LIB
2.1.16FN

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

Question Paper Code : 21763

B.E./B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2015.

Seventh Semester

Computer Science and Engineering

IT 2352/IT 62/10144 IT 603/10144 CSE 46 — CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Sixth Semester – Information Teehnology)

(Regulations 2008/2010)

(Common to PTIT 2352 – Cryptography and Network Security for B.E. (Part-Time) Seventh Semester – Computer Science and Engineering – Regulations 2009)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Encrypt 'amma' using affine cipher with key (15, 20).

2. Find the value of 6^{10} mod 11.

3. Define short notes on triple DES.

4. What is the need of AES?

5. Write short notes on MD5.

6. If two points $p=(x1, y1)$ and $q-(x2, y2)$ where $x1!=x2$ and $y1!=y2$ find third point $r(x3, y3) = p+q$ on ECC.

7. Write short notes on SET.

8. What is X.509 certificate and its revocation?

9. List out the different security models.

10. What is the need for trusted OS?

PART B — (5 × 16 = 80 marks)

11. (a) (i) Find the solution to the following equations

$x \equiv 2 \mod 3$

$x \equiv 3 \mod 5$

$x \equiv 2 \mod 7$.

(ii) Explain the possible attacks and services present in cryptography.

Or

(b) Explain in detail different types of cipher techniques. (16)

12. (a) Explain DES structure including key generation phase. Also explain the modes of operation.

Or

(b) Explain – RSA crypto system with suitable example. Also explain the possible attacks on RSA.

13. (a) (i) Explain – Diffie Hellman key exchange procedure with suitable example.

(ii) Explain the need for message authentication code and the procedure involved in the generation and verification of MAC.

Or

(b) (i) Explain ElGamal digital signature procedure with suitable example.

(ii) Explain the need for DSA compared to ElGamal digital signature procedure. Explain the creation and verification procedures of signatures in DSA.

14. (a) (i) Explain – Kerberos authentication procedure.

(ii) Explain about electronic mail security.

Or

(b) (i) Explain in detail about web security.

(ii) Brief – SSL and TLS.

15. (a) Explain – System security, intruders and security standards.

Or

(b) (i) Brief about malicious software-viruses.

(ii) Explain in detail the different types of firewalls.