DR. BABASAHEB AMBEDKAR TECHNOLOGICAL UNIVERSITY, LONERE

Question Bank

Cryptography and Network Security (BTETPE801E/BTETPE802E)

1) Discuss authentication , header and ESP in detail with their packet format
2) What is Cryptography? Explain types and features of Cryptography
3) Describe the SSL Architecture in detail
4) Explain SSL protocols
5) Explain about MD5 in detail
6) Write a detailed note on Digital signatures
7) What are the steps followed in creating digital signature
8) Explain Cryptanalytic attacks
9) Illustrate about the SHA algorithm and explain
10) Describe about Hash Function. How its algorithm is designed? Explain its features & properties
11) Explain RSA Approach, DSS Approach two approaches of Digital Signature
12) Explain the attacks related to Digital Signature
13) What is the difference between public key and private key cryptosystem
14) Explain in detail about elliptic curve cryptography
15) Explain the RSA algorithm and explain the RSA with p=7,q=11,e=17,M=8. Discuss its merit
16) Explain about AES in detail.
17) Explain in detail about DES and Triple DES
18) Explain the the following operations used in AES
    - Substitute bytes
    - Shift Rows
    - Mix Columns
    - Add Round Key

19) Perform encryption and decryption using RSA Alg. For the following. P=17; q=11; e=7; M=88

20) Explain are the following different modes of operation in DES
    - Electronic Code Book (ECB)
    - Cipher Block Chaining (CBC)
    - Cipher Feedback (CFB)
    - Output Feedback (OFB)
    - Counter Mode
21) Explain Classical cryptosystems and its types.
22) Define Euler's theorem and it's application also Find gcd (24140, 16762), gcd (1970, 1066) using Euclid's algorithm?
23) Specify and explain in details the four categories of security threads?
24) Explain following components of encryption algorithm.
    1. Plaintext
    2. Encryption algorithm
    3. Secret key
    4. Cipher text
    5.Decryption algorithm
25) Divide (HAPPY)26 by (SAD)26. Find quotient, Dividing (11001001) by (100111) find remainder and what is output In base 26 for multiplication of YES by NO
26) Let P, C, K denote plaintext space , Cipher text and Key space respectively. In shift cipher C=P=K=Z26 suppose the key for shift cipher Is K=6 and Cipher text is 1 then what is Plain text.

27) Suppose 25 is the plain text in caesar cipher cryptosystem then what is the ciphertext