###### ASSIGNMENT NO: BD2

**TITLE:**

Write a program to generate a pseudorandom number generator for generating the long-term private key and the ephemeral keys used for each signing based on SHA-1 using Python/Java/C++. Disregard the use of existing pseudorandom number generators available.

**PREREQUISITES**

* 64-bit Fedora or equivalent OS with 64-bit Intel-i5/i7
* Python 2.7

**OBJECTIVES:**

1. To develop problem solving abilities using Mathematical Modeling.
2. To understand the use and working of Pseudorandom number generator.

**MATHEMATICAL MODEL:**

Let P be the solution perspective.

Let, S be the System Such that,

A= {S, E, I, O, F, DD, NDD, success, failure}

Where,

S= Start state,

E= End State,

I= Set of Input

O= Set of Out put

F =Set of Function

DD=Deterministic Data

NDD=Non Deterministic Data

Success Case: It is the case a pseudorandom number is generated.

Failure Case: It is the case when some exception occurs and pseudorandom number is not generated.

**THEORY:**

**CONCLUSION:**

Hence, we have written program which is capable of generating pseudorandom number without using existing pseudorandom number generator available.