14/05/19

Roll No. | | | | | | | | | | |

[F.T]

B.E / B.Tech/ B. Arch END SEMESTER EXAMINATIONS APR/MAY 2019

A

ELECTRONICS AND COMMUNICATION ENGINEERING

VII Semester

EC8071 Cryptography and Network Security

(Regulation 2012)

Time: 3 Hours | Answer ALL Questions | Max. Marks 100

PART-A (10 x 2 = 20 Marks)

1. The encryption key in a transposition cipher is (3,2,6,1,5,7,4). The cipher text " RONMIGN" Find the plain text.
2. Define repudiation attack.
3. Give the advantages of galois field arithmetic in security.
4. Differentiate block and stream cipher.
5. Explain Kerckhoff's principle
6. What are the three kinds of witnesses a claimant must show for identification .
7. What is the use of KDC?.
8. Write the essential properties of a cryptographic hash function.
9. Explain the two basic ways to create firewall rulesets.
10. Expand PGP . where it is used?.

Part – B (5 x 16 = 80 marks)
(Question No.11 is Compulsory)

11. Differentiate symmetric key crypto grapy with asymmetric key. Explain the steps involved in RSA algorithm. (16)

12. a) Explain the DES Algorithm and discuss about its attacks and disadvantages (16)

(OR)

b) What is digital signature? How it is different form HASH function?. (6)
ii)Explain the Diffie –Hellman Key Exchange mechanism. Also discuss about the Man-in the middle attack . (10)

13. a) Explain the operation of KERBEROS. (16)

(OR)

b) Explain the IPsec architecture. Also discuss the authentication header and ESP frame format. (16)

14. a) i)Explain the process of challenge –response scheme. Also explain how Dual authentication is achieved?. (16)

(OR)

b) What are firewalls?.Discuss on the design principles of Firewalls (16)

15. a) Explain security at transport layer . (16)

(OR)

b) Explain the NIST security model (16)