IS (SYMCA)

1. Define threat and vulnerability.
2. What is CIA (Confidentiality, Integrity and Availability)?
3. Compare Authentication and Authorization.
4. Compare between stream cipher and block cipher. Why is it important to study Feistel cipher?
5. Write AES key expansion algorithm.
6. Briefly describe AddRoundKey transformation in AES.
7. Briefly describe the key expansion algorithm of AES.
8. Compare between public key cryptosystems and private key cryptosystems.
9. Which are different block cipher modes of operation? Give application of each.
10. Explain output feedback mode operation.
11. Define TRNG, PRNG and PRF.
12. Apply RSA algorithm to encrypt and decrypt following data.
    p = 3, q = 11, e = 7, M = 5
13. Apply AddRoundKey transformation of AES cryptosystem. Given 128 bits of state and 128 bits of the round key.

47	40	A3	4C
37	D4	70	9F
94	E4	3A	42
ED	A5	A6	BC

AC	19	28	57
77	FA	D1	5C
66	DC	29	00
F3	21	41	6A

14. Determine disadvantages of traditional authentication methods and find requirements of biometric security scheme?
15. i) Construct a Playfair matrix with the key *occurrences.*
    ii) Apply Transposition technique to encrypt the message “this is online exam” with a rail fence technique.