(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 2011-12

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.

(4) Make suitable assumptions, wherever required.

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

(a) Differentiate between the following terms clearly :—

(i) Cryptography and Steganography

(ii) Active attack and Passive attack

(iii) Stream Cipher and Block Cipher.

(b) What is polyalphabetic cipher ? Compare its strength with that of monoalphabetic cipher.

(c) What do you understand by chosen plaintext attack ? Hill cipher is vulnerable to chosen plaintext attack. How ?

(d) Draw block diagram of DES cipher showing size of input/output of every block. How important is swapping step at the end of every round ?

(e) Describe the Output Feedback (CFB) mode of a block cipher. If a bit error occurs in the transmission of a ciphertext character in a 8-bit CFB mode, how far does the error propagate ?

(f) Give an analysis of strength of Triple DES compared to Double DES.

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

(a) Determine the multiplicative inverse of 1234 mod 4321 using extended Euclid's algorithm.

(b) Define order of an element of Group. Prove that order of every element of a finite group is finite.

(c) In RSA cryptosystem, given that modulus n is 100 and public key e is 13. Determine the private key.

(d) Determine result of multiplication of polynomials $(x^5 + x^2 + x)$ and $(x^7 + x^4 + x^3 + x^2 + x)$ in $GF(2^8)$ with irreducible polynomial $(x^8 + x^4 + x^3 + x + 1)$.

(e) State Chinese Remainder theorem. Use it to solve the following simultaneous congruences :—

$$x \equiv 1 \bmod 5,\ x \equiv 5 \bmod 8,\ x \equiv 3 \bmod 13.$$

(f) State and prove Euler's theorem. Compute the value of Euler's totient function $\Phi(300)$.

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

(a) Write the signature generation and verification process of digital signature Algorithm of Digital Signature Standard.

(b) Discuss at least one approach that can be used to launch a birthday attack on a message authentication code.

(c) (i) What is difference between direct digital signature and arbitrated digital signature ?

(ii) What are the requirements of a message authentication code (MAC) ?

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

(a) What are the services provided by PGP ? Explain the various attributes stored in public key ring. Give the sequence of steps that a receiving PGP entity performs for decrypting the received message.

(b) Write and explain Diffie-Hellman algorithm used for key exchange.

(c) Give general format of X.509 certificate. How is an X.509 certificate revoked ?

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

(a) IP Security (IP Sec)

(b) Secure Socket Layer (SSL)

(c) Malicious Software.