

**Assignment Answer**

**CSE432, Computer Security**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name: | Adham Nour | ID: | 1600226 |  |

Assignment No: ( 2 )

Date: 2 / 2 /2021

To Encrypt your message using Data Encryption Standard All you need to do is to include the header “DES.h” in your main function and then instantiate a DES object which provide two functions , the first one is the encryption function and the second one is the decryption function.

The Encryption Function is implemented as following:

* Getting the key from keyGeneration class
* Binarize the plaintext (turning it into binary)
* Pad that binarized plain text if its length is not devisable by 64
* Dividing the binarized plaintext into blocks each block is 64bit block and encrypting these blocks
* Then returning the result after Hexadecimalizing it (turning it into hexadecimal)

The Decryption function is similar to the Encryption function except that we reverse the key we got from the keyGeneration

As it is clear, The DES implemented in the code has a lot of optimization potentials that include the following:

* Converting all binary string to vector<bool> that optimize the memory usage, as instead of one byte per bit, it would be one bit per bit
* Using deferent type of parallelization that include employing SIMD instruction such as AVX and distributing that load on many core using OpenMP(For CPU), OpenCL (For GPU) and OpenMPI(to distribute over multiple systems) for large amount of data to be encrypted/decrypted