Printed Pages : 3

ECS-084

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

PAPER ID : **110854**

Roll No.

B. Tech.

(SEM. VIII) THEORY EXAMINATION, 2014-15

CRYPTOGRAPHY & NETWORK SECURITY

Time : **3** Hours] [Total Marks : **100**

Note: 1. Attempt all questions.
2. All question carry equal marks.
3. Notations/Symbols/Abbreviations used have usual meaning.
4. Make suitable assumption ,whereever required.

1 Attempt any four parts of following (5×4=20)

(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 monoalphabetic cipher.

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

(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) Give general format of a PGP message. Explain why PGP generates a signature before applying compression?

(f) Describe the encryption and decryption process of a block cipher in Cipher Feedback(CFB) mode.

2 Attempt any four parts of following (5×4-20)

(a) Describe RSA algorithm. Whether RSA encryption and decryption works or not if message m has common factor with modulus n of the scheme.

(b) Define group. What is multiplication in use ?

(c) Give comparison of AES Cipher to the DES cipher.

(d) State Chinese Remainder theorem. Use it to solvc the following simultaneous congruence $x \equiv 4 \bmod 7, x \equiv 4 \bmod 13, x \equiv 5 \bmod 12$.

(e) State and prove Euler's theorem. Compute the value of Euler's totient function for 300.

(f) State and prove Fermat's theorem.

3 Attempt any two parts of the following (10×2=20)

(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 message authentication code.

(c) Draw a block level diagram to depict the structure of one round of DES. Prove that if plaintext block and encryption key are complemented then resulting ciphertext block of DES encryption is also complemented.

4 Attempt any two parts of the following (10×2=20)

(a) Explain the concept of dual signature in context of Secure Electronic Transaction(SET).Briefly describe the sequence of events that are required for a SET transaction.

(b) Describe the approaches used for intrusion detection.

(c) What is kerboros? What requirements were defined for Kerberos? Describe the sequence of message exchanges of kerberos Version 4.

5 Attempt any two parts of the following (10×2=20)

(a) What is permutation cipher? Whether permutation ciphers are susceptible to the statistical analysis or not? Discuss Encryption key in a permutation cipher is (3,7,2,6,1,8,5)

(b) Write short notes on any two

(i) IP Security(IP Sec)

(ii) Secure Socket Layer

(iii) Malicious Software

(c) What is S/MIME? Why is it used? What are the main functions S/MIME provides?