INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

USING 8'COMPLEMENT AND LINEAR FEEDBACK SHIFT REGISTERS TO ENCRYPT PLAIN TEXT

ANWAR ABDUL AZIZZ NAJI

AL SALAM UNIVERSITY COLLEGE, E-Mail: haideryanwar@yahoo.com

Abstract: - Over the past decade, there has been a rapid increase in communication and transmission of digital data by governments, industry and other organizations in the private sector. This amount of data we need to store them often because they contain a very large value and / or sensitive.
The research aims to convert data form to something unreadable by converting the plain text to 8'complemnt binary, gray code, XOR with a key generated by LFSR. The result will be modified to get the cipher text which is difficult to be analyzed.

Keywords: 8'complement, gray code, LFSR.

Introduction

Cryptography is the science of using mathematics to encrypt and decrypt data. It enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. In conventional cryptography, also called *secret-key* or *symmetric-key* encryption, one key is used both for encryption and decryption.[5] If the key is TRULY random and as large as the original text and has never been used then the cipher text will be impossible to decrypt without knowing the key.[1]

8's complement

Binary has only 1's-complement and 2's-complement; base-10 has only 9's-complement and 10's-complement. "53's-complement" only makes sense if you are working in base-53 or base-54 (the two cases have different meanings and will give different answers). As far as I'm aware, complements are only used in computing, so the only ones that are really important in the real-world are the two complements used in binary (and occasionally the decimal-complements.

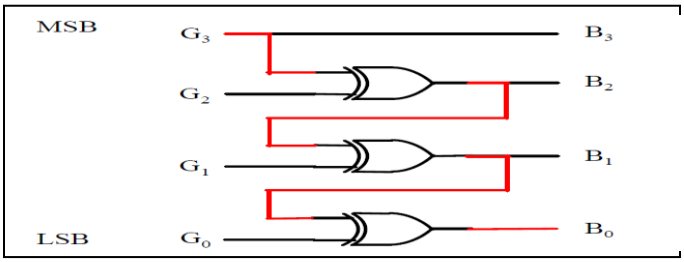
The 8'complement is a proposed new technique (base-10) with 3-bit result numbers, since all numbers are less than 8

Gray code

In digital system combination of two state called codes are used to represent numbers, symbols ,alphabetical ,character , and other types of information .the two state numbers system is called binary and its two digits are "0" and "1".

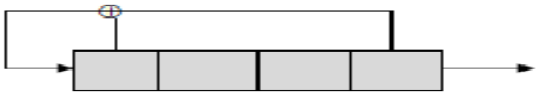
There are many specialized code used in digital system such as binary ,BCD ,Gray ,ASCII ,ect .the binary is commonly used in digital system ,to convert binary to gray is done with simple exclusive-OR .[2]

B3=G3
B2=B3 xor G2
B1=B2 xor G1
B0=B1 xor G0
TAP SEQUENCES



An LFSR is one of a class of devices known as state machines. The contents of the register, the bits tapped for the feedback function, and the output of the feedback function together describe the state of the LFSR. With each shift, the LFSR moves to a new state. For any given state, there can be only one succeeding state. The reverse is also true: any given state can have only one preceding state. For the rest of this discussion, only the contents of the register will be used to describe the state of the LFSR.[3] Suppose:

$f(x) = x^4 + x^3 + 1$ Tap x_4 with x_1



	X4	X3	X2	X1	F(x)
1	0	0	1	1	1
2	1	0	0	1	1
3	0	1	0	0	0
4	0	0	1	0	0
5	0	0	0	1	1
6	1	0	0	0	0
7	1	1	0	0	0
8	1	1	1	0	0
9	1	1	1	1	1
10	0	1	1	1	1
11	1	0	1	1	1
12	0	1	0	1	1
13	1	0	1	0	0
14	1	1	0	1	1
15	0	1	1	0	0
16	0	0	1	1	1

Table 1: Generate Key Using LFSR

Char :	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Weight:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Weights of characters

E1ncryption algorithm

1- Read plain text
2- Convert each character to its weight (one or two digits)
3- For each digit apply the following:
   1- Find 8' complement and convert to binary
   2- Convert each binary to gray code
   3- Generate a key using LFSR
   4- XOR the key with the gray code
   5- Change the LSB (zero to one and one to zero)
   6- Add new bit to the left, If the weight is one digit number then put zero in that bit otherwise put one
   7- The result is the cipher text

Decryption algorithm

1- Read cipher text ,divide to 5-bit parts
2- If the MSB is zero then the five bits represent one digit number otherwise it's a two digit number.
3- Change the LSB (zero to one and one to zero)
4- Generate a key then XOR with the number
5- Convert each part from gray code to binary
6- Apply 8'complment
7- Convert to character
8- The result is the plain text

The Implementation

If the plain text = "ANWER", then the encryption algorithm is as follows:

Char	Weight	8'complement	Binary	Gray code	key	XOR	LSB	CHNGE	Send
A	1	8-1=7	00111	00100	00011	00111	00110	00110	00110
N	1	8-1=7	00111	00100	01001	01101	01100	11100	11100
	4	8-4=4	00100	00110	00100	00010	00011	10011	10011
W	2	8-2=6	00110	00101	00010	00111	00110	10110	10110
	3	8-3=5	00101	00111	00001	00110	00111	10111	10111
E	5	8-5=3	00011	00010	01000	01010	01011	01011	01011
R	1	8-1=7	00111	00100	01100	01000	01001	11001	11001
	8	8-8=0	00000	00000	01110	01110	01111	11111	11111

Cipher text = 0011011100100111011010111010111100111111

To decrypt the cipher text:

cipher	Change MSB=0	Change LSB	key	XOR	binary	DEC	8'Comp	Number	CHAR
00110	00110	00111	00011	00100	00111	7	8-7=1	1	A
11100	01100	01101	01001	00100	00111	7	8-7=1	1	N
10011	00011	00010	00100	00110	00100	4	8-4=4	4	
10110	00110	00111	00010	00101	00110	6	8-6=2	2	W
10111	00111	00110	00001	00111	00101	5	8-5=3	3	
01011	01011	01010	01000	00010	00011	3	8-3=5	5	E
11001	01001	01000	01100	00100	00111	7	8-7=1	1	R
11111	01111	01110	01110	00000	00000	0	8-0=8	8	

Conclusion

Encryption algorithm used in this research depends on many steps each adds more complexity to the encryption process in such way that even if the cipher text is known there is no way to find the plane text without knowing the seed of the key and the tap function with the whole algorithm.

Using the 8's complement and gray code gave more complexity and secrecy to the algorithm.

REFERENCES

[1] http://www.springer.com/978-3-642-04100-6
[2] Delhi , Khanna , "Digital Electronics Principles and Applications" , Maini ,A.K(2002)
[3] Cryptography and network security, Behrouz A.Forouzan, McGraw-Hill Publishing Company, 2007.
[4] Modern Cryptography: Theory and Practice By Wenbo Mao Hewlett-Packard Company,2003
[5] http://support.gpgtools.org/kb/how-to/introduction-to-cryptography