(Following Paper ID and Roll No. to be filled in your Answer Book)

PAPER ID : 2757 Roll No. | | | | | | | | | | |

B.Tech.

(SEM. VII) ODD SEMESTER THEORY EXAMINATION 2012-13

CRYPTOGRAPHY AND NETWORK SECURITY

Time : 3 Hours *Total Marks : 100*

Note : *(1) Attempt **all** questions.*

(2) All questions carry equal marks.

(3) Notations/Symbols/Abbreviations used have usual meaning.

1. Attempt any **FOUR** parts of the following :

(a) Compare and contrast between the following :

(i) Monoalphabetic substitution cipher and Polyalphabetic substitution cipher.

(ii) Encryption and Steganography.

(iii) Known plaintext attack and Chosen plaintext attack.

(b) Some block cipher modes of operation use only encryption while others use encryption and decryption both. Why ?

(c) Draw the block diagram showing the structure of Fiestal cipher. Write down the important features of the Fiestal structure.

(d) Discuss the role of S-boxes in DES cipher.

(e) How is a Hill cipher vulnerable to chosen plaintext attack ?

(f) Explain the concept of differential cryptanalysis.

2. Attempt any **FOUR** parts of the following :

(a) Define Euler totient function. State and prove Euler's theorem.

(b) Describe RSA algorithm. Suppose in a public key system using RSA, the two prime numbers are $p = 17$ and $q = 31$. The public key is $e = 7$. Determine the private key. Perform the encryption and decryption of message $m = 2$.

(c) Define Cyclic Group. Does the set of residue class modulo 11 excluding 0 form a cyclic group with respect to multiplication modulo 11 ? Prove that a cyclic group is abelian.

(d) What is discrete logarithmic problem ? Find all the primitive roots of 25.

(e) Use extended Euclidean algorithm to find multiplicative inverse of 1234 mod 4321.

(f) Write Miller Rabin algorithm for testing the primality of a given number.

3. Attempt any **TWO** parts of the following :

(a) Describe the Digital Signature Algorithm (DSA) of Digital Signature Standard. What happens if a k value (User's per-message secret number) used in creating DSA signature is compromised ?

(b) (i) What is hash function ? List the requirements of a hash function ? In what ways, can a hash value be secured to provide message authentication ?

(ii) What are properties of a digital signature ? Differentiate between direct and arbitrated digital signature.

(c) What do you understand by birthday attack ? With the help of suitably chosen scenario, explain how a birthday attack can be launched.

4. Attempt any **TWO** parts of the following :

(a) Write and explain Diffie-Hellman scheme for exchange of the secret key. Users A and B use a Diffie-Hellman key exchange protocol with a chosen common prime $p = 11$ and a primitive root $g = 2$. Given that public keys of A and B are 9 and 3 respectively. Determine the shared secret key K.

(b) What do you understand by digital certificate ? Give format of X.509 digital certificate. What are forward and reverse certificates ? How is an X.509 certificate revoked ?

(c) What are the steps used by PGP to send a signed secret message ? Describe the structure of public and private key rings of PGP. Why owner trust field of a public key is not enough to permit PGP to use that public key ?

5. Write short notes on any **TWO** of the following :

(a) Secure Electronic Transaction (SET)

(b) IPSec

(c) Firewalls.