This question paper contains 4+1 printed pages]

Roll No. | | | | | | | | | | |

S. No. of Question Paper : 8086

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 No. 1, each part carries 3 marks.

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

1. (*a*) Use the Rail fence cipher of depth 3 to encrypt "there could be better questions." Which attack is this cipher vulnerable to ?

(*b*) Explain the term diffusion in the context of a block cipher. How does DES achieve diffusion ?

(*c*) What is the difference between a stream cipher and a block cipher ?

P.T.O.

(*d*) Describe a trap-door-one-way function.

(*e*) Define Euler totient function ϕ. Compute ϕ (105).

(*f*) Write the order in which Compression, Encryption and Digital Signatures are applied in PGP, while achieving both Authentication and Confidentiality, clearly state the reason behind this order.

(*g*) Describe the terms Non-Repudiation and Integrity in context of Cryptography. Mention the cryptographic primitives used to achieve these.

2. (*a*) Decrypt the following message encrypted using playfair cipher with the key "HER MAJESTY'S SHIP".

LVHZ CRJE RQQO ZRTY ERGM JRRM XOJR RANF RMOW ODNM AHYN WDER NMFM.

(*b*) What does it mean to say that the one time pad is unbreakable ? If the one time pad is unconditionally secure, why is it not widely used ?

(*c*) Describe the key expansion algorithm of DES with the help of a diagram.

3. (*a*) For any positive integers a and n, show that $b \equiv c \pmod{n}$ implies $ab \equiv ac \pmod{n}$. Show that converse is not true in general. In which case converse is also true ?

(*b*) Determine the GCD of $x^4 + 2x^3 + 5x^2 + 5x + 4$ and $x^3 + 2x^2 + 3x + 6$ over GF(7).

(*c*) State Fermat's Theorem. Use Fermat's Theorem to reduce $8^{109} \pmod{37}$.

4. (*a*) Describe the general structure of the encryption process in AES with the help of a diagram. Briefly comment on the various transformations performed in each round.

(*b*) Suppose that we have the following 128-bit AES key, given in haxadecimal notation :

287E151628AED2A6ABF7158809CF4F3C

(*i*) Express the initial round key (w_0 w_1 w_2 w_3) as a State matrix.

(*ii*) Given that RC[1] = 01, S(09) = 01, S(CF) = 8A, S(4F) = 84 and S(3C) = EB, where S denotes the S-box, calculate the first four bytes (w_4) for round one.

) Define the discrete logarithm of a number b for the base a $(mod\ p)$. Prove that : $dlog_{a,p}\ (xy) = [dlog_{a,p}\ (x) + dlog_{a,p}\ (y)]\ (mod\ \phi(p))$.

5. (*a*) Perform encryption and decryption using the RSA algorithm for $p = 7$, $q = 13$, $e = 5$ and $M = 8$.

(*b*) The public parameters of Alice consists of an elliptic curve $y^2 = x^3 + x + 6$ over the field GF(11) and a point G = (2, 7) on this curve. Suppose Alice's private key is $a = 2$. Bob sends the ciphertext ((8,3), (5,9)) to Alice. Find the message sent by Bob to Alice.

(*c*) For the elliptic curve $y^2 = x^3 + x + 6$ over the field GF(11) :

(*i*) Calculate P + Q, where P = (5,2), Q = (8, 3).

(*ii*) Calculate 2P, where P = (5,2).

6. (*a*) What is the maximum input size and length of output of hash function SHA-512. State the value of padding field and length fields if the message length is 1920 bits. What is the size of word (register used) in SHA-512 ?

(*b*) Alice uses Flgamal Digital signature scheme to sign a document with the parameters : A cyclic group GF(19) with generator $a = 10$ and private key $X = 16$. He generated the random $K = 5$, gcd $(K, 18) = 1$ as part of signing process. If Alice signed the document with hash value $m = 14$, claculate the signature.

(*c*) Define Digital Signatures, its parameters, input/output, and general working of signing and verification algorithms. Define three types of attacks on a Digital signature.