Password ➡️ cypherText

encryption

Randomisation

Song Ids : 1,2,3,4

Uniform ✅ 2,1,4,3

Periodic ✅ 2,1,4,3   2,1,4,3   2,1,4,3

Consistence ✅ Returns Consistence Results

Linear Congruential Generator

SampleSize represents number Of elements.

$x(n+1) = (a * x(n) + c)/ Modular$

Take (Modular, a , c) as primeNumbers
a & c < SampleSize
seedValue x(0), should be one of the value in the Sample

cypherText ⬅️ Password

Decryption

$Y = mx + c$

To avoid closest periodic in Randomisation,
make sure moduler is going to be the closest primeNumber of
SampleSize & consider a & c are also be the prime numbers.

x(n+1) = a x(n) + c/ Modular

Randomisation

a = 2 , c = 3, x(0) = 1 , Modular = 5

Uniform ✓   2,1,4,3

Song Ids : 1,2,3,4,5

Periodic ✓   2,1,4,3   2,1,4,3   2,1,4,3

n=0
x(0+1) = 2 * x(0)+ 3 % 4 = 2*1+3 %5=
5%5 = 0
x(1) = 0

Consistence ✓   Returns Consistence Results

linear congruential generator

SampleSize represents number
Of elements.

n=1
x(1+1) = 2 * x(1) + 3 % 5
= 2 * 0 + 3 % 5 = 3
x(2) = 3

x(n+1) = a x(n) + c/ Modular

a & c < SampleSize
seedValue x(0)= should be one of value in the Sample

n=2
x(2+1) = 2 * x(2) + 3 % 5
= 2 * 3 + 3 % 5 = 9%5 = 4
x(3) = 4

Finally 0,3,4,1   0,3,4,1

n=3
x(3+1) = 2 * x(3) + 3 % 5
= 2 * 4 + 3 % 5 = 11%5 = 1
x(4) = 1

n=4
x(4+1) = 2 * x(4) + 3 % 5
= 2 * 1 + 3 % 5 = 5%5 = 0
x(5) = 0

n=5
x(5+1) = 2 * x(5) + 3 % 5
= 2 * 0 + 3 % 5 = 3
x(6) = 3

n=6
x(6+1) = 2 * x(6) + 3 % 5
= 2 * 3 + 3 % 5 = 9 %5 = 4
x(3) = 4

....

Lets Analyse the Graph of out 10K Sample size output, we can not predict

Elements[1006, 2003, 3000, 3997, 4994, 5991, 6988, 7985, 8982, 9979, 969, 1966, 2963, 3960, 4957, 5954 ....]

9979
8982
7985
6988
5991
4994
3997
3000
2003
1006
2963
1966
969