SNS COLLEGE OF TECHNOLOGY

Coimbatore-35
An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A+' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

19ITB302-Cryptography and Network Security

UNIT-2 NUMBER THEORY AND PUBLIC KEY CRYPTOSYSTEMS

Random Numbers

1.Randomness

Sequence of numbers be random in some well- defined statistical sense.

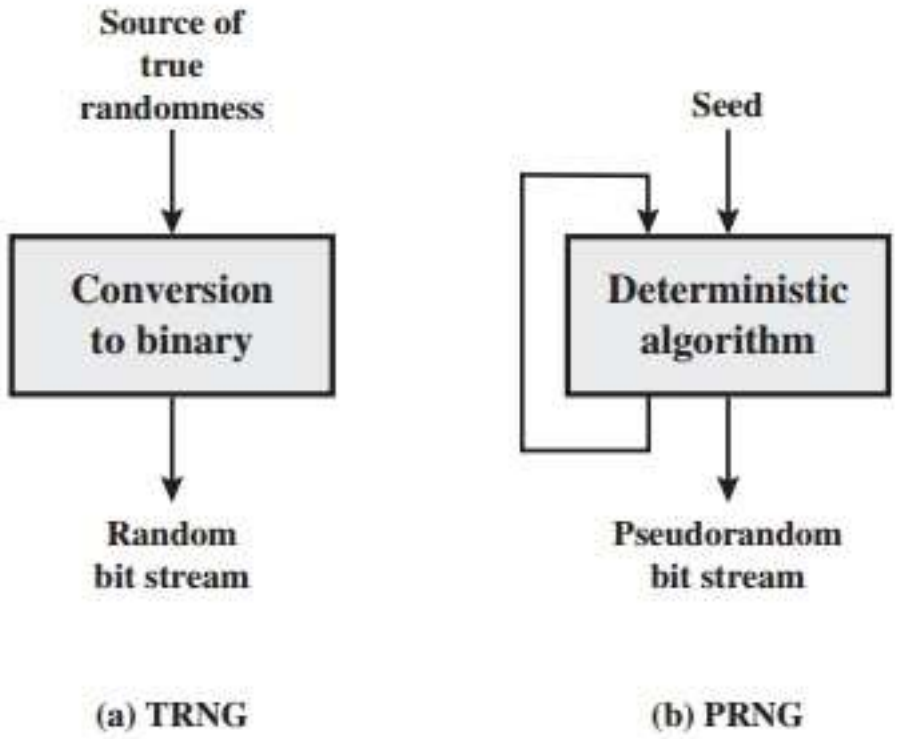
Uniform distribution: The distribution of bits in the sequence should be uniform; that is, the frequency of occurrence of ones and zeros should be approximately equal.

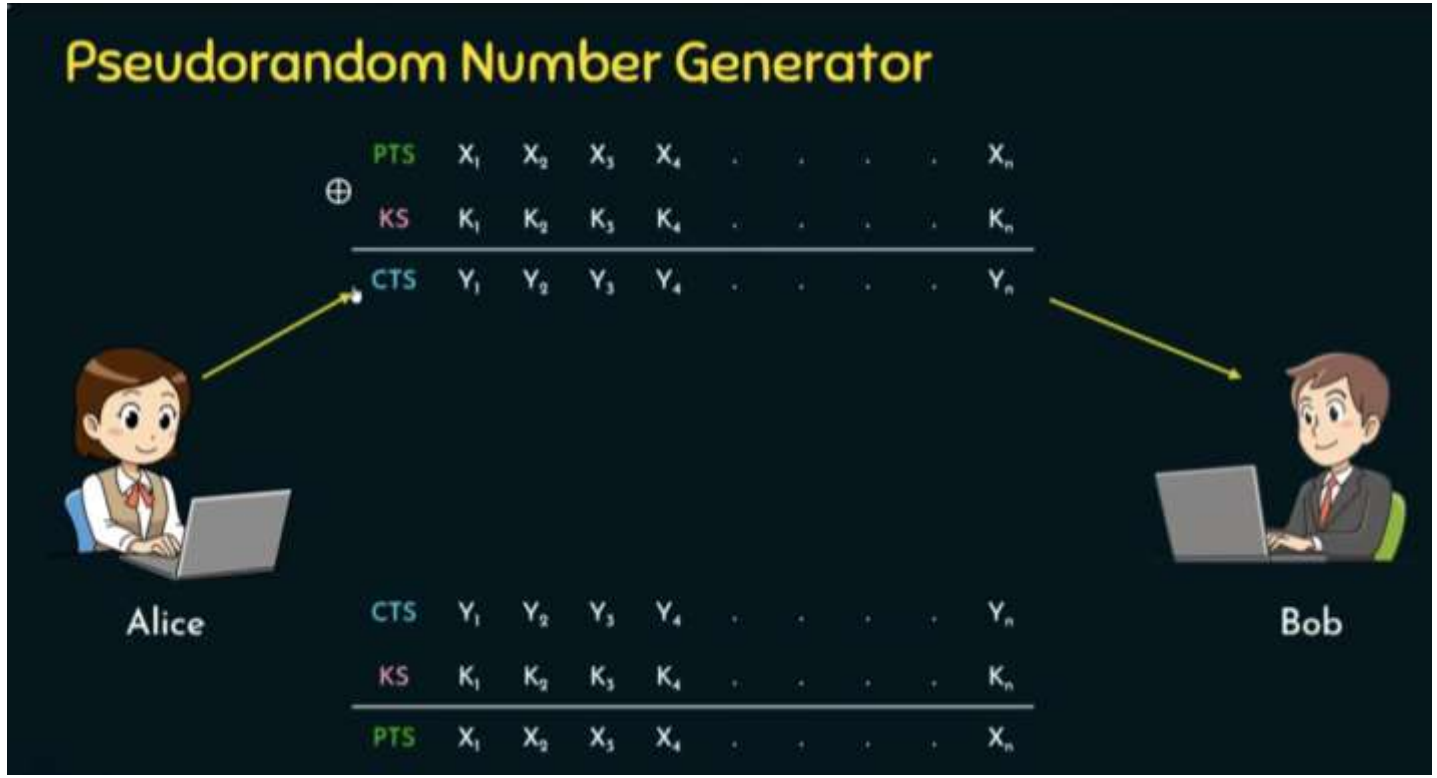
2.Unpredictability

The values are uniformly distributed over a defined interval or set, and it is impossible to predict future values based on past or present ones.

Pseudorandom Number Generator

Pseudo-random numbers are generated using deterministic algorithms and appear random




Pseudorandom Number Generator
PTS X_1 X_2 X_3 X_4 . . . . X_n
⊕
KS K_1 K_2 K_3 K_4 . . . . K_n
CTS Y_1 Y_2 Y_3 Y_4 . . . . Y_n
Alice
CTS Y_1 Y_2 Y_3 Y_4 . . . . Y_n
KS K_1 K_2 K_3 K_4 . . . . K_n
PTS X_1 X_2 X_3 X_4 . . . . X_n
Bob

Linear Congruential Generators

- $X_{i+1}=(a* Xi +c) \bmod m$
- $Ri=Xi/m$
- X_0=Starting Seed value
- a is the multiplier
- C is the increment
- m is the modulus

Example

Given values

- $X_{0=27,a=17,c=43,m=100}$
- $X_{i+1=(aXi+c)mod\ m}$
- **X1=(17*27+43)mod 100**

=502 mod 100

X1=2

X2=(17*2+43)mod 100

=77 mod 100

X2=77

- X3=(17*77+43)mod 100

=1352 mod 100

=52

X4=(17*52+43)mod 100

=927mod 100

=27

X5=(17*27+43)mod 100

=502 mod 100

=2

Ri=Xi/m

R1=2/100=0.02

R2=77/100=0.77

R3=52/100=0.52

R4=27/100=0.27

R5=2/100=0.02

Blum Blum Shub Generator

- It was created by Lenore Blum, Manuel Blum and Michael Shub in 1968.
- Cryptographically secure pseudorandom generator
- Choose two prime numbers p,q such that both have a remainder of 3 when divided by 4
- Next compute n=p*q(**eg:p=7,q=11**)
- Choose a random number s , such that s is relatively prime to n(**any integer that is not divisible by 7 or 11 will be relatively prime to 77.**)

Algorithm

$X_0=s^2 \bmod n$

For i=1 to infinity

$X_i=(X_i-1)^2 \bmod n$

$B_i= X_i \bmod 2$

Division Algorithm

The notation ***b | a*** is commonly used to mean ***b*** divides ***a***. Also, if ***b | a***, we say that *b* is a **divisor** of *a*.

Given any positive integer ***b*** and ***a***,

if we divide ***a*** by ***b,*** we get an integer quotient ***q*** and an integer remainder ***r*** that obey the following relationship:

$a=qb+r$ where $0<r<b$;$q=a/b$

Example

$a=21, b=2$

$a=10*2+1$(r=1 and r is between 0 and 2)

Euclidean Algorithm

The Euclidean algorithm is a way to find the greatest common divisor of two positive integers.

GCD of two numbers is the largest number that divides both of them

The Algorithm

The Euclidean Algorithm for finding GCD(A,B) is as follows:

- If A = 0 then GCD(A,B)=B, since the GCD(0,B)=B, and we can stop.
- If B = 0 then GCD(A,B)=A, since the GCD(A,0)=A, and we can stop.
- Write A in quotient remainder form (A = B·Q + R)
- Find GCD(B,R) using the Euclidean Algorithm since GCD(A,B) = GCD(B,R)