Encryption and Decryption

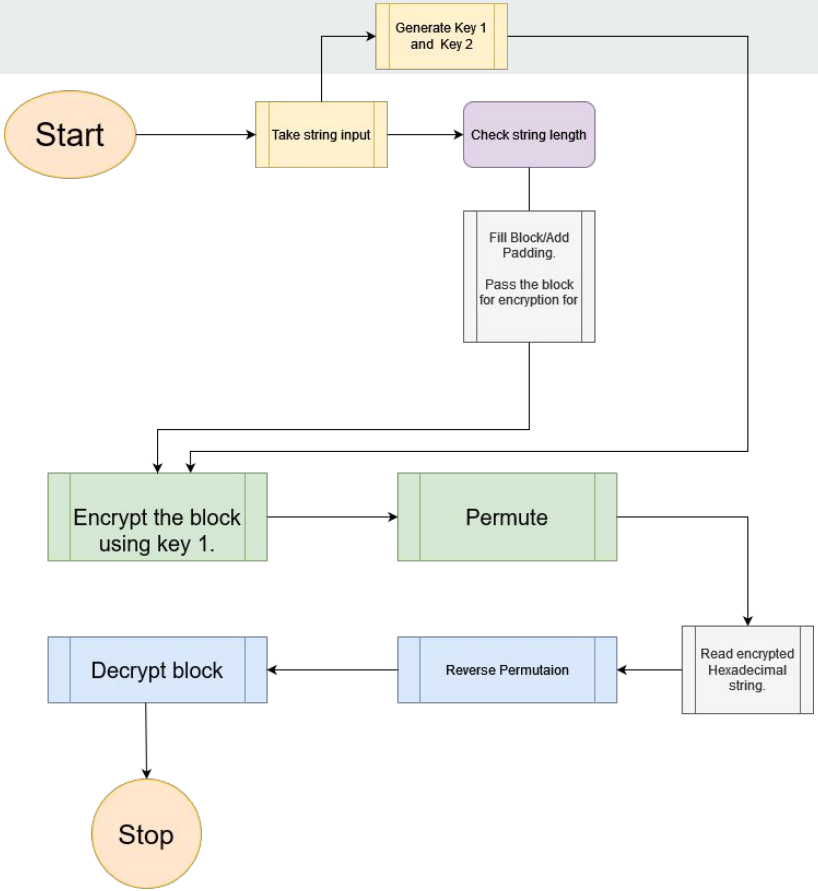
A method.

Overview

Encryption is a process which encompasses almost every facet of our lives be it transactions communication , data storage etc.

Providing security for such use cases is very important and many algorithms have been developed by professionals to address this.

The motive was to come up with a method which may potentially improve security or at the very least further discourse.



Data Flow Diagram

Algorithm Working:

Overview: We are taking a string input, processing it and encrypting it and storing values in Hexadecimal form.

Working:

Read the string.

(Generate a 512 bit Key1 and generate Key2 from a Set of 64 vector pairs)

Encrypt the string in block sizes of 64 bytes using Key1 and Key2.

Step 1:

Read the input string into the 8x8 matrix.

E	n	c	r	y	p	t	i
o	n	\0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Example:
String input = "Encryption";
//Let 0 be any random ASCII value

Step 2 : XOR using Key1

Q	r	:	L	u	m	c	s
-	-	?	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Step 3: Shuffle the matrix using Key2

0	Q	0	0	0	0	0	:
0	0	0	0	0	c	0	0
0	0	-	0	0	0	0	0
0	0	0	r	s	0	0	0
L	0	0	0	0	0	0	0
0	0	0	0	0	u	0	0
-	0	0	0	0	0	0	0
0	0	0	m	0	0	?	0

Proposed benefit:

The XOR operation on the matrix using Key1 provides a total combinations of **2^{512}** combinations.

The complete random shuffling of an 8x8 matrix gives us **1.268869321 E+89** possibilities.

Proposal:

Applying complete random shuffling on a matrix of substantial size after encryption can increase the total combinations.In this case by 1.268869321 E+89 times resulting in a total

2^{512} x 1.268869321 E+89 combinations.

Reordering of encrypted values makes pattern analysis difficult because no meaningful reorderings can be made unlike shuffling plain text , Therefore making deciphering the encrypted text more difficult.

Further Shuffling permutations can be increased by increasing block size.

For example a block of 12x12 dimension will have 144! Permutations i.e. **5.550293832 E+249 permutations.**