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

Question Paper Code : 40917

B.E./B.Tech. DEGREE EXAMINATION, APRIL/MAY 2018
Seventh/Eighth Semester
Computer Science and Engineering
CS6701 – CRYPTOGRAPHY AND NETWORK SECURITY
(Common to Electronics and Communication Engineering/Information Technology)
(Regulations 2013)

Time : Three Hours | Maximum : 100 Marks

Answer ALL questions

PART – A (10×2=20 Marks)

1. Why is asymmetric cryptography bad for huge data ? Specify the reason.
2. State Euler's theorem.
3. List the parameters (block size, key size, and no. of rounds) for the three AES versions.
4. Perform encryption and decryption using RSA Algorithm for the following. P = 7; q = 11; e = 17; M = 8.
5. What is a hash in cryptography ?
6. How digital signatures differs from authentication protocols ?
7. What is the main function of a firewall ?
8. What is a Threat ? List their types.
9. List out the services provided by PGP.
10. What is the difference between TLS and SSL security ?

PART – B (5×16=80 Marks)

11. a) Explain classical encryption techniques with symmetric cipher and Hill cipher model.

(OR)

b) State and prove the Chinese remainder theorem. What are the last two digits of 49^{19} ? $= ((49)^2)^9 \times 49$

$= (2402)^9 \times 49$

$= 81 \times 49 = 3969$ ∴ last two digit is 69

12. a) What do you mean by AES ? Diagrammatically illustrate the structure of AES and describe the steps in AES encryption process with example.

(OR)

b) With a neat sketch explain the Elliptic curve cryptography with an example.

13. a) How Hash function algorithm is designed ? Explain their features and properties.

(OR)

b) With a neat diagram, explain the MD5 processing of a single 512 bit block.

14. a) Explain briefly about the architecture and certification mechanisms in Kerberos and X.509.

(OR)

b) How does screened host architecture for firewalls differ from screened subnet firewall architecture ? Which offers more security for information assets on trusted network ? Explain with neat sketch.

15. a) Illustrate how PGP encryption is implemented through a suitable diagram.

(OR)

b) Write short notes on the following :

a) Public Key Infrastructure (8)

b) Secure Electronic Transaction (8)