Information Security (CS3002)

Sessional-I Exam

Total Time (Hrs): 1
Total Marks: 42
Total Questions: 4

Date: Sep 20th 2025

Course Instructors

Ammar Haider, Aqsa Khalid, Nosheen Manzoor, Zeeshan Ali Khan

Student Roll No _____ Section _____ Student Signature _____

Instructions:

1. Attempt all questions on the answer booklet.
2. If you think some information is missing then make an assumption and state it clearly.

[This paper is NOT for BCS-7D, BCS-7H and BCS-7J sections]

CLO-1	Explain key concepts of information security such as design principles, cryptography, risk management.
CLO-2	Discuss legal, ethical, and professional issues in information security.
CLO-3	Analyze real world scenarios, model them using security measures, and apply various security and risk management tools for achieving information security and privacy.
CLO-4	Identify appropriate techniques to tackle and solve problems of real life in the discipline of information security.
CLO-5	Describe issues related to ethics in the field of information security.

CLO 1

Q1: Multiple choice questions **[7 marks]**

1. A message is first encrypted with a Caesar cipher (with key 3) and then the resulting text is again encrypted with monoalphabetic substitution cipher where A is mapped to F, B to K, and so on. A cryptanalyst knows this two-step process. What is the most effective way to break this combined cipher without trying to guess the original plain text?
   a) Brute force the Caesar cipher, then perform a frequency analysis on the intermediate text.
   b) Perform frequency analysis on the final ciphertext, then brute force the Ceaser shifts.
   c) Brute force the monoalphabetic cipher, then brute force the Caesar cipher.
   d) Treat the combined cipher as a single monoalphabetic substitution cipher.

2. A cryptanalyst intercepts a ciphertext that is 300 characters long. They look for repeated strings, and find that the sequence UQE repeats at positions 25 and 100, while FPR repeats at positions 50 and 150. Which of the following is the most likely key length for the Vigenère cipher?
   a) 5
   b) 10
   c) 15
   d) 25

3. What is the biggest disadvantage of symmetric encryption?
   a) It requires more complex and time-consuming calculations.
   b) The secret key must be transmitted securely between parties.
   c) It uses a less secure encryption function.
   d) It is no longer in use.

4. Which statement best describes the role of a key in encryption?
   a) The key determines which encryption function is used, making decryption difficult if the function is unknown.
   b) The key contains a secret encryption function along with its parameters. A password is required to activate the key.
   c) The key only contains secret parameters used for both encryption and decryption.
   d) The key allows users to avoid reinstalling encryption software when the technology or encryption functions change.

5. In a hybrid cryptosystem (Digital Envelope), what is the primary role of asymmetric cryptography?
   a) To securely encrypt and exchange a symmetric session key
   b) To encrypt the entire bulk message for speed
   c) To generate the hash of the message for integrity
   d) To create a digital signature for non-repudiation

6. What is the correct sequence for creating a digital signature?
   a) Encrypt message with private key -> Hash the message
   b) Hash the message -> Encrypt hash with recipient's public key
   c) Hash the message -> Encrypt hash with sender's private key
   d) Encrypt message with public key -> Hash the ciphertext

7. Why are large prime numbers (e.g., 1024 bits) used in RSA?
   a) To make the encryption process faster
   b) To ensure the output ciphertext is smaller than the plaintext
   c) To make factoring the product $n = p \times q$ computationally infeasible
   d) To increase the likelihood that e and $\varphi(n)$ are co-prime

CLO 1

Q2: Short answer questions **[4 + 4 + 2 + 2 marks]**

A. Which information security property is being most directly impacted in the following scenarios? Choose one from Confidentiality, Integrity, Availability, Authenticity, Accountability

i. During a ransomware attack, the company loses access to its systems until ransom is paid.
ii. An employee receives an email that looks like it is from their boss, but it was actually sent by a pretending attacker.
iii. University's online portal crashes on the day grades are released, leaving students unable to access results.
iv. An angry employee modifies payroll data so that some staff salaries are reduced.

B. Review the below scenario, and then discuss how you could apply the following security design principles to improve the system's security. Give specific examples relevant to this system.

i. least privilege
ii. fail-safe defaults

Scenario: A healthcare startup has developed an online medical consultation portal. Patients register and book virtual appointments with doctors. During the consultation, doctors access the patient's medical history stored in the system. After the session, doctors update the record with prescriptions and treatment notes. Patients can later download their prescriptions or share them with pharmacies.

C. Referring to the block cipher modes of operation, mention one benefit and one drawback of the Cipher Block Chaining (CBC) mode.

D. Eve intercepts a message from Alice to Bob that is protected with an HMAC. She tries to modify the message as well as the MAC. Explain why will her attack fail when Bob verifies the message?

CLO 3

Q3: Practical problems **[4 + 4 + 2 + 4 marks]**

A. An adversary intercepts an encrypted message. He knows the message was first protected with a Caesar cipher with shift 3, but the output was then permutated using a rail fence cipher with a depth of 4. The final ciphertext is VWFHLBDKFUEHHXUV. Find the original plaintext message. Show your working.

B. Consider a Vigenère cipher where sixteen hexadecimal characters (0 to F) are used as the alphabet (instead of English letters).

i. For plaintext 3AE60A3 and keyword 17E, what will be the ciphertext?
ii. Using your answer in (i) argue that a polyalphabetic cipher such as the above is stronger against letter frequency analysis when compared to a monoalphabetic ciphers like Caesar.

C. Recall that DES Expansion P-box operates on a 32-bit input. Suppose we are working with a smaller version of DES in which expansion is performed on a 16-bit input. Expand the following input block, and provide the corresponding output in binary.

0010 1100 0011 0100

Expansion P-box

16	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	1

D. The AES SubBytes substitution table is provided below. Given the following state matrix (in hex) for an AES encryption round, perform the SubBytes operation *followed by* the ShiftRows operation. Show the intermediate output after SubBytes, and final matrix after ShiftRows.

1B	22	34	56
4A	FF	33	E3
2B	CD	4C	5B
22	AA	CC	BB

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

CLO 3

Q4: Numerical questions **[2 + (3 + 2 + 2) marks]**

A. In an RSA crypto system, you intercept the ciphertext $C = 10$ sent to a user whose public key is $e = 5,\ n = 35$. What is the plaintext M?

B. Alice and Bob are two business partners negotiating a sensitive deal. One of them is connected to an insecure public Wi-Fi network at an airport. To protect their communication, they decide to use the Diffie-Hellman Key Exchange to establish a shared secret key. Once the key is agreed upon, they plan to use it with a symmetric encryption algorithm such as AES to secure all further messages.

They publicly agree on two parameters: Prime $p = 11$, and Generator $g = 6$

Alice selects her private number $a = 7$ and computes her public value A.

Bob selects his private number $b = 8$ and computes his public value B.

Meanwhile, a hacker named Mallory, who is on the same airport Wi-Fi, launches a man-in-the-middle attack. She intercepts and modifies all messages between Alice and Bob. Mallory chooses her private number $m = 4$ and computes her public value M. She then sends M to Bob while pretending to be Alice, and sends the same value M to Alice while pretending to be Bob. As a result:

Alice computes a shared secret K_{AM} with Mallory, believing it to be with Bob.

Bob computes a shared secret K_{BM} with Mallory, believing it to be with Alice.

Neither Alice nor Bob shares the same key with each other — only Mallory knows both.

Questions

i. Compute the public values A, B and M, as well as the shared keys K_{AM} and K_{BM}.
ii. Explain why this situation is catastrophic for Alice and Bob. What can Mallory do at this stage?
iii. What is the fundamental weakness in the basic Diffie-Hellman protocol that allows this attack?