Pandit Deendayal Energy University

B.Tech. (CSE) – Sem V

Information Security (20BCP304T) Assignment

Final Submission Deadline : 5 Nov 2023

1. In an RSA cryptosystem, a particular A uses two prime numbers p = 13 and q =17 to generate her public and private keys. If the public key of A is 35. Then the private key of A is?
2. Using p=3, q=13, d=7 and e=3 in the RSA algorithm, what is the value of cipher text for a plain text 5?
3. Suppose that two parties A and B wish to set up a common secret key (D-H key) between themselves using the Diffie Hellman key exchange technique. They agree on 7 as the modulus and 3 as the primitive root. Party A chooses 2 and party B chooses 5 as their respective secrets. What is their shared D-H key ?
4. In a Diffie-Hellman Key Exchange, Alice and Bob have chosen prime value q = 17 and primitive root = 5. If Alice's secret key is 4 and Bob's secret key is 6, what is the secret key they exchanged?
5. What is trapdoor one-way function?
6. Explain knapsack cryptosystem.
7. Name 7 categories of attacks on RSA. Explain any five in detail.
8. Discuss the security issues in
   a) cipher feedback mode
   b) output feedback mode
9. Explain why there is no need for ciphertext stealing in CFB, OFB, and CTR modes.
10. A) What is the need of S-box? Explain two types of S-boxes.
    B) What is the need of D-box? How many types of D-boxes can be used in modern block ciphers?
11. Name any 10 components used in modern block ciphers.
12. Differentiate between the two classes of product cipher.
13. Distinguish between synchronous and asynchronous stream ciphers.
14. Name any two block ciphers influenced by DES.
15. Comment on the weaknesses in DES due to
    a) Design of S-box
    b) Design of D-box
    c) Key size
16. Explain the steps in 1 round of AES with example.
17. List the criteria defined by NIST for AES.
18. Find the inverse of 550 in GF(1759) using extended Euclidean Theorem.
19. Prove the secret exchange of key proposed by Diffie Hellman.

20. A) Explain with an example how meet in the middle attack is possible in Diffie Hellman key exchange.

    B) Prove meet in the middle attack in Diffie Hellman key exchange.

21. Describe pseudorandom number generation based on RSA.

22. Illustrate Elgamal cryptographic system.

23. On the elliptic curve over the real numbers $y^2 = x^3 - \frac{17}{12}x + 1$, let P=(0,1) and Q=(1.5,1.5). Find P+Q and 2P.

24. Solve for the elliptic curve encryption/ decryption. The cryptosystem parameters are $E_{11}(1,6)$ and G=(2,7). B's private key is n_B=7.

    a) Find B's public key P_B

    b) A wishes to encrypt the message P_m= (10,9) and chooses the random key k=3. Determine the ciphertext C_m.

    c) Show the calculation by which B recovers P_m from C_m.

25. You want to secretly send a message to your friend using public key cryptography. Which one would you prefer: RSA or ECC? Justify your choice.

26. a) Identify the security service(s) offered by the models described in

    i. FIGURE 1 ii. FIGURE2 iii. FIGURE 3

    b) Give suggestions to improve the cryptography model described in FIGURE 3 so that it is resistant to release of message content attack.

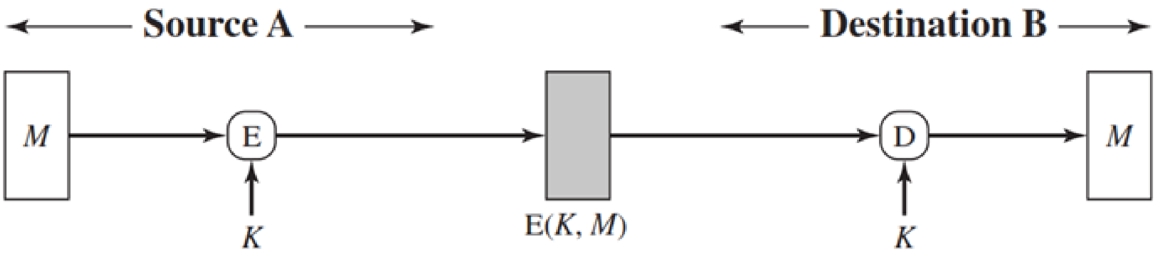

FIGURE 1

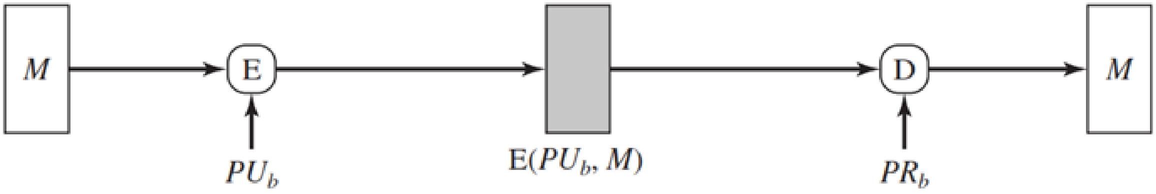

FIGURE 2

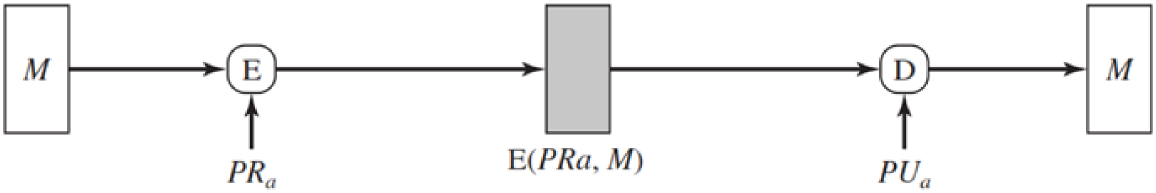

FIGURE 3