# REPORT

# ASSIGNMENT-3

Assignment: Symmetric Key Encryption and Digital signatures.

In this assignment I choose to use block ciphers as efficient encryption functions and implemented Data Encryption Standard (DES) which is most used method in 90's.

These block ciphers operate on digital data (bits) so we first have to hash the message and have to convert it into bits representation and then encrypt it. Modern cryptosystems have to covert this binary string to another binary string. In block ciphers, the plain binary text is processed in blocks (groups) of bits at a time, i.e. a block of plaintext bits is selected, a series of operations is performed on this block to generate a block of ciphertext bits. The number of bits in a block is fixed.

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST). The DES satisfies both the desired properties of block cipher. These two properties make cipher very strong. Firstly, A small change in plaintext results in the very great change in the ciphertext. And also A small change in plaintext results in the very great change in the ciphertext.

## Vulnerability of the system:

the DES is vulnerable to brute force attack. Brute Force is the most simple and practical way to break a cipher. It consists in trying every key combination possible until right one is found. Having the right key you can break the cipher and read what was ciphered. The number of

possibilities is determined by the key size in bits, since DES only has a 64 bit key, the number of combinations is rather small and a personal computer can break it in few days.

## Hash Function:

The function implemented in this assignment is inspired from MD5 and modified to generate a 32 byte hash. The non-linear operation is fixed and not chosen arbitrarily. It is Vulnerable to collision same as MD5.