1-draw in detail , one round DES algo. (put on your sketch all necessary explanation to show how the operation is performed , its order and necessary explanation)

2-sketch the diagram showing key distribution scenario in DES encryption (single /symmetric key)
(put on your sketch all necessary explanation to show how the operation is performed , its order and necessary explanation)

3-In the RSA algo , used to encrypt a plan message M to a cipher text C .
1-write- the steps briefly – the key generating algo
2-explain the notation used in your algo and the condition that each should satisfy to guarantee that the two keys generated 're useful to perform the necessary functions of secrecy and authentication
The algo uses usually the variable (p q n …….etc)

3.b compute the public and private key if you select p=11 and l=17 show all the steps

4- sketch the block diagram for public key cryptosystem which will perform source A send a message to destination B , only B can decrypt the message and B can also prove A is the sending entity of that message (put on your sketch all necessary explanation to show how the operation is performed , its order and necessary explanation)

5-a- briefly describes triple DES with 2 keys (use only the space below ) you can sketch it .
b-why double DES with 2 keys is not assumed to secure , explain in detail

6- a) briefly define a group / ring / field ?
6- b) use extended Euclidean algo to find the multiplicative inverse (if exists) of 826 mod 2789 show steps in detail .

7- a) for each of the mode ECB , CBC and CTR
Identify which decrypted plaintext blocks px will be corrupted if cipher text C3 is corrupted . explain each case to show how you arrived the answer .

7- b) for each of the mode ECB and CTR assuming that cipher text contains N blocks and that there was a one bit in error in the source

version of p3 , identify how many cipher text blocks this error is propagated (explain each case to show how you arrived to your answer)