CRYPTOGRAPHY & NETWORK SECURITY

Unit - I

1. Write and discuss the relation between security mechanisms and attacks.
2. Draw the model for Network Security and show that there are four basic tasks in designing a particular security service.
3. Explain different types of security services.
4. List and explain security Mechanisms defined by X.800
5. Explain various active and passive attacks.

Unit - II

1. Explain simplified DES with example.
2. How is AES used for encryption/decryption? Discuss with example.
3. Justify that substitution and transposition techniques are two basic blocks for all encryption techniques with an example each.
4. Mention the strengths and weakness of DES Algorithm.
5. What are the different modes of operation in DES?

Unit – III

1. Explain principles of public key cryptosystems
2. Explain RSA algorithm with example.
3. Explain Diffie-Hellman Key agreement protocol for a symmetric key agreement.
4. Explain about Euclidean algorithm for Greatest Common Divisor
5. Illustrate El Gamal Encryption and Decryption Algorithms.
6. State and prove Chinese Remainder Theorem.

Unit – IV

1. Explain SHA – 512 algorithms with a neat sketch.
2. Explain symmetric key distribution using symmetric key encryption.
3. What are the environmental shortcomings of Kerbos4? How does Kerbos 5 address them?
4. What is the purpose of digital signature? Explain its properties and requirements.

5. Give the structure of CMAC. What is the difference between CMAC and HMAC?
6. Define hash? List the variants in SHA by explaining SHA-1 in detail.

Unit – V

1. Explain TLS Functions and alert codes of TLS.
2. Explain various PGP Cryptographic functions and services in detail.
3. With a sketch explain IPSec scenario and IPSec services.
4. List and explain the PGP services and explain how PGP message generation is done with a neat diagram.
5. Explain the protocols defined by SSL.
6. Explain in detail about Transport Layer Security
7. Explain IP security protocols in detail.
8. Write short notes on Signature based IDS.