Divyanshu Shrivastava

187909 - MCA 5th Sem

Network Security Assignment

Q. Design principles of block cipher, substitution and permutation operation necessity in adapting confusion and diffusion.

Ans In block cipher plain text should not bring one bit change in the cipher text, it should bring more bit change in the cipher text (diffusion), while in the case of block cipher must ensure that one bit change in key stream should bring more bit changes in the ciphertext (confusion). This confusion and difusion is achieved by repeated substitution and permutation.

This is sometimes also reffered as SP-Network. If a person changes one bit of plaintext, then it is fed into a S-box, whose output will change at several bits, then all these changes are distributed by the

P-box among several S-boxes hence the outputs of these S-boxes are again changed at several bits and so on by the end of all the rounds the ciphertext get changed completly and on output what we will get is our desired ciphertext.