

Roll No.

Total Pages : 4

221309

May, 2019

**M.Tech. (ECE) - III SEMESTER (Reappear)
Security in Communication Network (E16C-707C)**

Time : 3 Hours]

[Max. Marks : 75

Instructions :

1. *It is compulsory to answer all the questions (1.5 marks each) of Part-A in short.*
2. *Answer any four questions from Part-B in detail.*
3. *Different sub-parts of a question are to be attempted adjacent to each other.*

PART-A

1. (a) What is OSI security architecture? (1.5)
- (b) What should be the minimum length of secret key in a cryptosystem that cannot be cracked by brute-force means within a reasonable period of time? Justify your answer. (1.5)
- (c) Briefly describe web security threats and their consequences. (1.5)
- (d) What services are provided by IPsec? (1.5)

221309/20/111/454

[P.T.O.
23/5

- (e) Which operation is used in the Fiestel cipher? Give its expression. (1.5)
- (f) How many rounds a Data Encryption Standard (DES) system has with an initial and final permutation block? What is the size of key in each round? (1.5)
- (g) Advanced Encryption Standard (AES), has three different configurations with respect to _____ and _____. List all the configurations. (1.5)
- (h) For RSA (modulus $n = pq$, where p and q are distinct primes and d is the secret exponent) to work, value of P (plaintext) must be less than which parameter for correctness of decryption? (1.5)
- (i) What is the last digit of 17^{17} ? (1.5)
- (j) Give the Input and Output block size for SHA-1 and MD-5 (1.5)

PART-B

- 2. (a) What is the difference between passive and active attack? List and define categories of passive and active security attacks. (7.5)
- (b) Alice publishes her RSA public key : modulus $N = 77$ and exponent $e = 37$. Bob wants to send Alice the message $m = 2$. What cipher text does bob send to Alice? Explain each step in detail. (7.5)

- 3. (a) List and explain the major security services provided by AH and ESP. (7.5)
- (b) What is Key distribution center? Describe its role in security applications. (7.5)
- 4. (a) What is the difference between a block cipher and a stream cipher? What is the purpose of S-boxes in DES? (7.5)
- (b) What are the principal elements of a public-key cryptosystem? What are the roles of the public and private key? (7.5)
- 5. (a) How many properties a Hash function must satisfy? Explain with suitable examples. Which property indicates that it must be extremely difficult to create the message if the message digest is given? (7.5)
- (b) Enlist different cipher block modes of operation. Explain any *two* in detail. (7.5)
- 6. (a) Alice and Bob agree to use the prime $p = 5$ and the primitive root $g = 2$. Alice chooses the secret key $a = 4$ and Bob chooses the secret key $b = 3$. Then, using Diffie-Hellman Key Exchange Protocol, what is the common secret key share between Alice and Bob. Explain the algorithm in detail. (7.5)

(b) What are the properties a digital signature should have?
In what order should the signature function and the confidentiality function be applied to a message and why? (7.5)

7. Explain in detail the widely used web traffic security approaches. Compare all the approaches. (15)
