Research Methodology

Assignment: 2

Name: Nazmul Hasan

Id: 18-37377-1

Section: H

Department : CSE

Q1. Write down the Motivation of your proposal

Topic:

Hashing Function on Random Number Generator on Chaotic Function using Monte Carlo Method.

Motivation:

A Hash Function maps arbitrary strings. A simple hash function taking a mod with a prime number. We use Number Theory in hashing Function. Hash table are widely using in database indexing, caching, error finding, programming and much more. If we want to password verification we should use Cryptographic hash function.

Q2. Make a reference list of paper to do your Literature review

1. R. Benny Gandara ,Gunawan Wang, DitditNugerahaUtama , “Hybrid Cryptography on Wireless Sensor Network: A Systematic Literature Review ”.

2. Muhammad Rashid ,Malik Imran , AtifRazaJafri , “Comparative Analysis of Flexible CryptographicImplementations ”

3. Anders J Johansson ,HenrikFloberg,“ Random Number Generation by Chaotic Double Scroll Oscillator on Chip”.

4. B. Cornelissen, A. Zaidman, A. Deursen, L. Moonen, and R. Koschke, “A systematic survey of program comprehension through dynamic analysis,” *TSE*, vol. 35, no. 5, pp. 684–702, 2009.

5.M.M. MahbubulSyeed, ImedHammouda, TarjaSyst¨a, “Evolution of Open Source Software Projects: A Systematic Literature Review” . JOURNAL OF SOFTWARE, VOL. 8, NO. 11, NOVEMBER 2013

6.Gupta S, Chattopadhyay A, Sinha K, Maitra S, Sinha BP. High-Performance Hardware Implementation for RC4 Stream Cipher. IEEE Trans Comp 2013; 62(4):730-743.

7.Thomas DB, Luk W. High quality uniform random number generation using LUT optimised state-transition matrices. Journal VLSI Signal Process 2007; 47(1).

8. Castro, et.al., 2005, "The strict avalanche criterion randomness test", Mathematics and Computers in Simulation 68 (2005) 1–7,Elsevier

9.MalteSharupke, 2018, "Fibonacci Hashing: The Optimization that the World Forgot (or: a Better Alternative to Integer Modulo)"

10. Knuth, D. 1973, The Art of Computer Science, Vol. 3, Sorting and Searching, p.512-13. Addison-Wesley, Reading, MA., United States

Q3. Present the abstract of a single paper

Abstract :

A Hash Function maps arbitrary strings simple hash function taking a mod with prime. It is a simply a question of computing a hash and because the fixed length output is going to be something on the order of 160 bits or 256 bits. Randomness is going to because of Collision resistance..Pseudo random function can generate by using shift register. PRNGs are used in Simulations, Gaming and Cryptography.