16/6/16 AN

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

Question Paper Code : 51763

B.E./B.Tech. DEGREE EXAMINATION, MAY/JUNE 2016

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 Technology)

(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. The cipher text CRWWZ was encrypted by an affine cipher mod 26. The plain text starts with 'ha'. Decrypt the message.

2 Define Euler's Φ function and find the values of (i) Φ (35) (ii) Φ (27).

3. What is meant by Avalanche effect in DBS ?

4. State the significance of blinding in RSA.

5 Define 'man in the middle attack'.

6. List the requirements of hash functions.

7. State the reasons to revoke a certificate before its expiry time.

8. How can the signed data entity of S/MIME be prepared ? Write the steps.

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

10. Does the firewall ensure 100% security to the system ? Comment.

PART – B (5 × 16 = 80 Marks)

11. (a) (i) State and explain Chinese Remainder theorem. Using the same, find an integer that has a remainder of 3 when divided by 7, 4 when divided by 13 but is divisible by 12. **(8)**

(ii) State the rules to perform encryption using playfair cipher and encrypt 'snowshooos' using the key 'monarchy'. I and J count as one letter and x is the filler letter. **(8)**

OR

(b) (i) Explain the different security mechanisms focused by OSI security architecture. **(8)**

(ii) State Euclidean algorithm and find the inverse of 550 mod 1759. **(8)**

12. (a) (i) Explain the different modes by which any block cipher can operate with suitable diagrams. **(8)**

(ii) Explain RC4 stream cipher algorithm in detail. **(8)**

OR

(b) (i) Let $f(x) = x^6 + x^4 + x^2 + x + 1$ and $g(x) = x^7 + x + 1$, with an irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$. Multiply $f(x)$ by $g(x)$ in $GF(2^8)$. **(3)**

(ii) Explain how encryption is done using advanced encryption stansard with necessary block diagrams. **(13)**

13. (a) (i) How MD5 method provide security to the system ? Explain with suitable diagram. **(8)**

(ii) What are digital signatures ? Explain DSA algorithm to generate the same. **(8)**

OR

(b) Explain the secure hash algorithm to generate message digest in detail. **(16)**

14. (a) Discuss elaborately how Kerberos provides the different authentication services with necessary diagrams. **(16)**

OR

(b) What is the importance of web security ? Explain how secure socket layer provides the reliable service. **(16)**

15. (a) (i) Explain the different password selection strategies in detail. **(12)**

(ii) Write short notes on Trojan horses. **(4)**

OR

(b) (i) Define virus. Explain the different types of viruses in detail. **(8)**

(ii) Explain the application level and circuit level gateway firewalls with suitable diagrams. **(8)**
