# 2019

# COMPUTER SCIENCE

## Paper : CSM-304

## (Cryptography and Network Security)

**Full Marks : 70**

*The figures in the margin indicate full marks.*

*Candidates are required to give their answers in their own words as far as practicable.*

Answer ***question no.*** **1, 2** and ***any four*** from the rest.

1. Answer ***any five*** from the following : 2×5

(a) Distinguish between Diffusion and Confusion.

(b) Find out the multiplicative inverse of each non zero element in $Z_5$.

(c) Is it possible to perform encryption operations in parallel on multiple blocks of plaintext?

(d) What is Euler's Totient function? Compute the value of $\phi(231)$.

(e) Is AES a Feistel cipher? Justify your answer.

(f) State the Extended Euclidian algorithm. What is it's application in cryptography?

(g) State the importance of Galois field in cryptography.

(h) What do you mean by Packet sniffing?

(i) Give an example of 'reflection attack'.

2. Answer ***any five*** from the following : 4×5

(a) Describe the utility of Trap-door-one way function in context of RSA encryption.

(b) Compute $21^{24}$ mod 8 using fast exponentiation. Show each steps.

(c) Show that the group $< Z_{10^*}, X>$ is s cyclic group.

(d) Discuss the role of Key Distribution Centre in Secret Key cryptography.

(e) 'Meet-in the Middle' attack is a specific attack for 2-DES'– Explain.

(f) State the principle of Zero Knowledge authentication. Is it better than Challenge-Response approach?

(g) Determine the multiplicative inverse of $X^3 + X + 1$ in GF $(2^4)$ with irreducible polynomial $X^4 + X + 1$.

(h) What is Key wrapping? Comment on the strength of this approach.

**Please Turn Over**

3. Describe the block diagram of AES encryption. "Mixing transformation i.e. "Mix-column" is needed in AES but not needed in DES"– Comment on the statement with justification. Compare the performance of AES over DES. 3+5+2

4. Describe the possible classification of attacks, based on the information known to an attacker. Discuss a possible attack on RSA. Is there any advantage(s) of using Eliptic curve over RSA? 4+3+3

5. State the conditions that a has *h* function should satisfy. Prove that the difficulty of an alternative collision attack in message integrity is proportional to $2^{n/2}$. Is there any difference between Message Authentication Code and Message Digest? Justify your answer. 3+5+2

6. How the problem of Key exchange is addressed in IP Sec? State the purpose of a firewell. How an application gateway firewall offers the security? State the difference between http and https protocol. 5+1+3+1

7. "Sub-key generation process also affects the strength of an encrytion technique"– Discuss the issue in context of DES algorithm. Discuss the Miller Rabin test for primality testing. State the principal difference between Tunnel mode and Transport mode implementation of IP Sec. 3+4+3

8. In context of ElGamal cryptosystem, Describe the Key generation and encryption-decryption process. Comment on the security of the system. How it can be used to prepare digital signature? 4+2+4

9. How is SHTTP different from SSL? State the role of CA and RA. What are the basic approache(s) to bundle SA? State the purpose of DMZ. 2+2+4+2