DES & AES

ANMOL YADAV 140010018
PUNEET MAHAJAN 140010013
SARTHAK MITTAL 14D170018
AKHILESH VYAS 14D110013

PROBLEM STATEMENT

- *To make cipher encrypter and decrypter.*
- *In module one of the project we will be using DES(data encryption standard) algorithm.*
- *In module two of the project we will be using AES (advanced encryption standard) algorithm.*
- *Also to make user friendly interface .*

DES ALGORITHM

- The input of 64 bit is taken with a 56 bit key.
- From this 56 bit key we have to make 16 48 bit keys.
- Now we divide the input into 2 halfs of 32 bit each named left and right.
- This is followed by 16 rounds in which the input is modified i.e the right part of the next input is the left part of the previous input and the right part is first expanded into 48 bit keys which is Xored with the corresponding keys. This is then converted back to 32 bit using s-box. This is xored with the left part and stored in the right part.
- This is then repeated 10 times.
- The result is than mapped to the ascii between 32 and 96.

AES ALGORITHM

- The input and keys are of 128 bit each.
- The input and the keys are converted into hexadecimal and stored in the 4 by 4 matrix.
- The key is expanded into 10 keys by using row const matrix and Xoring it in a particular fashion.
- Then the main rounds are then going under the following for encryption:-

1) Shift rows 2) Sub bytes 3) Mix columns 4) Add round keys

For Decryption:- 1) Inverse Shift rows 2) Inverse bytes 3) Add round keys 4) Inverse Mix Col

(The keys are in the reverse order)

```
        unsigned int colcur[4];
        unsigned int coltemp[4];

        for(int y=0;y<4;y++)
        {
            co
            co
        }

        unsigned in
        for(int p=
        colcur[3]=

        for(int y=
        {
            int

            int
            co
        }



        for(int y=

        for(int y=

        for(int i=
        {
            for
            {
                }
            }
        keytemp->ne
        keytemp=key
    }
}


void AesClass::reverse_keys()
{
    key_node* keytemp;
    keytemp = keyhead;

    int vec1[4][4];
    int vec2[4][4];
```

MainWindow

Data Encryption Standard & Advance Encryption Standard

INPUT

He

AES

OUTPUT

Encrypt

Decrypt

KEY

CHALLENGS FACED

- ***Understanding the algorithm was very difficult as we started with it, and it was new to us.***
- ***The Expandable Ascii were not printed on the terminal and this could not be used.***

- ***The extensive use of linked list and pointers made it difficult to manage and debug.***
- ***The mix columns part of AES was rather tedious and confusing as it was some complex matrix multiplication.***

FUTURE WORK

- *As it was used for security purposes(keeping data secret,etc), future applications just include making the algorithm more difficult to crack, currently both AES and DES are cracked.*
- *The user can input multiple keys making the code more strong . We can have multiple encryptions.*

- *Like double DES, triple DES*
- *We thought of a code that will permute the data in random number of times the value of which will be stored in the encrypted code(From both AES and DES) , and same number of times of permutation will be read and used to decrypt.*
- *We can do the step by step encryption (AES followed by DES,etc).*