N/E/TX

Reg. No:

VIT
Vellore Institute of Technology

Final Assessment Test – May 2024

Course: **BITE401L - Network and Information Security**

Class NBR(s): **3898/3903/3909/3913** Slot: **C2+TC2**

Time: **Three Hours** Max. Marks: **100**

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

Answer any TEN 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) BigBox customer data for sale online, October 2021
   b) Amount credited to xxxx9876; instead of xxxx8765
   c) VTOP becomes slow / unresponsive during course registration
   d) Someone on social media creating fake profiles to deceive others

2. Utilize the Simplified Advanced Encryption Standard (S-AES) algorithm to produce the Cipher text for the provided inputs. Clearly demonstrate the process with the following specifications:

   16-bit Plaintext, P: 1101 0111 0010 1000

   16-bit Key, K: 0100 1010 1111 0101

   Encryption S-box:

	00	01	10	11
00	1001	0100	1010	1011
01	1101	0001	1000	0101
10	0110	0010	0000	0011
11	1100	1110	1111	0111

   Multiplication Table:

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	0	2	4	6	8	A	C	E	3	1	7	5	B	9	F	D
3	0	3	6	5	C	F	A	9	B	8	D	E	7	4	1	2
4	0	4	8	C	3	7	B	F	6	2	E	A	5	1	D	9
5	0	5	A	F	7	2	D	8	E	B	4	1	9	C	3	6
6	0	6	C	A	B	D	7	1	5	3	9	F	E	8	2	4
7	0	7	E	9	F	8	1	6	D	A	3	4	2	5	C	B
8	0	8	3	B	6	E	5	D	C	4	F	7	A	2	9	1
9	0	9	1	8	2	B	3	A	4	D	5	C	6	F	7	E
A	0	A	7	D	E	4	9	3	F	5	8	2	1	B	6	C
B	0	B	5	E	A	1	F	4	7	C	2	9	D	6	8	3
C	0	C	B	7	5	9	E	2	A	6	1	D	F	3	4	8
D	0	D	9	4	1	C	8	5	2	F	B	6	3	E	A	7
E	0	E	F	1	D	3	2	C	9	7	6	8	4	A	B	5
F	0	F	D	2	9	6	4	B	1	E	C	3	8	7	5	A

3. Consider a Diffie-Hellman key scheme with a global components q=11 and α =2,
   a) If Bob has Alice's public key YA =9, what is the corresponding private key XA?
   b) If Alice has Bob's public key YB =3, what is the corresponding private key XB?
   c) Calculate the shared secret key generated by both Alice and Bob and verify whether they do match or not.

4. a) Describe the steps for generating the public/private key pair in RSA. You must state the conditions/properties of any values to be selected or calculated. [7]

b) Given C, e and n, calculate the inverse of $C=M^e \bmod n$. Is it feasible to compute M? Justify your claim. [3]

5. a) Alice now wants to send three n-bit messages m1, m2 and m3 to Bob. She encrypts, XOR plaintext with Key, them using the one-time pad with keys k4, k5, and k4 $\oplus$ k5, respectively. Can the attacker recover any information about the plaintexts given only the ciphertexts? Give an explanation (if secure) or an attack (if insecure). [4]

29468178

b) List the basic properties of a Hash function. [6]

6. a) Apply the Majority function on buffers A, B, and C. If the leftmost hexadecimal digits of these buffers are 0xA, 0xF, and 0xF, respectively, what is the leftmost digit of the result? [3]

b) Apply the Conditional function on E, F, and G buffers. If the leftmost hexadecimal digits of these buffers are 0xC, 0xD and 0xE respectively, what is the leftmost digit of the result? [3]

c) If the prime number is 13, find out the corresponding constant ki used in SHA-512. [2]

d) Derive the word W69 for the compression function in SHA-512. [2]

7. The following statements show different uses of hash functions and MACs. All the shown operations occur at the sender side. Draw a figure and specify a statement for the operations at the receiver side. In addition, for each statement specify which of the following properties are achieved: confidentiality, integrity, non-repudiation.

- $M \parallel H(k \parallel M)$
- $M \parallel E(k, H(M))$
- $M \parallel H(M)$
- $E(k, (M \parallel H(M)))$
- $E(k1, M) \mid\mid E(k2, H(M))$

8. Alice used Digital Signature Algorithm, DSA, to generate and verify the signature.

a) Alice chooses p = 1279, and calculates q = (p-1) mod q =71, h=3, Compute g. [1]

b) She has chosen the private key value as 15 and the random integer k=10. Compute the public key. [1]

c) Hash of the message as 123. Generate Digital signature components r and s. [4]

d) Verify the generated signature by computing u1, u2 and v. [4]

diagrammatic representation

face considered much anth

9. a) How was the user authenticated to access a particular server by AS in Kerberos? [7]

   b) Why did the addition of a timestamp become necessary for the Kerberos protocol? [3]

10. Explain the five distinct phases of operation IEEE 802.11i RSN with neat sketches wherever necessary.

11. a) Identify E-mail security threats and explain, how are these major E-mail security threats addressed by PGP?

    b) A PGP user may have multiple public keys. How does a recipient know which public key is being used by a sender?

12. a) In the IPSec protocol, which of the security services are provided by the Authentication Header (AH)? Explain in detail.

    b) IPsec's Authentication Header in transport mode is used to secure an IP packet. Which of the packet fields are used to create the Message Authentication Code (MAC)?

⇔⇔⇔ N/E/TX ⇔⇔⇔

ESP AH.

Auth Encryp Auth

1/