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

Question Paper Code : 91379

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

Seventh Semester

Electronics and Communication Engineering

EC 2035/EC 702/10144 ECE 23 — CRYPTOGRAPHY AND NETWORK SECURITY

(Regulation 2008/2010)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Differentiate between passive and active attacks.

2. What would be the transformation of a message "A successful team is a group of many hands but of one mind " using Rail Fence technique?

3. What is a trap-door one way function?

4. Using Fermat's theorem, find $5^{301} \bmod 11$.

5. Distinguish between entity authentication and message authentication.

6. Explain weak collision property of a hash function.

7. Why does an ESP include a padding field?

8. What is a worm? What is the difference between a worm and a virus?

9. What is a threat? How it differs from Vulnerability?

10. List the different security management practices.

PART B — (5 × 16 = 80 marks)

11. (a) (i) Explain the Cipher Feedback and Output Feedback Block cipher modes of operation. (8)

(ii) Encrypt a message "Behavior is a mirror in which everyone displays his own image" with the keyword "monarchy" using Playfair cipher technique. (8)

Or

(b) Explain in detail Encryption and Decryption process of DES Algorithm. (16)

12. (a) (i) Explain the different ways of key distribution in Asymmetric key cryptography. (8)

(ii) Perform encryption and decryption using the RSA algorithm for the following : (8)

(1) $p = 7; q = 13\ e = 79; M = 11$

(2) $p = 19; q = 23\ e = 3; M = 11$.

Or

(b) (i) How do Elliptic Curve take part in Encryption and Decryption process? (8)

(ii) Users A and B use the Diffie-Hellman key exchange technique, a common prime q = 71 and a primitive root $\alpha = 7$. If user A has a private key $X_A = 3$, what is A's public key Y_A? If user B has a private key $X_B = 10$, what is B's public key Y_B? What is the shared secret key? (3 + 3 + 2)

13. (a) (i) Explain the Digital Signature Standard. (8)

(ii) Describe the requirements of a Hash function. (8)

Or

(b) Briefly explain with diagram the SHA-512 Processing of a single 1024-Bit Block. (16)

14. (a) (i) What is Kerberos? Explain how it provides authenticated service. (12)

(ii) Describe the benefits of IPSec. (4)

Or

(b) (i) Discuss the services provided by SSL Record Protocol. (6)

(ii) Briefiy explain the functionality of S/MIME. (10)

15. (a) Discuss the different approaches to IDS. (16)

Or

(b) (i) Describe the different techniques used by firewalls to control access and enforce a security policy. (8)

(ii) Explain the characteristics of firewalls. (8)