Important Topics- cryptography and Network Security

Unit-1:

1. Security Mechanisms, attacks.
2. Computer security concepts and challenges.
3. Difference between differential and linear cryptanalysis.
4. Types of Ciphers-Feistel, Stream, block
5. DES
6. Steganography

Unit-2:

1. Diffie- Hellman key exchange
2. Fermat’s and Euler’s theorems
3. Chinese remainder theorem
4. Euclidean algorithm, Elgamal cryptosystem
5. Pseudorandom number generation
6. RSA algorithm
7. Public Key cryptosystems

Unit-3:

1. Cryptography hash functions
2. Hash functions based on cipher block chaining
3. SHA algorithm
4. MAC, HMAC algorithm
5. Digital signature,Digital signature standards.
6. Elgamal,schnorr digital signature algorithm

Unit-4:

1. Symmetric key distribution using Asymmetric encryption
2. X.509 certificates
3. Kerberos
4. Public key infrastructure(PKI)
5. Remote user authentication
6. HTTP,HTTPS

Unit-5:

1. S/MIME
2. PGP
3. Intruders and intruders detection
4. SSL and transport security layer
5. IP security policy, Encapsulating security payload
6. Types of malicious softwares
7. Types of firewalls and configurations