**SWARNANDHRA COLLEGE OF ENGINEERING & TECHNOLOGY**

DEPARTMENT OF MASTER OF COMPUTR APPLICATIONS

**V SEMESTER**

SUBJECT: Cryptography and Network Security Subject Code: 16MC5T01

Regulation: R16

**UNIT-1**

1. (i) Discuss any four Substitution Technique and list their merits and demerits.

(ii) Explain in detail Transposition Technique?

2. Write short notes on

(i). Security attacks

(ii). Security services.

3. (i) Convert “MEET ME” using Hill cipher with the key matrix

Convert the cipher text back to plaintext

[](http://lh6.ggpht.com/-9xF6gxNAj2o/T3WuKxU1DDI/AAAAAAAACMc/lnpL999V-ds/s1600-h/clip_image001%255B6%255D.png)

(ii) Explain in detail the Legendre and Jacobi symbols.

4. (i) Briefly explain the design principles of block cipher.

(ii) Discuss in detail

block cipher modes of operation.

5. Write short notes on

(i)Fermat and Eluer’s theorem

(ii)Chinese Remainder theorem

**UNIT-2**

1. (i) Identify the possible threats for RSA algorithm and list their counter

measures.

(ii) Perform decryption and encryption using RSA algorithm with p=3, q=11, e=7 and N=5.

1. (i) Draw the general structure of DES and explain the encryption decryption process.

(ii) Mention the strengths and weakness of DES algorithm.

1. (i) Explain the generation sub key and S Box from the given 32-bit key by Blowfish.

(ii) In AES, hoe the encryption key is expanded to produce keys for the 10 rounds

1. (i) Describe about RC4 algorithm.

(ii) Explain the Miller-Rabin Algorithm .

**UNIT-3**

1. Briefly explain Deffie Hellman key exchange with an example.
2. Write and explain the digital signature algorithm.
3. Explain in detail Hash Functions.
4. Compare the Features of SHA-1 and MD5 algorithm.
5. Discuss about the objectives of HMAC and it security features.
6. Users A and B use the Diffie Hellman key exchange technique, a common prime q=11 and a primitive root alpha=7.
   1. If user A has private key XA=3.What is A’s public key YA?
   2. If user B has private key XB=6 What is B’s public key YB?
   3. What is the shared secret key? Also write the algorithm.
   4. How man in middle attack can be performed in Diffie Hellman algorithm.
7. Explain in detail EIGamal Public key cryptosystem.
8. Discuss clearly Secure Hash Algorithm(SHA)
9. Describe the MD5 message digest algorithm with necessary block diagrams.

**UNIT-4**

1. How does PGP provide confidentiality and authentication service for e-mail and file storage applications? Draw the block diagram and explain its components.
2. Write Short notes on S/MIME .
3. Explain the architecture of IP Security
4. Describe the SSL Specific protocol – Handshake action in detail.
5. Explain Secure Electronic transaction with neat diagram.
6. What is Kerberos? Explain how it provides authenticated service.
7. Explain the format of the X.509 certificate.

**UNIT-5**

1. Explain any two approaches for intrusion detection.
2. Identify a few malicious programs that need a host program for their existence.
3. Explain firewalls and how they prevent intrusions.
4. List and Brief, the different generation of antivirus software
5. Define intrusion detection and the different types of detection mechanisms, in detail.
6. Explain the types of Host based intrusion detection. List any two IDS software available.
7. What are the positive and negative effects of firewall?
8. Describe packet filtering router in detail.
9. Describe the familiar types of firewall configurations.