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

Question Paper Code : Q 2760

B.E./B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2009.

Seventh Semester

(Regulation 2004)

Computer Science and Engineering

IT 1352 — CRYPTOGRAPHY AND NETWORK SECURITY

(Common to B.E. (Part-Time) Sixth Semester Regulation 2005)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. What is cryptanalysis and cryptography?

2. Define threat and attack.

3. What is the role of session key in public key schemes?

4. What is a zero point of an elliptic curve?

5. What are the functions used to produce an authenticator?

6. List the properties a digital signature should possess?

7. Mention the scenario where kerberos scheme is preferred.

8. What are the technical deficiencies in the kerberos version 4 protocol?

9. List the classes of intruders.

10. Give the types of viruses.

PART B — (5 × 16 = 80 marks)

11. (a) Explain the OSI security architecture along with the services available. (16)

Or

(b) (i) Given 10 bit key $K = 1010000010$. Determine K_1, K_2 where

$P_{10} = 3\ 5\ 2\ 7\ 4\ 10\ 1\ 9\ 8\ 6$

$P_8 = 6\ 3\ 7\ 4\ 8\ 5\ 10\ 9$

by using SDES key generation method. (10)

(ii) Using the positional value of alphabets, represent them in 5 bit binary. Apply the transformation $C_i = K_i \oplus P_i$, $P_i = C_i \oplus K_i$ where P_i = "Scheme " K_i = "Cipher". Find the cipher text. (6)

12. (a) (i) Perform Encryption/Decryption using RSA algorithm for the following :

$p = 3$, $q = 11$, $e = 7$, $m = 5$. (12)

(ii) What attacks are possible on RSA algorithm? (4)

Or

(b) (i) Given the key 'MONARCHY' apply play fair to plain text "FACTIONALISM" to ensure confidentiality at the destination, decrypt the ciphertext and establish authenticity. (8)

(ii) Apply public key encryption to establish confidentiality in the message from A to B. you are given $m = 67$, $KU = \{7, 187\}$, $KR = \{23, 187\}$. (8)

13. (a) (i) Apply the MAC on the cryptographic checksum method to authenticate build confidentiality of the message where the authentication is tied to message.

$M = 8376$, $K_1 = 4892$, $K_2 = 53624071$. (10)

(ii) What are the properties a hash function must satisfy? (6)

Or

(b) Explain MD5 message digest algorithm, with it's logic and compression function. (16)

14. (a) Explain X.509 authentication service and it's certificates. (16)

Or

(b) (i) Explain the services of PGP. (12)

(ii) Write down the functions provided by S/MIME. (4)

15. (a) (i) List the approaches for the intrusion detection. (4)

(ii) Explain firewall design principles, characteristics, and types of firewalls. (12)

Or

(b) (i) Give the basic techniques which are in use for the password selection strategies. (8)

(ii) Write down the four generations of antivirus software. (8)