No. of Printed Pages : 4

Sl. No.

C8-R4 : INFORMATION SECURITY

DURATION : 03 Hours **MAXIMUM MARKS : 100**

Roll No. : | | | | | | |

Answer Sheet No. : | | | | | | |

Name of Candidate : _____ **; Signature of Candidate :** _____

INSTRUCTIONS FOR CANDIDATES :

- Carefully read the instructions given on Question Paper, Answer Sheet.
- Question Paper is in English language. Candidate has to answer in English Language only.
- **Question paper contains Seven questions. The Question No. 1 is compulsory. Attempt any FOUR Questions from Question No. 2 to 7.**
- **Parts of the same question should be answered together and in the same sequence.**
- **Questions are** to be answered in the **ANSWER SHEET** only, supplied with the Question Paper.
- **Candidate cannot leave the examination hall/ room without signing on the attendance sheet and handing over his/her Answer Sheet to the Invigilator. Failing in doing so, will amount to disqualification of Candidate in this Module/Paper.**
- After receiving the instruction to open the booklet and before answering the questions, the candidate should ensure that the Question Booklet is complete in all respects.

DO NOT OPEN THE QUESTION BOOKLET UNTIL YOU ARE TOLD TO DO SO.

1. (a) Specify the four categories of security threats.

(b) Explain simplified DES with example.

(c) Differentiate between confidentiality and authentication.

(d) Convert "MEET ME" using Hill cipher with the key matrix. Also, convert the cipher text back to plaintext.

(e) Compare stream cipher with block cipher with example.

(f) What is the difference between link and end-to-end encryption ?

(g) Explain ECC - Diffie Hellman key Exchange with both keys in detail with an example. **(7x4)**

2. (a) Describe RSA algorithm in detail. Calculate the private key of A where in RSA cryptosystem a particular A uses two prime numbers $p = 13$ and $q = 17$ to generate her public and private keys. Let the public key of A is 35.

(b) Explain the concept of block cipher and stream cipher in cryptography. Discuss the modes of operations of block cipher. **(12+6)**

3. (a) State and prove Fermat's theorem. Use Fermat theorem to find a number 'a' between 0 and 72 with $a \equiv 9794 \bmod 73$.

(b) Describe how Diffie-Hellman algorithm used for key exchange is vulnerable to man in middle attack. Determine the shared secret key in a Diffie-Hellman scheme with a common prime 71 and primitive root 7. Given the private keys of the communicating parties A and B are 5 and 12 respectively. **(9+9)**

4. Compute the values of the following :

(a) $\Phi(35)$

(b) $3^{55} \bmod 11$

(c) gcd (2070, 1009) **(6+6+6)**

5. (a) Draw a block level diagram to depict the signature of one round of DES. Prove that if plaintext block and encryption key are complemented then resulting cipher text block of DES encryption is also complemented.

(b) What is Digital Certificate ? Give the format of X.509 certificate showing the important elements of the certificate. How is an X.509 certificate revoked ? **(9+9)**

6. (a) Explain Chinese Remainder Theorem (CRT) and find X for the given set of congruent equations using Chinese Remainder Theorem.

$X = 1 \bmod 5$

$X = 2 \bmod 7$

$X = 3 \bmod 9$

$X = 4 \bmod 11$

(b) What is the most security-critical component of DES round function ? Give a brief description of this function. **(9+9)**

7. (a) Discuss the design of S-Box of AES. How it differs from the S-Boxes of DES ?

(b) Explain the sequence of steps involved in the message generation and reception in Pretty Good Privacy (PGP) with block diagrams. **(9+9)**

- o O o -

SPACE FOR ROUGH WORK