Assignment II

Cryptography and Network Security(CSE324)

1a. Differentiate between confusion and diffusion.

b. Draw a neat diagram and explain Feistel encryption and decryption. What are the 2 considerations in the design of Feistel cipher.

2a. Draw a neat diagram and explain DES sub key generation.

b. Explain the substitution operation during DES encryption and decryption.

3a. Along with neat diagrams differentiate between cipher feedback mode and output feedback mode.

b. Explain the construction of S-box and Inverse S-box in AES.

4a. Along with neat diagrams explain AES encryption and decryption.

b. What is double DES? How is it different from triple DES?

5a. How are the sub keys generated for AES encryption?

b. What is meet in the middle attack?

6a. What is electronic code book mode of operation? What is its drawback? How is it overcome? Explain.

b. Discuss the different types of attacks that can be applied on DES.