고급 소프트웨어 실습

분반: 월분반

학번: 20181702

이름: 홍주표

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

LCG(선형합동법)과 MT(메르센 트위스터) 이외의 난수 생성 방식에는 중앙제곱법, XOR 시프트, 진짜 난수 생성 등이 있다.

중앙제곱법(Middle-square method)은 의 가운데 a자리를 사용한다. 이 때, X는 난수 수열, a는 원하는 자릿수, 시드(는 임의의 a자리인 수이다. 이는 폰 노이만이 고안한 의사난수법이지만 생성된 품질이 좋지 않다는 단점이 있다.

XOR 시프트(Xorshift)는 XOR과 비트시프트 연산을 사용하는 난수 발생법이다. 구조상 현대의 컴퓨터에서 연산 속도가 매우 빠르고 품질도 선형합동법보다 좋다는 장점이 있지만, 몇몇 난수 품질 테스트를 통과하지 못하는 경우가 있다는 단점이 존재한다. 따라서 여러 변종이 생겼다.

LCG, MT, 중앙제곱법, XOR 시프트는 모두 의사난수(Pseudo Random)에 속한다. 이들은 소프트웨어상으로만 난수를 생성하려고 하다보니 발생한 한계이다. 자연계에 존재하는 무작위성을 센서 시스템을 이용하여 관찰하고 난수를 만들어내는, 하드웨어를 통해 진짜 난수를 만들어낼 수 있다. 진짜 난수 생성의 예시로는 SK텔레콤에서 개발하고 삼성전자의 스마트폰 True Random Number Generator 사이트 등이 있다.