P/E/TX

Reg. No:

Final Assessment Test – May 2024

Vellore Institute of Technology
(Deemed to be University under section 3 of the UGC Act, 1956)

Course: **BCSE309L - Cryptography and Network Security**

Class NBR(s): **0696/0724/0727/0728/0731/0733/ 0737/0739/0742/0743/0744/0745/0749/0750/ 0751/0752/0753/0754/0755/0756/0757/0759/ 0761/2367/2369**

Slot: **E2+TE2**

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. a) A child has some fruits in a box. If the fruits are grouped in 7's, there will be 5 left over; If they are grouped in 11's, there will be 6 left over; If they are grouped in 13's , 8 will be left over; Find the least number of fruits in the box. **[6] BL4 CO1**

   b) Find the last 2 digits of 9^{100}. **[4]**

2. a) Use Extended Euclidean algorithm to find the GCD and MMI of (42823, 6409) and its linear combination. **[5] BL4 CO1**

   b) Calculate the 3^{64} mod 67 using Fermat's little theorem. **[5]**

3. In DES, given that K= 133457799BBCDFF1,generate subkeys K1 & K2 & K3 (Data tables are given for PC-1 & PC-2). Show DES key generation algorithm. **BL4 CO1**

DATA TABLES:

PC-1

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

PC-2

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

4. In AES, given that plaintext, {0F0E0D0C0B0A09080706050403020100} and the key {02020202020202020202020202020202}: Show the value of state after mixcolumns (4 columns) **BL4 CO1**

State Matrix $\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$

5. a) Alice and Bob use the Diffie-Hellman key exchange technique with a common prime q = 71 and its primitive root=7 **[4] BL3 CO1**

i. If Bob has public key $Y_B = 4$, what is Bob's pvt key X_B?

ii. If Alice has public key $Y_A = 51$, what is the shared key K with Bob.

b) In Elgamal cryptosystem, global prime p =107, generator g=2. Alice chooses private key Xa=67 and Bob's unique random integer k=45. Encrypt the message ='A' (ASCII:65) **[6]**

6. Consider the elliptic curve $y^2 = x^3 + 9x + 17 \bmod 23$. Find the cryptosystem parameter 'n' for the equation Q = np, where Q = (4, 5) and P = (16, 5). **BL4 CO1**

7. Given a text: "VIT" Create the process of deriving eighty 64-bit words from1024 bits for processing of a single message block of SHA-512 algorithm. Show the values of W16, W17, W18 and W19. ASCII DATA V : 86 1 : 73 T : 84 (Decimal). **BL4 CO2**

8. Alice and Bob use the Diffie – Hellman key exchange technique with a common prime P = 227 and primitive root g = 14. **BL4 CO2**

a) If Alice has a private key $X_a = 227$, find her public key Y_a? **[2]**

b) If Bob has a private key $X_b = 170$, find her public key Y_b? **[2]**

c) What is the shared secret key between Alice and Bob? **[2]**

d) Illustrate the Man – in the middle attack that can be launched in the DH protocol? **[4]**

9. a) Compute the value of the padding field, Length field and number of blocks in MD5 if the message = "VIT VELLORE" **[4] BL4 CO2**

b) Assume **[6]**

A: 10 32 54 76

B: BA FE CD 98

C: 78 CE AE DE

D: 01 23 45 67

Find the output of the logical functions F, G, H, I after one round of operation.

10. Generate the Digital Signature and signature verification using DSS for the following parameters. **BL4 CO2**

- Public key components (p, q, g) = (283, 47, 60)
- Alice private key = 24
- H(M) = 41

11. Alice started an online classes and hosted an application. He got a merchant account from national credit card company. He wants to provide payment option with PayPal. Suggest suitable protocol with diagrams for this in transport layer and internet layer and discuss the Crypto algorithms steps involved in this electronic fund transfer. **BL3 CO3**

12. a) Consider a banking application to provide MAC and encryption for the electronic transaction. Suggest a suitable protocol with diagrams for this and discuss the Crypto algorithms and steps involved in this electronic fund transfer. **[5] BL3 CO3**

    b) Discuss the challenges in protecting an organization against cyber security threats. **[5]**

⇔⇔⇔ **P/E/TX**⇔⇔⇔