1) Single round DES figure (ch3)
2) DES key exchange figure (ch3)
3) Multiplicative inverse using extended Euc. alg.
4) RSA p,q key pair generation and encryption/decryption technique (ch9)
5) Group, Ring , Field (ch4)
5-2) two binary numbers multiply them in GF(2^3) , m(x)= X^3 +X +1 (ch4)
6) mod(29), GF(2^6), GF(2^8), mod(16) which of them can be used to encode binary data,which can be used but will increase the number of bits, which can't be used and why?
6) Traffic Padding : def, why using it?
7) Arabic rotor machine 29 characters , 4 rotors... how many different substitutions?why?
8) if 6 rotors ,,how many diff. subs and why?