CS203

PROJECT PROPOSALS

::By Arshdeep Singh (2020CSB1074) and Ankit Sharma (2020CSB1072).

1. Encryption-Decryption Using Matrix Multiplication

Objective:

To make an Encrypter and decrypter, using the concept of Matrix Multiplication.

RTL or Software implementation:

Code in C/C++ and Verilog for encryption-decryption.

Displaying the result:

> Idea is to implement a 14 segment LED display to represent characters of the decrypted string. This would be implemented totally in Verilog.

Functionality:

Encryption-decryption

The program will take a string as input, convert it into a 2 x (n/2) matrix. (append a space character at the end if n is odd). The user will select a key matrix (a m x 2 matrix that is like a password). The program will then multiply those 2 matrices and output an encrypted matrix.

Now to decrypt the matrix, you will need to input the key matrix and encrypted matrix, our program will find the inverse of it and multiply it with encrypted matrix to get a matrix, which will be then converted into a string.

The string will be converted into an array of numbers, for example:

string= “CS203”

Ascii codes = 67 83 50 48 51

Since converted codes are odd in number, we will append an empty character code 32(ASCII for space).

M=Obtained Matrix= $\begin{pmatrix} 67 & 83 & 50 \\ 48 & 51 & 32 \end{pmatrix}$

K=We will choose a key matrix (like a password): $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$

K*M= E(Encrypted matrix) = $\begin{pmatrix} 163 & 185 & 114 \\ 393 & 453 & 278 \end{pmatrix}$

For decrypting, we would use inv(K)*E = M ----**converted to string**---> “CS203”.