XOR Shift

Random Number Generator

P. Ram Anudeep P. Pavan

8th March, 2019

Random Number Generator

- A random number generator (RNG) is a device that generates a sequence of numbers or symbols that cannot be reasonably predicted better than by a random chance.

Random Number Generator

- A random number generator (RNG) is a device that generates a sequence of numbers or symbols that cannot be reasonably predicted better than by a random chance.
- Random number generators have applications in gambling, statistical sampling, computer simulation, cryptography, completely randomized design, and other areas where producing an unpredictable result is desirable.

Random Number Generator

- Various applications of randomness have led to the development of several different methods for generating random data, of which some have existed since ancient times, among whose ranks are well-known "classic" examples, including the rolling of dice, coin flipping, the shuffling of playing cards

Random Number Generator

- Various applications of randomness have led to the development of several different methods for generating random data, of which some have existed since ancient times, among whose ranks are well-known "classic" examples, including the rolling of dice, coin flipping, the shuffling of playing cards
- Because of the mechanical nature of these techniques, generating large numbers of sufficiently random numbers (important in statistics) required a lot of work and/or time.

XOR Shift

- Xorshift random number generators are a class of pseudorandom number generators.

XOR Shift

- Xorshift random number generators are a class of pseudorandom number generators.
- They generate the next number in their sequence by repeatedly taking the exclusive or of a number with a bit-shifted version of itself.

XOR Shift

- Xorshift random number generators are a class of pseudorandom number generators.
- They generate the next number in their sequence by repeatedly taking the exclusive or of a number with a bit-shifted version of itself.
- Xorshift generators are among the fastest non-cryptographically-secure random number generators, requiring very small code and state.

XOR Shift

- Although they do not pass every statistical test without further refinement, this weakness is well-known and easily amended by combining them with a non-linear function, resulting e.g. in a xorshift+ or xorshift* generator.

XOR Shift*

- A xorshift* generator takes a xorshift generator and applies an invertible multiplication (modulo the word size) to its output as a non-linear transformation

XOR Shift+

- Instead of multiplication ,we can use addition as a fast non linear transformation.It adds two consecutive outputs of an underlying xorshift generator based on 32-bit shifts

Input and output

- The first random number(seed)will be given in the code by user.We will generate the random number in the ico board and the output is given to the arduino through digital pins and the output is displayed using serial monitor in arduino.

Implementation

- The random number generator will be implemented as state machine.The random number generator will be initially seeded.The output is shown using arduino.The random number is generated using the following algorithms. 1.XOR SHIFT 2.XOR SHIFT* 3.XOR SHIFT+