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

**Question Paper Code : 60763**

B.E./B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2016.

Sixth/Seventh Semester

Computer Science and Engineering

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

(Common to Information Technology)

(Regulations 2008/2010)

(Also common to PTIT 2352 – Cryptography and Network Security for BE (Part-Time) Sixth Semester — CSE — Regulations 2009)

Time : Three hours | Maximum : 100 marks

Answer ALL questions.

PART A — ($10 \times 2 = 20$ marks)

1. State Fermat's theorem and compute $2^{53} \pmod{11}$ using the same.

2. The ciphertext CRWWZ was encrypted by an affine cipher mod 26. The plaintext starts with 'ha'. Decrypt the message.

3. If a bit error occurs in plain text block $b_1$, how far does the error propagate in CBC mode of DES?

4. Define order of a group. Find the order of all elements in $G =< Z_{10}^*, * >$.

5. Write the three fold properties of cryptographic hash functions.

6. Compare and contrast the attacks on digital signatures with attacks on cryptosystems.

7. How can the signed data entity of S/MIME be prepared?

8. Mention the purposes of handshake SSL protocol.

9. Write short notes on the three types of intruders.

10. Mention any two security standards for wireless LAN.

PART B — (5 × 16 = 80 marks)

11. (a) (i) Explain the possible cryptanalytic attacks on any cryptosystem. (4)

(ii) Write the rules for decryption using playfair cipher and decrypt KNDMGO using the keyword GUIDANCE. Y and Z count as one letter. (6)

(iii) Discuss the significance of LFSR sequences in cryptography. (6)

Or

(b) (i) State and explain Chinese Remainder theorem. (6)

(ii) Using Chinese remainder theorem, find an integer that has a remainder of 3 when divided by 7 and 13 but is divisible by 12. (4)

(iii) Discuss the importance of Legendre and Jacobi symbols in cryptography. (6)

12. (a) (i) Illustrate single round details of DES and its sub keys generation with appropriate diagrams. (8)

(ii) Explain cipher block chaining and cipher feedback modes of operation with suitable diagrams. (8)

Or

(b) (i) Give the steps involved in encrypting the message block M = 7 using RSA with the parameters e = 23 and n = 233 × 241. Also show that the decryption yields the actual message. (8)

(ii) Discuss RC4 stream cipher in detail. (8)

13. (a) (i) Explain Man in the middle attack with respect to Diffie Hellman Key exchange. (6)

(ii) Explain ElGamal Crypto system with an example. (10)

Or

(b) Explain the following:

(i) Birthday attacks in hash. (4)

(ii) MD5 hash algorithm with all diagrams. (12)

14. (a) (i) Explain the architecture of Kerberos in brief. (8)

(ii) Discuss the different PGP messages and key rings in detail. (8)

Or

(b) (i) Explain the two protocols in IP security with their stack diagrams. (8)

(ii) Describe SSL architecture with a neat diagram. (8)

15. (a) Define virus. Discuss the negative impact caused by virus in a system? Describe the various methods to resolve it. (16)

Or

(b) Explain the types and configurations of firewalls. (16)

---