This question paper contains **4+1** printed pages] 4/11/19 M

Roll No. □□□□□□□□□□□

S. No. of Question Paper : **7946**

Unique Paper Code : **32357506** **J**

Name of the Paper : **Cryptography and Network Security**

Name of the Course : **B.Sc. (Hons.) Mathematics : DSE-1**

Semester : **V**

Duration : **3 Hours** Maximum Marks : **75**

(Write your Roll No. on the top immediately on receipt of this question paper.)

All questions are compulsory.

Attempt any *five* parts from question **1**, each part carries **3** marks.

Attempt any *two* parts from questions **2** to **6**, each part carries **6** marks.

1. (*a*) Define a stream cipher. State the *three* important design considerations for a stream cipher.

(*b*) Briefly describe ShiftRows transformation of AES.

(*c*) What is an Avalanche effect ? Does DES show avalanche effect ? Justify your answer.

P.T.O.

M.phil

(*d*) What is an ideal block cipher ? Why it cannot be used practically ?

(*e*) What does SHA stand for in SHA family of hash functions ? Mention any *two* hash functions from SHA family with the length of message digest.

(*f*) Write the general equation of an Elliptic curve. State the Discrete Log Problem over the Elliptic curve

(*g*) Describe requirements of a good digital signature scheme.

2. (*a*) Encrypt the message "CRYPTO" using the Hill Cipher with the key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$. What is the decryption matrix ?

(*b*) Explain the Feistel structure of a block cipher with the help of a diagram.

(*c*) Discuss various types of active and passive security attacks on a communication network.

3. (*a*) Use the Euclidean Algorithm to find the multiplicative inverse of 5994 modulo 20736.

(*b*) Identify GF(2^8) with the field of polynomials over GF(2) modulo $m(x) = x^8 + x^4 + x^3 + x + 1$. If the byte $b_7b_6b_5b_4b_3b_2b_1b_0$ represents the polynomial $b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$ in the field, find the product :

(01010111) × (10111011).

(c) State Fermat's Theorem. Is the converse true ? Justify your answer.

4. (*a*) Describe the forward and inverse SubBytes transformation of AES and the rationale behind it.

(*b*) Represent the hexadecimal {53} as a bit-string and a polynomial. Find the inverse of the polynomial obtained in GF(2^8) modulo irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$.

(*c*) State the Chinese Remainder Theorem. If $x \equiv 23 \bmod 37$ and $x \equiv 34 \bmod 49$ then find x.

5. (*a*) Perform encryption and decryption using the RSA algorithm for $p = 5$, $q = 7$, $e = 7$ and M = 12.

(*b*) Consider the following Key exchange mechanism known a *Elliptic Curve Key exchange* :

Step 1 : Alice and Bob chooses an elliptic curve $y^2 = x^3 + rx + s$ over the field GF(p), p is prime with an element G of order n on this curve.

Step 2 : Alice chooses secret $a < n$ and sends a.G to Bob.

Step 3 : Bob chooses secret $b < n$ and sends b.G to Alice.

Step 4 : Alice calculates $a.(b.\text{G}) = ab\text{G}$.

Step 5 : Bob calculates $b.(a.\text{G}) = ab\text{G}$. Thus Alice and Bob have same shared secret key abG.

Suppose Alice and Bob chooses an elliptic curve $y^2 = x^3 + x + 6$ over the field GF(11) and G = (2, 7) on this curve. Alice and Bob selected secret keys $a = 2$, $b = 3$ respectively. Given 3G = (8, 3), find the secret key shared by Alice and Bob.

(*c*) Through help of a diagram show how hash function can be used to achieve integrity, authentication and confidentiality using only a symmetric key encryption scheme.

6. (*a*) Describe the Elgamal Digital signature scheme, that is, its public/private parameters, signing algorithm and verification algorithm.

(*b*) Write the services provided by PGP. Mention the different Symmetric key schemes, Public Key schemes and Hash function used in PGP.

(*c*) Describe a hash function. What is the main functionality of a hash function in a cryptographic secure communication mechanism ? Give *three* applications of hash functions, clearly specifying role of hash function in each application.