# 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.

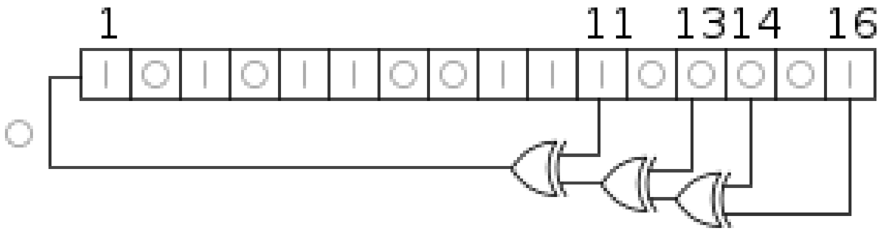
Linear Feedback Shift Registers (LFSR): is a shift register whose input bit is a linear function of its previous state.

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.

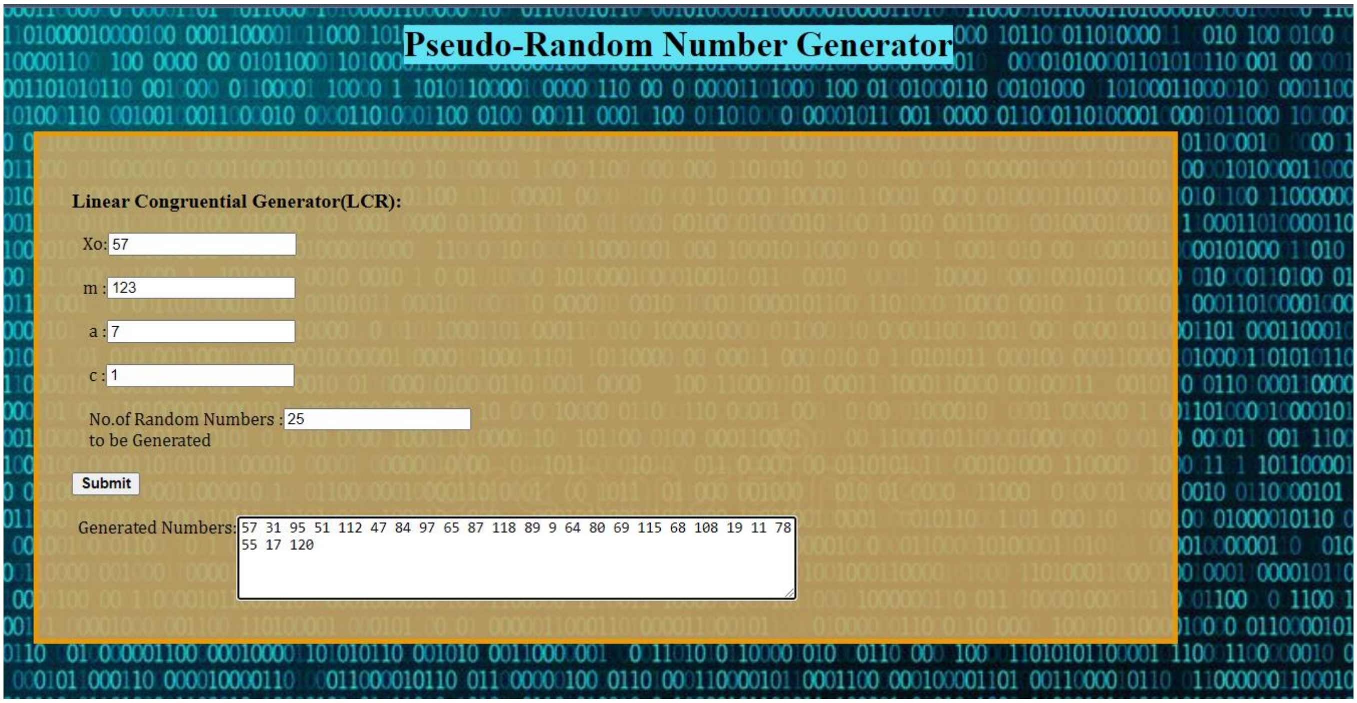
Fibonacci LFSRs: The bit positions that affect the next state are called the taps. In the diagram the taps are [16,14,13,11]. The rightmost bit of the LFSR is called the output bit. The taps are XOR'd sequentially with the output bit and then fed back into the leftmost bit. The sequence of bits in the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



## Pseudo-Random Number Generator

**Linear Congruential Generator(LCR):**

Xo: 57

m : 123

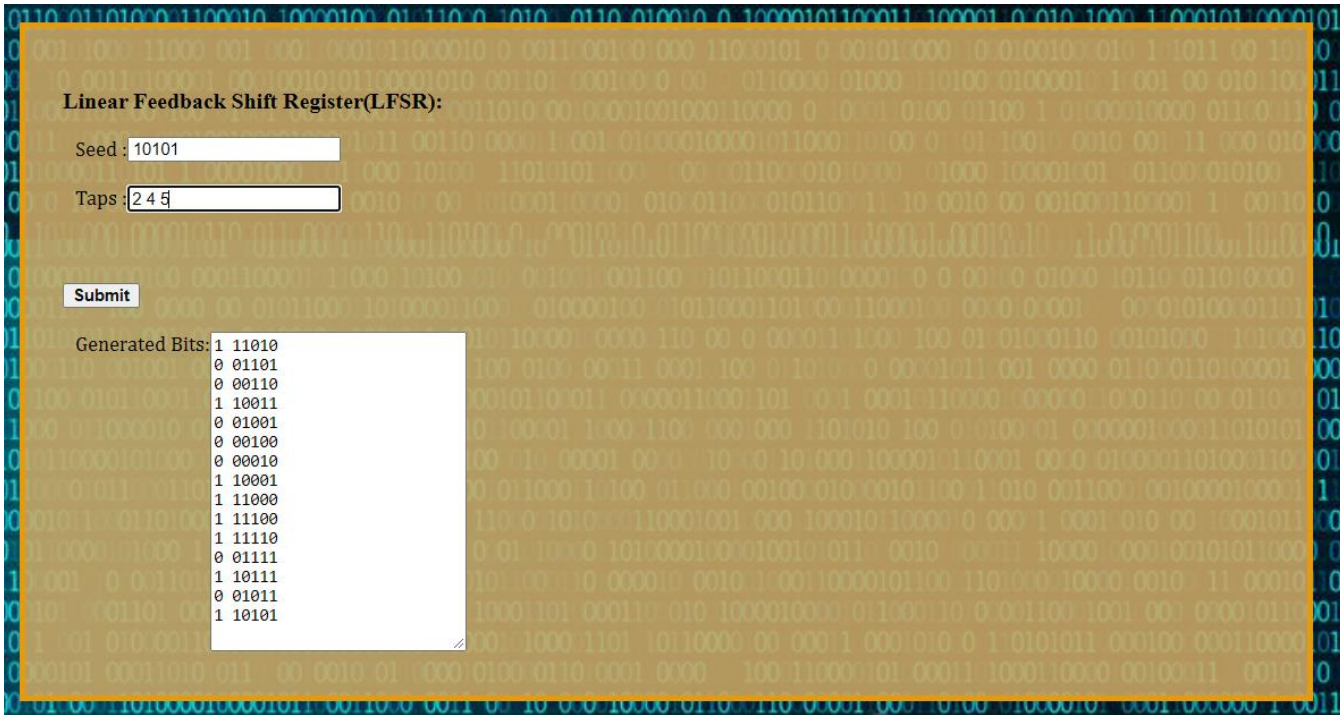
a : 7

c : 1

No.of Random Numbers to be Generated : 25

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
```



**Linear Feedback Shift Register(LFSR):**

Seed : 10101

Taps : 2 4 5

Generated Bits:

```
1 11010
0 01101
0 00110
1 10011
0 01001
0 00100
0 00010
1 10001
1 11000
1 11100
1 11110
0 01111
1 10111
0 01011
1 10101
```

## 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)