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

Question Paper Code : 41160

B.E./B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2013.

Seventh Semester

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. Distinguish between a substitution cipher and a transposition cipher.

2. List the attacks that threaten the integrity of information.

3. Distinguish between diffusion and confusion.

4. List the operation modes that can be speed up by parallel processing.

5. Mention the properties of trap door one-way function.

6. Illustrate chinese remainder theorem with an example.

7. What is arbitrated digital signature?

8. Why does PGP generate a signature before applying compression?

9. Mention the characteristics of firewall.

10. What is a VPN?

PART B — (5 × 16 = 80 marks)

11. (a) Why is confidentiality an important principle of security? How will you achieve the same? Discuss the reasons behind the significance of authentication. Find out simple mechanisms for authentication. What is access control? How is it different from availability?

Or

(b) (i) Encrypt the message "Roger arrived" using play fair cipher. Ignore the space between words. Use the matrix in figure 1. (8)

L	G	D	B	A
Q	M	H	E	C
U	R	N	I/J	F
X	V	S	O	K
Z	Y	W	T	P

Fig.1

(ii) Describe double columnar transposition cipher with an example. (8)

12. (a) Draw the general structure of Multiple DES and explain the encryption - decryption process.

Or

(b) Describe AES Cipher in detail.

13. (a) (i) What are the principal elements of a public key cryptosystem? (6)

(ii) In RSA, given the product of prime numbers N = 221 and the Encryption key E = 5, find the decryption key. (6)

(iii) Mention the applications of public key cryptosystems. (4)

Or

(b) In the Elliptic Curve E(1,2) over the GF(11) field.

(i) Find the equation of the curve. (4)

(ii) Find any 2 points (P, Q) on the curve. (4)

(iii) Find a 3rd point R = P + Q and show that it satisfies the Elliptic curve equation. (8)

14. (a) List the security services provided by a digital signature. Explain the signing and verification process of DSA.

Or

(b) Write any 2 key distribution facilities which can be adopted by a local area network vendor. Discuss about its pros and cons.

15. (a) Write a note on the following :-

(i) Security in Java. (8)

(ii) Security in Operating Systems. (8)

Or

(b) What are the approaches for achieving single sign on (SSO)? Explain in detail.