Individual Assigment

QN1. Decrypt the cipher text to plain text with the key = 7 in A-Z (0-25) cipher text = YVTL PZ AOL NYLHALZA LTWPYL

QN2. Encrypt the plain text into cipher text by using substitution technique: plain text = I will be in town next week Note: Choose a key in A-Z (1-26) Space = 00, key = 3

QN3. Find out cipher text of below plain text using “PlayFair Cipher”.

Plaintext: TREE IS GREEN, Keyword: ENVIROMENT

Presentation

Group 1. a. Explain Data Encryption Standard (DES) Algorithm with example.

b. Strength & Weakness of DES, Avalanche effect.

Group 2. a. Explain Advanced Encryption Standard (AES) Algorithm with structure and example.

Group 3. a. RSA algorithm (Explain with example step by step)

Group 4. a. Diffie-Hellman Key Exchange algorithm (Explain with example)

Group 5. a. Introduction of Hash Function, Properties of Hash Function & Simple Hash Function

b. Applications of Hash Function

Group 6. a. Explain Secure Hash Algorithm (SHA-1)

b. Message Digest (MD - 5)

c. Difference between SHA 1 & MD 5

Group 7. a. Explain Message Authentication Code (MAC) and Applications

b. MAC based on Hash Functions

c. MAC based on Block Ciphers

d. Difference between hash function and MAC

Group 8. a. Explain the Digital Signature and its Properties, Requirements and Security

Group 9. a. Explain Key management and distribution

b. Explain Symmetric key distribution using symmetric Encryption

Group 10. a. Explain Symmetric key distribution using asymmetric Encryption

b. Discuss the Distribution of public keys

Group 11. a. Explain X.509 Certificate Format

b. Discuss how to Obtain & Revoke X.509 Certificate

Group 12. a. Explain Public key infrastructure

b. Discuss Remote user authentication with symmetric encryption