


National University of Computer and Emerging Sciences, Lahore Campus

	Course Name:	Information Security	Course Code:	CS3002
	Program:	BS(Computer Science)	Semester:	Fall 2023
	Duration	60 minutes	Total Marks:	35
	Date:	02-10-23	Weight	12.5
	Exam Type:	Midterm-I	Pages	4

Student : Name: _____ Roll No. _____ Section: _____

Instruction: If you think some information is missing then make an assumption and write it clearly.

Question 1: [CLO:1] [5 marks]

- The process of identifying vulnerabilities and threats and their impact and probability of occurring an attack is called _____.
 - Vulnerability assessment
 - Vulnerability identification
 - Threat detection
 - Risk analysis
- Receiving an SMS message where the sender's number is fake, is an attack against _____.
 - Confidentiality
 - Integrity
 - Availability
 - Authenticity
- Which block cipher mode does not allow parallel encryption of blocks?
 - Cipher Block Chaining (CBC)
 - Counter mode
 - Electronic Code Book (ECB)
 - All of these
- Sam maintains a public key ring in his computer. He will pick a key from the ring during
 - Asymmetric encryption
 - Signing a message
 - Asymmetric decryption
 - Both a and c
- In the DES algorithm the Round Input is 32 bits, which is expanded to 48 bits via _____.
 - Scaling of the existing bits
 - Substitution of the existing bits
 - Addition of zeros
 - Addition of ones

Part I:

Identify the kind of attacks in each of the following statements and identify at least a couple of reasons the people fall for that

- a. You receive a phone call. The caller claims that they are from a bank, and ask your debit card number and OTP for the purpose of account confirmation, otherwise your account will be blocked.

social engineering, or more specifically phishing

people get panic by such threats and make decisions in haste

- b. You tried to login to your flex account during which you ignored a warning displayed by the browser and later on you came to know that your login credentials have been stolen.

phishing attack bcoz it was a look-alike web page operated by attacker

most people do not understand the meaning of SSL warnings, and want to finish their intended task asap.

- c. The outgoing network traffic of your system has suddenly increased and on diagnosis, you have identified that your system is constantly sending a specific request to a server.

This computer has become a zombie, and is participating in a DDoS attack. Attackers infected the computer with a bot malware.

People fall for this attack due to not having good anti malware software, and downloading software from dangerous sources like torrents or piracy sites.

Part II:

We studied following security design principles: Least privilege, Failsafe defaults, Separation of privilege, Economy of mechanism, Psychological acceptability, Complete mediation, Least common mechanism. Analyze the following scenarios and identify, with reasoning, what security design principle is being applied? Also state what advantages are achieved due to that principle.

- A. Marketing staff do not have access to engineering design files.

principle of least privilege. Minimize the chances of access misuse.

- B. Company database is protected by only one layer of encryption rather than two layers.

economy of mechanism, since a single layer is enough. Do not needlessly complicate the system.

Question 3:

[CLO:1]

[2+4+4 marks]

- a. Encrypt the text “voteforme” using Vigenère cipher with a key 245.

Plaintext: v o t e f o r m e
Key: 2 4 5 2 4 5 2 4 5
Ciphertext: x s y g j t t q j

- b. Show the process of Diffie-Helman key exchange using a prime 47 and generator 11. Suppose Alice chooses a secret 9 and Bob chooses 16.

Alice computes $A = 11^9 \bmod 47 = 38$

Bob computes $B = 11^{16} \bmod 47 = 3$ (hard to get it via calculator)

After sharing public keys, Alice computes shared key as $K = 3^9 \bmod 47 = 37$

Bob gets $K = 38^{16} \bmod 47 = 37$

- c. What is a digital envelope? Demonstrate its working with the help of an example! What are the advantages of this mechanism?

Use diagram from slides

Advantages

Gain the speed of symmetric encryption, and convenience of PKC

Question 4:**[CLO:1]****[10 marks]**

Describe the key development mechanism using RSA when the values of p and q are given to be 7 and 11 respectively? Although there are multiple options for choosing the encryption value 'e', let's choose 7 that fulfill the criteria and then find 'd' accordingly. You should provide all details and outcome should be written in the form of private and public keys. Demonstrate the working of your system by encrypting a number and then retrieving it back using decryption.

$$p = 7, q = 11$$

$$n = 77$$

$$\phi = 60$$

$$\text{given } e = 7$$

$$\text{Solving } 7 \times d \bmod \phi = 1, \text{ we get smallest } d = 43$$

$$\text{Public key} = 7, 77$$

$$\text{Private key} = 43, 77$$

Encryption of message, say 5

$$5^7 \bmod 77 = 47$$

Decryption

$$47^{43} \bmod 77 = 5$$