Y/K/TX

Reg. No: 21BCE

VIT
Vellore Institute of Technology

Final Assessment Test – November 2024

Course: BCSE309L - Cryptography and Network Security
Class NBR(s): 2351 Slot: A
Time: Three Hours Max. M

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

Answer ALL Questions
(10 X 10 = 100 Marks)

1. (a) Solve the following using suitable methods. The problem has to be solved in steps. [3+7]

$$16^{-100} \bmod 41$$

(b) Solve the following

$$(8^9 + 9^8 + 10^6 + 11^7 + 12^8 + 13^9) \bmod 7$$

2. (a) Prove whether 7 is a primitive root of 13 in steps. [4+6]

(b) In a gift box, there were many balloons. The balloons had to be distributed to children participating in a birthday party. When 11 balloons were given to each child, 5 were left over. So, the host starts all over again and gives 9 balloons to each child and now around 7 is left over. The host then gives 7 and now nothing was left over. Find out how many balloons were there in the gift box?

3. Implement the Stream Cipher RC4 algorithm for the State vector 'S' initialized with values ranging from 0 to 7 where the Key K is [1 2 3 5] and the Plaintext P is given by [1 2 3 2]. Find out the Cipher bitstream C.

4. Find the Plain Text using SDES decryption for the following Cipher Text 0111 0111. Let the key for Round1 (K_1) and key for Round2 (K_2) be 1010 0100 and 0100 0011 respectively.

IP							
2	6	3	1	4	8	5	7

IP^{-1}							
4	1	3	5	7	2	8	6

E/P							
4	1	2	3	2	3	4	1

S0 = [1,0,3,2 S1= [0,1,2,3
3,2,1,0 2,0,1,3
0,2,1,3 3,0,1,0
3,1,3,2] 2,1,0,3]

P4			
2	4	3	1

5. In Elgamal cryptosystem, global prime q =101 and its primitive root g=2. Alice chooses private key X_A=35 and Bob chooses his private key X_B = 19. Bob wants to encrypt the message(m) =17. Find the ciphertext describing each step in detail.

6. Assume Global prime p= 19, its primitive root (α)= 3, Alice selected her private key as X_A = 5, Bob selected his private key as X_B = 9. Find the public keys of Alice and Bob. Show the scenario of man in the middle attack where Darth assumes private key of Alice as X_{D1} =2 and private key of Bob as X_{D2}=7

7. a) In SHA-512, the 8, 64bit buffers a, b, c, d, e, f, g and h are initialized to the following hex values. [6+4]

a = 6A09E667F3BCC908 e = 510E527FADE682D1
b = BB67AE8584CAA73B f = 9B05688C2B3E6C1F
c = 3C6EF372FE94F82B g = 1F83D9ABFB41BD6B
d = A54FF53A5F1D36F1 h = 5BE0CD19137E2179

Compute and show how the first 3 hex digits of buffer 'b' are computed.

b) In SHA-512, we take each 1024bit message subblock and perform 80 rounds. For each of these rounds, we need to derive a 64bit word W_t from the message subblock where t varies from 0 to 79. Explain with a neat block diagram how the key expansion happens in SHA-512.

8. Given parameters (p,q,h) =(31,5,3) and Alice's private key (x)= 4; Alice's random integer k is 3. Hash of message H(M)=21. Generate digital signature using Digital Signature Standard (DSS) and verify the same.

9.a) Describe how Kerberos-V4 provides authentication service in an open distributed environment where users work in different workstations and access services from the servers distributed throughout the network.

OR

9.b) Transport layer security is a transport layer protocol that enables secure communication in Internet. Describe its function, the issues addressed by it and the benefits achieved.

10.a) In a military application, it is desired to enforce email security as the adversaries are constantly watching and monitoring the communication channel to tap the mail contents. Suggest a suitable protocol that provides email security with the necessary block diagrams.

OR

10.b) An online textile business aims to achieve secure E-commerce credit card transactions. Suggest a suitable protocol in Internet which addresses this issue. Describe how the same can be adapted to improve security in the current business scenario stated.

⇔⇔⇔ Y/K/TX ⇔⇔⇔