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

# Question Paper Code : 31160

B.E./B.Tech. DEGREE EXAMINATION, MAY/JUNE 2013.

Seventh Semester

30th AN

Computer Science and Engineering

080230043 — CRYPTOGRAPHY AND NETWORK SECURITY

(Regulation 2008)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Define Notarization.

2. Give an example for Caesar cipher.

3. Differentiate ABS and DES.

4. What is meant by Known plaintext attack?

5. Find the value of $21^{24}$ mod 8 using square and multiply method.

6. What is short pad attack?

7. Why MDC has been used? Explain it.

8. List various characteristics of Secure Hash Algorithm.

9. What is WAP protocol stack?

10. List the advantages of VPN.

PART B — (5 × 16 = 80 marks)

11. (a) (i) Explain about various security mechanisms. (5)

(ii) With example, explain various types of transposition techniques and its vulnerability. (11)

Or

(b) (i) Consider "*CNS*" as Plain Text and "*PERFORMER*" as Key. Encipher and decipher using Hill cipher. (10)

(ii) Explain mono alphabetic cipher and poly alphabetic cipher with examples. (6)

12. (a) Explain DES and its weaknesses. (16)

Or

(b) Explain various modes of operation for block ciphers. Which is suitable for better communication? Justify your answer. (16)

13. (a) (i) Explain Rabin cryptosystem. (8)

(ii) Write RSA algorithm and Solve the following : p = 7; q = 13; e (select least possible prime no); M = 10; Perform encryption and decryption. (8)

Or

(b) (i) Write an algorithm in pseudocode for Chinese remainder theorem. Give an example. (8)

(ii) Discuss about Elgamal algorithm. (8)

14. (a) (i) Explain HMAC and CMAC. (10)

(ii) Why digital signature has been used? Explain some attacks on digital signature. (6)

Or

(b) (i) Explain S/MIME. (8)

(ii) Explain SSL. (8)

15. (a) (i) Explain how the security will be provided in GSM. (8)

(ii) Explain WAP and WTLS architecture. (8)

Or

(b) (i) Explain about VPN. (8)

(ii) Explain about Denial of Service. (8)

---