Reg. No. : | | | | | | | | | | | | |

Question Paper Code : 91567

B.E./B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2014.

Seventh Semester

Computer Science and Engineering

IT 2352/IT 62/10144 IT 603/10144 CSE 46 — CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Sixth Semester – Information Technology)

(Regulation 2008/2010)

(Common to PTIT 2352 – Cryptography and Network Security for B.E. (Part-Time) Seventh Semester – Computer Science and Engineering – Regulation 2009)

Time : Three hours Maximum : 100 marks

(Codes / Tables / Charts to be permitted, if any, may be indicated)

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Decipher the following cipher text using brute force attack :

   CMTMROOEOORW (Hint : Algorithm – Railfence)

2. What are the two basic functions used in encryption algorithms?

3. Point out the types of cryptanalytic attacks.

4. What are the performance differences between MD5, SHA-512 and RIPEMD-160?

5. Is it possible to use the DES algorithm to generate message authentication code? Justify.

6. What are the protocols used to provide IP Security?

7. List the difference between stream and block cipher.

8. What are the security services provided by Digital Signature?

9. Differentiate macro Virus and boot Virus.

10. Sketch the general format for PGP message.

PART B — (5 × 16 = 80 marks)

11. (a) Encrypt the message "PAY" using Hill cipher with the following key matrix and show the decryption to get the original plain text.

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}.$$

Or

(b) Write short notes on :

(i) Fermat and Euler's theorem (8)

(ii) Chinese Remainder theorem. (8)

12. (a) Brief out the encryption and decryption process of DES and depict the general structure. List out the strengths and weaknesses of the same.

Or

(b) Describe the mathematical foundations of RSA algorithm. Perform encryption and decryption for the following.

$p = 17, q = 7, e = 5, n = 119$, message = "6"

Use Extended Euclid's algorithm to find the private key.

13. (a) Explain the process of deriving eighty 64-bit words from the 1024-bits for processing of a single block and also discuss single round function in SHA-512 algorithm. Show the values of W_{16}, W_{17}, W_{18}, and W_{19}.

Or

(b) Explain Diffie-Hellman key exchange algorithm with an example. Consider a Diffie-Heliman scheme with a common prime $q = 353$ and a primitive root $\alpha = 3$. Users A and B have private keys $X_A = 17, X_B = 21$ respectively. What is the shared secret key K_1 and K_2?

14. (a) Alice chooses $Q = 101$ and $P = 7879$. Assume (q, p, g and y): Alice's Public Key. Alice selects h=3 and calculates g. Alice chooses $x = 75$ as the private key and calculates y. Now, Alice can send a message to Bob. Assume that $H(M) = 22$ and Alice choose secret no $K = 50$. Verify the Signature.

Or

(b) For what purpose Zimmerman developed PGP? Brief the various services provided by PGP. Discuss the threats faced by an e-mail and explain its security requirements to provide a secure e-mail service.

15. (a) Explain NIST and VISA International Security Models and list the evaluation criteria set by it.

Or

(b) Discuss the architecture of distributed intrusion detection system with the necessary diagrams. Illustrate the three common types of firewalls with diagrams.

———————