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

PAPER ID : 2870 Roll No. | | | | | | | | | | |

B.Tech.

(SEM. VIII) EVEN THEORY EXAMINATION 2012-13

CRYPTOGRAPHY AND NETWORK SECURITY

Time : 3 Hours *Total Marks : 100*

Note :– (i) Attempt **ALL** questions.

(ii) All questions carry equal marks.

(iii) Notations/ Symbols/ Abbreviations used have usual meaning

(iv) Make suitable assumptions, wherever required.

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

(a) Explain the following terms :

(i) Replay attack

(ii) Traffic analysis

(iii) Access Control

(iv) Message Integrity

(v) Trojan Horse.

(b) Discuss the strengths of pure substitution cipher and pure transposition cipher against statistical analysis.

(c) List various modes of operation of block ciphers. Give advantages and disadvantages of each.

(d) Prove that if plaintext block and encryption key are complemented in DES then resulting ciphertext block of DES encryption is also complemented.

(e) What are the characteristics of a Ideal Cipher ?

(f) Explain the concept of differential cryptanalysis. You may choose suitable example for illustration.

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

(a) Determine all invertible residue classes modulo 25 and determine their inverses.

(b) Define Group, Semi Group and Sub Group. Determine all the primitive roots of 13.

(c) Write RSA algorithm for encryption and decryption explain the reasons behind choice for various parameters of the algorithm.

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

(e) Using Fermat's theorem, obtain $3^{201} \bmod 11$.

(f) Write and explain the Miller Rabin primality test. Apply Miller-Rabin Algorithm using base 2 to test whether the number 561 is composite or not.

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

(a) Consider a n-bit hash function H. H is applied to k random inputs. Prove that probability of at least one duplicate (i.e. $H(x) = H(y)$ for some distinct x, y) is more than ½ for $k = \sqrt{2^n}$.

(b) What properties should a digital signature scheme satisfy ? Describe the Signature generation process of Digital Signature Standard.

(c) (i) What is difference between weak collision resistance and strong collision resistance ?

(ii) What is the order of effort required to launch birthday attack on SHA.

(iii) With DSS, why do signatures of the same message, signed on different occasions, differ ?

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

(a) Describe how Diffie-Hellman algorithm used for key exchange is vulnerable to man in the 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.

(b) What were the requirements defined for Kerberos. Write and explain the seqence of message exchanges in Kerberos Version 4.

(c) Give a general format of PGP message. Why does PGP generate a signature before applying compression ?

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

(a) Secure Electronic Transaction (SET)

(b) Firewalls

(c) Intrusion detection.