고급 소프트웨어 실습

분반: 1 반(월요일)

학번: 20181662

이름: 이건영

과제 1. LCG, MT 이외의 난수 생성 방식에 관하여 3 가지 이상 열거하고 설명하시오. (폰트 10, 반페이지 분량)

- 중앙 제곱법

$$X_{n+1} = (X_n)^2 \text{의 가운데 } a \text{자리}$$

시드 X0(a 자리의 수)를 사용하여 난수를 생성한다. 폰 노이만에 의해 1949 년에 고안되었으며 수식이 간단하나 생성된 난수를 예측하기 쉬워 현재는 잘 사용되지 않는다.

- XOR shift

XOR 과 Bit shift 연산을 사용하여 연산 속도가 빠르고 품질이 좋은 난수를 생성한다.

- True Random Number Generator

LCG 와 MT 를 포함한 위의 방식들은 모두 Pseudo Random 방식의 난수를 생성하는 알고리즘이다. 그러나 하드웨어를 통해 자연계에 존재하는 무작위성을 이용한 난수를 생성할 수 있고, 이렇게 생성한 난수의 패턴을 파악하여 이후에 나올 난수를 특정하는 것은 거의 불가능하다.