CSS CUSTOM ALGORITHM

Shubham Mankar, 7948
TE Computer

Using Diffie Hellman or similar algorithm the sender and the receiver decide upon a large number K to use as the base key.

Divide the message into blocks of 10 characters, further divide the block into sub-parts of 2 characters.

here, the key K must have 6 digits or more. This initial key is called the BASE KEY. From this base key, we consider the 5 MSBs. Thus you get K' which is a 5-digit number.

if A

K' has distinct digits

PROCEED FURTHER

K' doesn't have distinct digits

DO THE FOLLOWING:

1. Subtract 1 from K'
2. Square K' and the 5 MSBs of the square becomes the new K'.
3. Go to A

Now that K' has distinct digits, consider the following matrix:

$$\begin{array}{c|ccccc} & 2 & 3 & 4 & 5 & 8 \\ \hline 2 & A & B & C & D & E \\ 3 & F & G & H & I & K \\ 4 & L & M & N & O & P \\ 5 & Q & R & S & T & U \\ 8 & V & W & X & Y & Z \end{array}$$

Sample K'

= 4 8 3 2 5

↓

2 3 4 5 8

- now, arrange the K' digits in ascending order and align them with the above matrix as shown
- using K', rearrange the matrix

step 1

rearrange columns

$$\begin{array}{c|ccccc} & 4 & 8 & 3 & 2 & 5 \\ \hline 2 & C & E & B & A & D \\ 3 & H & K & G & F & I \\ 4 & N & P & M & L & O \\ 5 & S & U & R & Q & T \\ 8 & X & Z & W & V & Y \end{array}$$

step 2

rearrange rows

$$\begin{array}{c|ccccc} & 4 & 8 & 3 & 2 & 5 \\ \hline 4 & N & P & M & L & O \\ 8 & X & Z & W & V & Y \\ 3 & H & K & G & F & I \\ 2 & C & E & B & A & D \\ 5 & S & U & R & Q & T \end{array}$$

This is the final matrix for Block 1.

Using the Playfair cipher rules, the characters in the sub-blocks within the block will be encrypted.

After this encryption, we generate a new K'. Let us call it K''.

$K'' \Rightarrow$ select 5 MSB of $(K')^2$

after this proceed to the next block and go back to A

For the above example,

$$K'' = A\ (48325)^2$$

$$K'' = 29741$$

Thus a new matrix will be generated for each block at both sides. This matrix will be used for encryption and decryption.