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

Question Paper Code : 11158

B.E./B.Tech. DEGREE EXAMINATION, MAY/JUNE 2014.

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. Define confidentiality.

2. What you mean by passive attack?

3. Define Stream and Block cipher.

4. What are the disadvantages of double DES?

5. State Cryptography.

6. Define Elliptic Cryptosystem.

7. Write out – Hash Function.

8. Mention the services provided by the Pretty Good Privacy (PGP).

9. How is security handled in .NET?

10. Define – DoS.

PART B — (5 × 16 = 80 marks)

11. (a) Explain in detail about the Security services classifications and security mechanism.

Or

(b) Compare and contrast Symmetric crypto primitives and Asymmetric crypto primitives with suitable examples.

12. (a) Explain briefly – Substitution ciphers and Transposition ciphers.

Or

(b) Explain in detail about the DES Algorithm.

13. (a) Discuss in detail about the Rabin Cryptosystem.

Or

(b) State and explain RSA Cryptosystem.

14. (a) Write out –key management concept and Diffie-Hallman Key Exchange concept.

Or

(b) How is security provided at Transport Layer, Network Layer and in Application Layer? Discuss.

15. (a) Explain in detail about the WAP Security and GSM Security.

Or

(b) Write a detailed technical note Single Sign On (SSO).

———————