If Alice has a public key $Y_A = 8$, what is the shared key K with Bob?

Question 4. [4 + 4 = 8 Marks]

Q 4.1 Imagine a peer-to-peer network where 1000 users want to communicate in an authenticated and confidential way without a central Trusted Third Party (TTP).

1. How many keys are collectively needed, if symmetric algorithms are deployed? 2^{1000}

2. How are these numbers changed, if we bring in a central instance (Key Distribution Center, KDC)?

3. What is the main advantage of a KDC against the scenario without a KDC?

4. How many keys are necessary if we make use of asymmetric algorithms?

Also differentiate between keys which every user has to store and keys which are collectively necessary.

Q 4.2 A decentralized key management system (DKMS) is an approach to cryptographic key management where there is no central authority.

Below is an example de-centralized key distribution protocol that may be used. **MK_m** is the master key shared between two nodes A and B (this sharing must be done manually/physically), and **K_s** is the session key.

How many master keys are needed in a network using this key distribution protocol if there are 10 and 20 nodes in the network? 5 + Nodes - 3

