# Linear Congruential Generators &

# Linear Feedback Shift Registers

### Title:

Implementation of linear congruential generators and linear feedback shift registers with user interface.

## Description:

What are linear congruential generators (LCG) and linear feedback shift registers (LFSR)?

Both LCG and LFSR are methods used to produce pseudo-randomized numbers using a linear recurrence.

Linear Congruential Generators (LCG): LCG is an algorithm which uses piecewise linear equation to get a sequence of pseudo-randomized numbers

Recurrence Relation:

#### $Xn+1 = (aXn + c) \mod m$

Were,

X, is the sequence of pseudo-random numbers

m, (> 0) the modulus

a, (0, m) the multiplier

c, (0, m) the increment

X0, [0, m) – Initial value of sequence known as 'seed'

For a = 1, it will be the additive congruence method.

For c = 0, it will be the multiplicative congruence method.

LCG is most common and oldest algorithm to generate pseudo randomize numbers.

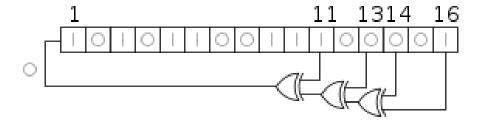
Linear Feedback Shift Registers (LFSR): is a shift register whose input bit is a linear function of its previous state.

The most commonly used linear function of single bits is exclusive-or (XOR). Thus, an LFSR is most often a shift register whose input bit is driven by the XOR of some bits of the overall shift register value.

Applications of LFSRs include generating pseudo-random numbers, pseudo-noise sequence, fast digital counters.

LFSRs have long been used as pseudo-random number generator for use in stream ciphers.

Fibonacci LFSRs: The bit positions that affect the next state are called the taps. In the diagram the taps are [16,14,13,11]. The rightmost bit of the LFSR is called the output bit. The taps are XOR'd sequentially with the output bit and then fed back into the leftmost bit. The sequence of bits in the rightmost position is called the output stream.



**Codes:** All the codes have been uploaded in GitHub Repository and can be accessed with the following link.

GitHub - skykiran/Crypto

# Screen Shots:

UUU	$11^{1000} \cdot 0^{1000} \cdot 1^{101} \cdot 01^{1000} \cdot 1^{101000010000010} \cdot 01101010110 \cdot 01101000110000011000011010 \cdot 0110001101000110100011010001101000110100011010$	M10000100 00 110
110	1000010000100 0001100001 11000 101 Pseudo-Random Number Generator 000 10110 011010000 1	010 100 0100 0
100	00110 100 0000 00 01011000 101000 1 10000 1 10000 1 1000 1	101100001 000001
001	101010110 001 000 01100001 10000 1 10101100001 0000 110 00 0	10000100 0001100
101	00.110.001001.001100.010.00011010.01100.0100.00011.0001.100.011010.0.0001011.001.0000.0110.0010001.0	001011000 10000
n n		01100001 000 1
0 U	00.011000010.0000110000110100001100.10.1	0000101000011000
010		010 100 110000
001	Linear Congruential Generator(LCR):	1 00011010000110
OOT	Xo: 57	1 00011010000110
IUU	diff and of	00101000 1 010
w	m ! 123	010/00110100 01
011	10001 0 0 111011100010 00 00101011 00010 110 110 000010 0010 1100110000101100 1101010 10000 0010 11 00010	. 1000110100001000
000	10 a:7	01101 0001100010
010	1 00 010 0010 0010 0010 0000 000 000 00	.010000110101010110
110	0010 01 1 00010 01 00 01 0000 0100 0110 0001 0000 100 110000101 00011 1000110000 00100011 00101	0 0110 0001 10000
000	No.of Random Numbers : 25	1101000010000101
001	to be Generated	00001 001 1100
100	1001000011010110100010 00001 0000010000 00111111	0 11 1 101100001
0 0	10 Submit 20011000010 1 01100 0001000011010001 (0 1011 01 000 001000 ( 010 010	0010 0110000101
011	00.20100.000.00	00.01000010110.0
00	Generated Numbers: 57 31 95 51 112 47 84 97 65 87 118 89 9 64 80 69 115 68 108 19 11 78 55 17 120	010000001 0 010
n	0000 001000 0000	010000001
00		0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
001		10000 011000101
OU.	The state of the s	100-0 0110000101
ULL	0 01 0 000100 0001000 10 01010 001100 001 00 10 1	.100.1100.00010 0
UU	0101 000110 000010000110 011000010110 011 0000110 00110 00011000101 0001100 00010001101 00110000 0110	11000000100010

0110100001100010 10000100 0	1.110.0 1010 0110 010010 0.10000101100011 100001 0.010 100	0.11000101100
Linear Feedback Shift Register(LF	SR):	
Seed: 10101		
mir for a grotom of or		
Taps : 2 4 5		
Submit		
0000 00 01011000 101		
Generated Bits: 1 11010	0101100000 00000 110 00 0 000011 1000 100 01 01	
0 01101	100 0100 00011 0001 100 0 1010 0 00001011 001 0000 0	
0 00110	00101100011 00000110001101 001 00010110000 00000110	
1 10011 0 01001	00.0010.011 000001100.101 001 0001110000 00000010	
0 00100	10 100001 1000 1100 000 000 1101010 100 010100 01 01	
0 00010	100 010 00001 0000 01 00 10 00 10 000 1000010110001 0000 01	
1 10001 1 11000	00.011000.10100.01.000.00100.01000010.100.1.010.001100	
1 11100	11000 1010 00110001001 000 100010 10000 0 000 1 0001	
1 11110	0.01 (0.00 10100001000010010 011 0010 0011 10000 0	
0 01111 1 10111	150 00 00 00000 0010 1000110000101100 1100000	
0 01011	10 10 000010 0010 110011000101100 1101000 10000	
1 10101	10001101 000110 010 1000010000 011000 10 0.001100 100	
01-01000011	d 001 1000 1101 10110000 00 000 1 000101 0 1 0101011 0	

#### **TEAM Members:**

- B. Sai Kiran (AM.EN.U4CSE19212)
- G. Bharath Schneider (AM.EN.U4CSE19213)
- A. Hemanth Naidu (AM.EN.U4CSE19223)
- C S. Phanindra (AM.EN.U4CSE19263)