Y/D/TY

Reg. No: 22BIT0691

VIT
Vellore Institute of Technology

Final Assessment Test – April 2025

Course: **BITE401L - Network and Information Security**
Class NBR(s): **3076 / 3083 / 3088**
Time: **Three Hours**
Slot: **C1+TC1**
Max. Marks: **100**

- **KEEPING MOBILE PHONE/ANY ELECTRONIC GADGETS, EVEN IN 'OFF' POSITION IS TREATED AS EXAM MALPRACTICE**
- **DON'T WRITE ANYTHING ON THE QUESTION PAPER**

Answer ALL Questions
(10 X 10 = 100 Marks)

1. Identify the type of security attack occurred in the following scenarios by compromising the type of security service, brief the attack and the service compromised.

   a) Disabling file management systems.

   b) Amount credited to account 6543; instead of 9876.

   c) An entity deceives another by falsely denying responsibility for an act.

   d) Hackers gaining access to a personal email and sending message.

   e) Wire tapping to capture data in a network.

2. Compute the AES Mix column process for the given values and derive the new bytes to fill the mentioned columns. Show the computations in detail to derive the value for the '?' column.

2	3	1	1
1	2	3	1
1	1	2	3
3	1	1	2

*

63	EB		
2F	93		
AF	C7		
A2	20		

=

BA	?		
75	?		
FA	?		
7A	?		

3.a) Imagine you are designing a new secure messaging protocol. Your task is to implement a key exchange mechanism using Diffie-Hellman.

i) What parameters (eg. prime and primitive root) would you choose for the Diffie-Hellman exchange, and why?

ii) How would you ensure the security of your key exchange? What measures would you implement to protect against man-in-the-middle attacks or other attacks?

iii) How could you verify the identity of the parties involved in the exchange to prevent impersonation attacks?

OR

3.b) A user obtained the Ciphertext C=8 using RSA approach with the public key e=13 and n=33. What is the Plaintext 'M'?

Identify M and encrypt it using another RSA system, with the values p=11, q=7 and the public key e=11. Now, what is the Ciphertext 'C' and prove its decryption process? Discuss the algorithmic steps in arriving the results, in detail.

[Hint: A=0; B=1...Z=25]

4. What is the approach where MAC is obtained based on Hash Functions? Describe it with a neat structure and the algorithmic steps.

5. On an authentication process between two Users A and B using the Digital Signature Algorithm, the domain parameters p, q and g has values 23, 11 and 2, respectively. The signing process owns the private key as 5, a random key chosen is k=3 and the Hashed Message is 3. Perform the authentication process with detailed steps and describe the strength of this algorithm.

6.a) On a user authentication process, what are the ways used to counter the suppress-replay attacks? Explain the approach in detail with protocol steps. Also, discuss the major role of realm, in the context of Kerberos.

OR

6.b) i) What are the principal differences between version 4 and version 5 of Kerberos? Discuss in detail.

ii) Answer the following questions in perception of Kerberos:

I. When Bob receives a Ticket from Alice, how does he know it came from Alice?

II. When Alice receives a reply, how does she know it came from Bob (that it's not a replay of an earlier message from Bob)?

III. What does the Ticket contain that allows Alice and Bob to talk securely?

7. How does IEEE 802 protocol stack are defined according to IEEE 802.11 standards. Also, discuss the security protocols and the cryptographic algorithms associated with IEEE 802.11i Services, in detail.

8. What are the services provided by the SSL Record Protocol? In SSL and TLS, why is there a separate Change Cipher Spec Protocol rather than including a ***change_cipher_spec*** message in the Handshake Protocol? Explain with a detailed note.

9. Assume that User-B want to communicate the cipher message "OMRMPCSGPTER" to User-A. Here, B has applied Playfair Cipher using the key "COMPUTER". What would be the Plaintext message derived by A using the key matrices? Finally, encrypt the arrived Plaintext with the Key "HEALTH" using Vigenere cipher method. Depict the step-by-step process involved in this cryptographic process.

10. a) Explain the following protocol and identify the attack susceptible to and suggest possible mitigation measures. **[5]**

$$A \rightarrow B : M \,||\, E[K, H(M)]$$

b) Analyse the functionality of Mixer operators in secure hash algorithm and illustrate how to compute the majority and conditional function of the buffers [A, B ,C] and [E, F, G] if the leftmost hexa decimal digits of these buffers are (0x7, 0xA and 0xE) and (0x9, 0xA and 0xF), respectively. What would be the leftmost digit of these results? **[5]**

⇔⇔⇔ **Y/D/TY** ⇔⇔⇔