고급 소프트웨어 실습

분반: 1 분반

학번: 20181687

이름: 정지석

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

1. XOR Shift

XOR 연산과 Bit Shift 연산을 사용하여 난수를 생성하는 방법이다. 수업시간에 다루었던 Mersenne Twister 와 유사하다.
난수 생성방식은 초기에 들어온 값을 shift 연산을 하여 계산한 뒤, 그 결과값에 다시 XOR 연산을 하여 난수를 생성하는 식으로 이루어진다.

2. 중앙제곱법(Middle-square Method)

중앙제곱법은 1949 년 폰 노이만이 고안해낸 난수 생성 방법론으로, 임의의 숫자를 제곱한 뒤, 그 제곱한 값의 일부분 n 자리 숫자를 뽑아내서 난수를 생성하는 방식이다.
예를 들어 자연수 123 을 제곱한 뒤, 그 값의 중앙에 있는 3 자리를 뽑아 난수를 생성한다 하면, 123 * 123 = 1**512**9 => 512 가 된다. 즉 중앙제곱법을 통해 512 라는 난수를 생성한 것이 된다.

3. True Random Number Generator

위에서 설명했던 방식들과 수업시간에 다루었던 LCG, 메르센 트위스터의 단점을 보완한 방법론이다. 위의 방식들은 모두 소프트웨어에서 난수를 생성하려 하니 한계가 발생하게 되는데, True Random Number Generator 는 특수한 하드웨어를 사용하여 난수를 생성한다. 이 하드웨어는 주변 환경에서 발생하는 무작위한 현상들을 관찰하여 이를 난수로 출력하기 때문에 난수 값을 예측하는 것이 불가능하다.