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.

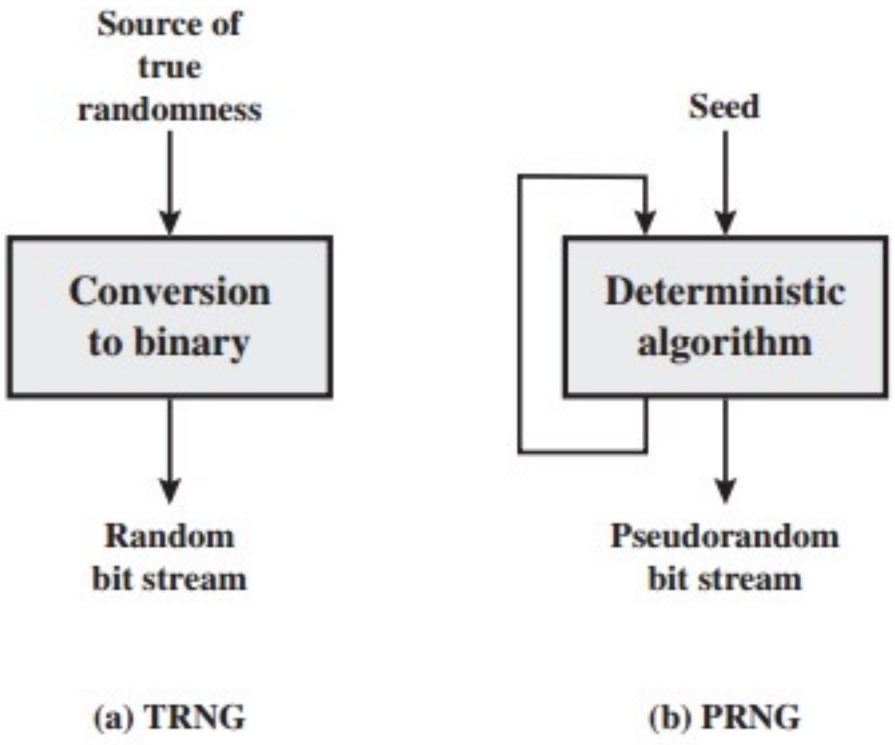
Uniform distribution: The distribution of bits in the sequence should be uniform; that is, the frequency of occurrence of ones and zeros should be approximately equal.

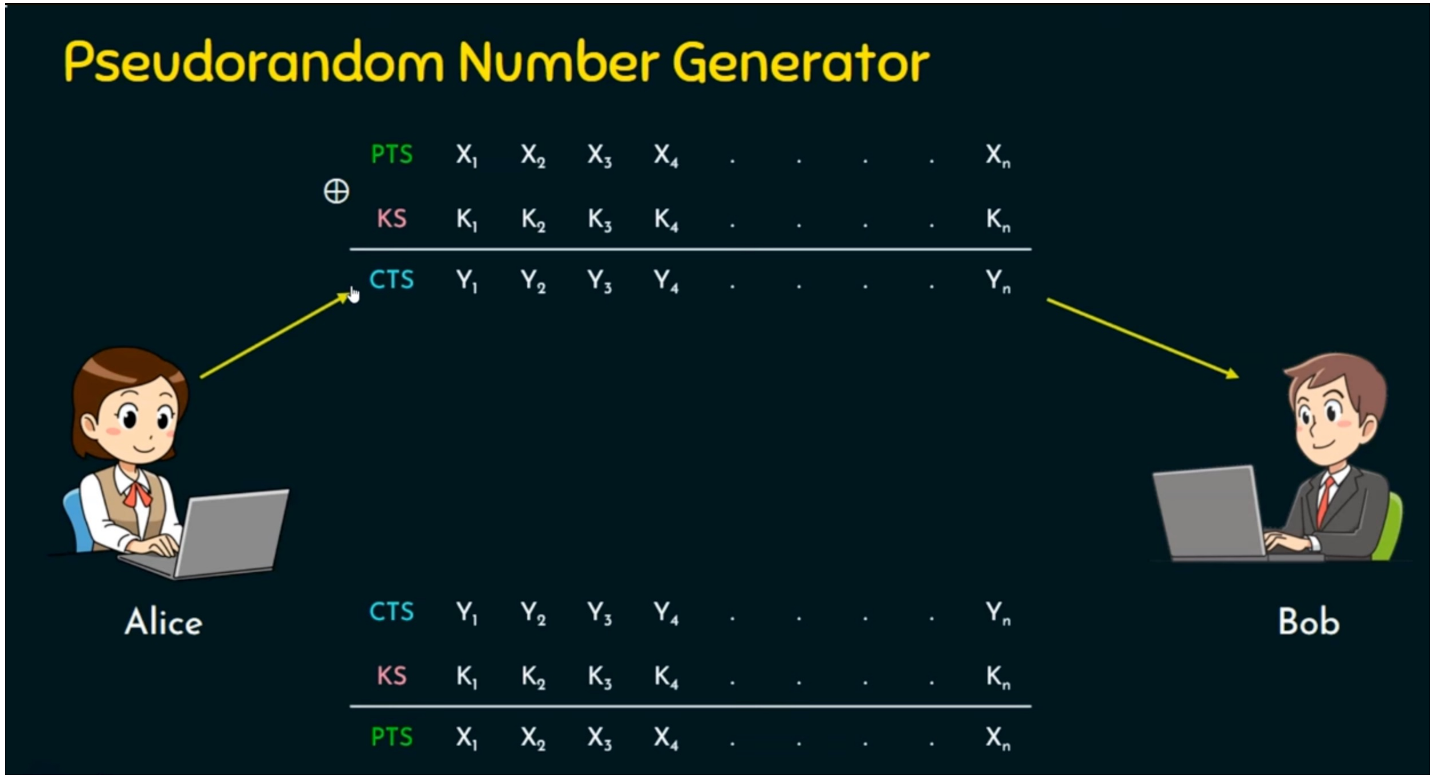
2.Unpredictability

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
$\oplus$	KS	K_1	K_2	K_3	K_4	.	.	.	.	K_n
	CTS	Y_1	Y_2	Y_3	Y_4	.	.	.	.	Y_n

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