Assignment

Course Code :CO 402U Cryptography and Network Security (Option I)

Academic Year : 2023-24

Date of Submission: 06/10/2023

QueNo

1 Explain about OSI Security architecture model with neat diagram

2 Enumerate the security mechanisms defined by X.800. Explain each.

3 Differentiate passive attack from active attack with example

4 What are the 3 aspects of security?

5 What is cryptanalysis and cryptography?

6 Distinguish between Substitution and Transposition techniques

7 What are Confusion and Diffusion properties of Modern Ciphers?

8 Using Play fair cipher Encrypt the following. Use X for Blank Spaces. Keyword: MONARCHY. Message: SWARAJ IS MY BIRTH RIGHT

9 Differentiate between a block cipher and a stream cipher with neat sketch diagram

10 Define Euler’s totient function or phi function and their applications

11 Define Fermat Theorem.Define Euler’s theorem and it’s application

12 Draw the general structure of DES and explain the encryption decryption process.

13 Mention the strengths and weakness of DES algorithm

14 Convert the Given Text “CRYPTOGRAPHY” into cipher text using Rail fence Technique.

15 What are the different modes of operation in DES?

16 Describe the working principle of DES with an example

17 Write down the purpose of S-Boxes in DES?

18 What is an avalanche effect?

19 State Chinese remainder theorem and find X for the given set of congruent equations using CRT.
$X=2\ (\text{mod } 3)$
$X=3(\text{mod } 5)$
$X=2\ (\text{mod } 7)$

20 What is stegnography? What are the drawbacks of steganography?

21 What are the critical aspects of Feistel Cipher design?

22 What are the properties a digital signature should have? What requirements should a digital signature scheme satisfy?

23 User A & B exchange the key using Diffie Hellman alg. Assume a=5 q=11 XA=2 XB=3. Find YA, YB, K.

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

25 What are the properties a digital signature should have? What requirements should a digital signature scheme satisfy?