**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 Computer Security Concepts.
4. Explain different types of security services.
5. List and explain security Mechanisms defined by X.800
6. Explain various active and passive attacks.
7. Explain the following mathematical terms and their role in Cryptography i) Prime numbers ii) The Modulus operator iii) The modular inverse.

**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. Explain in detail the key generation in AES algorithm and its expansion format.
5. Mention the strengths and weakness of DES Algorithm.
6. What are the different modes of operation in DES?
7. Write down the purpose of S-Boxes in DES.
8. Give the structure of AES. Explain how Encryption/Decryption is done in AES.

**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 elliptic curve cryptography.
5. Is RSA an asymmetric encryption algorithm? Explain with an example.
6. Explain elliptic curve cryptography.
7. Explain about Euclidean algorithm for Greatest Common Divisor
8. Describe about public and private keys in ECC System and explain about security of ECC.
9. Illustrate El Gamal Encryption and Decryption Algorithms.
10. State and prove Chinese Remainder Theorem.
11. State and prove Fermat’s Little theorem.

**Unit – IV**

1. Explain SHA – 512 algorithms with a neat sketch.
2. Explain symmetric key distribution using symmetric key encryption.
3. Describe the steps in finding the message digest using SHA-512 algorithm. What is the order of finding two messages having the same message digest.
4. What are the environmental shortcomings of Kerbos4? How does Kerbos 5 address them?
5. What are the requirements of Cryptographic hash functions.
6. Discuss about the objectives of HMAC and it security features.
7. What is the purpose of digital signature? Explain its properties and requirements.
8. Give the structure of CMAC. What is the difference between CMAC and HMAC?
9. 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. Explain IP Security Architecture and explain basic combinations of security associations.
5. List and explain the PGP services and explain how PGP message generation is done with a neat diagram.
6. Explain the protocols defined by SSL.
7. What are the services provided by IPSec? Where can be the IPSec located on a network.
8. Explain in detail about Transport Layer Security
9. Explain IP security protocols in detail.
10. Discuss the IEEE 802.11i Wireless LAN security.
11. Write short notes on Signature based IDS.