– ,

==========

Department of Computer Science and Engineering

Cryptography and Network Security

UNIT 1

1. Discuss various security attacks.

2. Explain about different types security services ?

3. Analyze symmetric ciper model ?

4. Explain about TCP and UDP session hijacking ?

5. Briefly define the monoalphabetic cipher. What is the difference between a Monoalphabetic cipher and a polyalphabetic cipher?

6. What is Buffer Overflow? What are the tasks in exploiting the overflowable Buffer?

UNIT 2

1.Discuss Traditinal Block Cipher Structure.

2. Explain about DES?

3. Explain about AES-Structure?

4. Discuss Key Expansion, Blowfish and IDEA.

5. Write about the CAST-128 key expansion, encryption and Decryption

6. Write about the following in AES cipher:
   Substitute Bytes Transformation
   Shift Rows Transformation
   Mix Columns Transformation
   Add Round Key Transformation

UNIT 3

1.Define Prime and Relative Prime Numbers,Modular Arithmetic.

2. Explain about Fermat's and Euler's Theorems?

3. Discuss about Chinese Remainder theorem, Discrete Algorithms.

4. Explain about Public Key Cryptography?

5. a) Explain about Euclidean algorithm for Greatest Common Divisor.
   b) Define elliptic curves and explain their application in cryptography

6. a) Use discrete logarithm properties to solve the following equation $x5 \equiv 11 \mod 17$. Using quadratic residues solve $x2 \equiv 5 \mod 11$.
b) Given p=19, q=23, and e=3 Use RSA algorithm to find n, $\phi(n)$ and d.

UNIT 4

1. Analyze applications of Cryptographic Hash Functions .

2. Discuss about secure hash algorithm and message authentication functions.

3. Explain about HMAC and CMAC?

4. Demonstrate Digital Signatures,NIST Digital Signature Algorithms.

5.Explain about Key Management and Distribution?

6. Give the structure of HMAC. Explain the applications of HMAC

7. Describe the attacks on digital signatures

UNIT 5

1.Explain about Kerberos?

2. Demonstrate Web Security Requirements.

3. Discuss Secure Socket Layer(SSL) , Transport Secure Layer(TSL) and Secure Shell(SSH).

4. Explain about S/MIME?

5a) In S/MIME, how does a receiver find out what cryptographic algorithms the sender has used when receives an S/MIME message.
b) Explain about the trust mechanism and certificates used by PGP and S/MIME.

UNIT-6

1.Explain aboutIP Security Overview and Architecture?

2. Discuss about Authentication Header and Encapsulating Security Payload.

3. Discuss about Combining Security Associations and Key Management.

4. Demonstrate Signature based IDS and Hot based IDS/IPS.

5.What are the basic approaches of building Security Associations