Assignment -2
Cryptography and Network Security (MC 407)
Department of Applied Mathematics **August 2021**
Delhi Technological University

---

1. Given a Feistel cipher to encrypt a block of "n" bits, prove that number of different reversible mappings for the ideal block cipher is $2^n!$.

2. Discuss the principles of block cipher design.

3. Consider a block encryption algorithm that encrypts blocks of length *'n'*, and let $N = 2^n$. Assume we have *"t"* plaintext–ciphertext pairs P_i, $C_i = E(K, P_i)$, where we assume that the key *K* selects one of the *N!* possible mappings. Imagine that we wish to find *K* by exhaustive search. We could generate key K' and test whether $C_i = E(K', P_i)$ for $1 \leq i \leq t$. If K' encrypts each P_i to its proper C_i, then we have evidence that $K = K'$. However, it may be the case that the mappings $E(K, \bullet) = E(K', \bullet)$ exactly agree on the *"t"* plaintext–cipher text pairs P_i, C_i, and agree on no other pairs. What is the probability that $E(K, \bullet)$ and $E(K', \bullet)$ are in fact distinct mappings?

4. Differentiate between:
   a. Fiestal Cipher and Non-Fiestal Cipher
   b. Confusion and Diffusion

5. Explain the avalanche effect in DES.

6. Let X' be the bitwise complement of X. Prove that if the complement of the plaintext block is taken and the complement of an encryption key is taken, then the result of DES encryption with these values is the complement of the original ciphertext, i.e.,
   If $Y = E(K, X)$, then $Y' = E(K', X')$.

7. Show that in DES the first 24 bits of each subkey come from the same subset of 28 bits of the initial key and that the second 24 bits of each subkey come from a disjoint subset of 28 bits of the initial key.

8. Discuss the following with respect to the International Data Encryption Algorithm (IDEA):

   a. Steps involved in one round of IDEA
   b. Output Transformation
   c. Strength of IDEA