RESEARCH METHODOLOGY
ASSIGNMENT 1

Name : Nazmul Hasan
Id : 18-37377-1
Section : H

1. Write several general problems related to CS & ICT(at least 15).

i. Computer viruses and main principles of work.
ii. Biotechnology, medicine, and computer science.
iii. Database architecture and management.
iv. Digital security versus private information.
v. The importance of open source software.
vi. Biometric systems and recognizing.
vii. DDOS attacks, their danger on the global scale and their prevention.

Write several general problems related to CS & ICT(at least 15).

viii. AI and robotics.
xi. Computer techniques in photography.
x. 3-D object modelling.
xi. Media security: basic techniques.
xii. Databases and information retrieval systems.
xiii. Cyber-physical systems.
xiv. Future of 5G wireless systems.
xv. Networking and security.

2. **Build argument why such general problems are worth to do research.**

Answer : Today we are living in the era of technology. Without technology we can't think about ourselves. We are depending on technology in every seconds. We are storing all ours important information on internet, these data can be lost any time so we should do more research about it to make it secured. We should work more all about these to increase efficiency. So that we can find the hundred percent accurate result. How more research we will do on them the more accuracy and perfection we will find.

3. Select a topic as your project proposal's topic of this course (individual project).

- **Hashing Function on Random Number Generator on Choatic Function using Monte Carlo Method.**

4. **Make a two minute slide presentation (individual presentation).**

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.

INTRODUCTION: Cryptography means secret of writing code. There are two things. One is cryptography and other is cryptanalysis. Cryptography means making code and Cryptanalysis means breaking code. In Cryptography there are many times of cipher .Transposition cipher, Substitution cipher, Vigenerecipher, play fair cipher etc. Transposition cipher is one that does not change any letters of the original message. In Transposition cipher the letter was same when reverse the original message. The Rail fence Cipher means count the number of letters. Decoding the message is easy as Encoding the message. We use Genetic algorithm to break Transposition cipher. In the early decade Arab use Cryptography. They use Quran Ayat for secret Communication. Frequency analysis use for breaking Ceasercipher. CharlesBabez was the father of Cryptography. He break the Vigenere cipher to use mathematical equation. Telegraph and Engima machine use before Cryptography. A cryptographic system has two main operators, which are diffusion and confusion.

Example: When you use any online website which requires a user login, you enter your E-mail and password to authenticate that than you go the website. A hash of the password is computed when the password enter than it go to the server and sent it for password verification..In File system we use hash function. We use hash function in google searching.