CRYPTOGRAPHY AND NETWORK SECURTY

UNIT-1:-

1. Explain about security attacks.
2. Explain about cyber threats and their defences.
3. Explain about buffer overflow and format string vulnerabilities.
4. Describe symmetric cypher model
5. Explain about substitution techniques.

UNIT-2:-

1. Explain and draw the flowchart of DES.
2. Explain IDEA algorithm.
3. Describe modes of operations for block cipher.
4. Explain about BLOWFISH algorithm.

UNIT-3:-

1. Explain about Chinese remainder theorem.
2. What are the principles of public key cryptography?
3. Explain about discrete algorithms.
4. Explain about elgamal encryption and decryption.
5. Explain about elliptical curve cryptography.

UNIT-4:-

1. What are the applications of cryptographic hash functions?
2. Explain about secure hash algorithm.
3. Describe about HMAC & CMAC.
4. Explain about NIST digital signatures.
5. Describe about key management and distribution.

UNIT-5:-

1. Explain about PGP.
2. What are remote user authentications?
3. What is SSL/SSH/TLS.
4. Explain about S/MIME.

UNIT-6:-

1. Explain about intrusion detection techniques.
2. Explain about key management and authentication center.
3. Describe IP security overview.