UB

16/11

Reg. No. : □□□□□□□□□□□□

Question Paper Code : 91409

B.E./B.Tech. DEGREE EXAMINATIONS, NOVEMBER/DECEMBER 2019
Seventh/Eighth Semester
Computer Science and Engineering
CS6701 – CRYPTOGRAPHY AND NETWORK SECURITY
(Common to Electronics and Communication Engineering/Information Technology)
(Regulations 2013)
(Also common to PTCS6701 – Cryptography and Network Security for B.E. Part-time – Sixth Semester – Computer Science and Engineering – Regulations 2014)

Time : Three Hours

Maximum : 100 Marks

Answer ALL questions

PART – A

(10×2=20 Marks)

1. Define Field and Ring in number theory.

2. Consider the RSA encryption method with p = 11 and q = 17 as the two primes. Find n and ϕ (n).

3. Does the set of residue classes (Mod3) form a group
   a) With respect to modular addition ?
   b) With respect to modular multiplication ?

4. List the entities that are to be kept secret in conventional encryption techniques.

5. State the requirements of a digital signature.

6. Compare direct and arbitrated digital signature.

7. What is realm in Kerberos ?

8. List the five principal services provided by PGP.

9. In SSL and TLS, why is there a separate change_cipher_spec protocol rather than including a change_cipher_spec message in the Handshake Protocol ?

10. What entities constitute a full service in Kerberos environment ?

PART – B (5×13=65 Marks)

11. a) i) Explain in detail about the entities in the symmetric cipher model with their requirements for secure usage of the model. (6)

ii) Demonstrate that the set of polynomials whose coefficients form a field is a ring. (7)

(OR)

b) Write a note on different types of security attacks and services in detail. (13)

12. a) Explain Diffie Hellman Key exchange algorithm in detail. (13)

(OR)

b) Explain the working of RSA and choose an application of your choice for RSA and show how encryption and decryption is carried out. (13)

13. a) i) Compare the uses of MAC and Hash function. Represent them using appropriate diagrams. (8)

ii) List down the advantages of MD5 and SHA algorithms. (5)

(OR)

b) List the design objectives of HMAC and explain the algorithm in detail. (13)

14. a) Discuss about the components involved in e-transactions using secure electronic transaction protocol. Specify how it ensures the security during transactions. (13)

(OR)

b) Explain in detail about the types of firewalls and mention the design criteria of a firewall to protect the host machines in an educational institution. (13)

15. a) Using the PGP cryptographic functions, explain the security features offered for e-mails in detail. (13)

(OR)

b) Discuss in detail about IP security architecture and the services offered by IPSec. (13)

PART – C (1×15=15 Marks)

16. a) Consider a banking application that is expected to provide cryptographic functionalities. Assume that this application is running on top of another application wherein the end customers can perform a single task of fund transfer. The application requires cryptographic requirements based on the amount of transfer.

Transfer amount	Cryptography functions required
1 – 2000	Message digest
2001 – 5000	Digital signature
5000 and above	Digital signature and encryption

Suggest the security scheme to be adopted in client and server side to accommodate the above requirements and justify your recommendations. (15)

(OR)

b) Suggest and explain about an authentication scheme for mutual authentication between the user and the server which relies on symmetric encryption. (15)