[Nov - 24]

GITAM (Deemed to be University)

GST/GSS/GSB/GSHSS Degree Examination

V Semester

CSEN2071 : CRYPTOGRAPHY AND NETWORK SECURITY

Time: 2 Hours **Max. Marks: 30**

Instruction: All parts of the unit must be answered in one place only.

Section - A

1. Answer all questions **(5x1=05)**

a. What is a monoalphabetic cipher?

b. Write down the formula for Triple DES Encryption and Decryption.

c. What is Euler's Totient Function $\phi(n)$?

d. What is the value of ipad and opad used in HMAC algorithm? Write it down in hexadecimal as well as binary.

e. List out the five header fields defined in MIME.

Section - B

Answer the following **(5x5=25)**

UNIT - I

2. Decrypt the plaintext “HDSIOEYQOCAA”, using Hill cipher for the given key: “ciphering”.

OR

3. What do you mean by security mechanism? Explain atleast 4 different types of security mechanisms.

UNIT - II

4. Outline the process of key schedule generation in the DES algorithm. How are round keys derived from the main key?

OR

5. Illustrate atleast 4 block cipher modes of operation with diagram.

UNIT - III

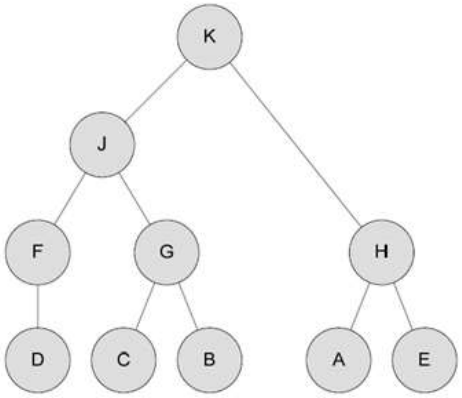
6. Demonstrate how the Euclidean Algorithm can be used to solve the equation 56x+98y=GCD(56,98) for integers x and y. Provide a complete solution showing all steps, and explain how the algorithm helps in finding such integer solutions.

OR

7. Assume Alice and Bob use Diffie-Hellman key exchange with a prime number p = 23 and base g = 5. Alice selects a private key a = 6 and Bob selects a private key b = 15. Compute the shared secret key that Alice and bob will use.

UNIT - IV

8. Draw format of certificate revocation list and Discuss how a certificate can be revoked from a CA. Also explain How a certification path will be established from A to B and B to A in the below diagram.



OR

9. Discuss the steps and equations used in SHA-512 with a block diagram.

UNIT - V

10. What is intrusion detection? Explain intrusion detection techniques in detail.

OR

11. What is a Firewall? Explain Different types.