

Quiz 5

student name:

1: 20 what is secret-key Encryption, is it secure enough and why, or why not?

2: 25 what is mono and poly alphabetic substitute cipher? What is the famous example for poly? Why is it is hard to decode?

3: 25 what is DES? How does it work(briefly)? What is AES? Why is AES better?

4: 30 What are those Encryption modes discussed in the book and lectures? Brief explain the encryption method for each mode ECB, CBC, CFB and OFB and and if you change one bit in second block of encrypted file, when you decode it, how many and which blocks stay the same and how many and which blocks get corrupted.