고급 소프트웨어 실습

분반: 1

학번: 20191574

이름: 김예진

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

첫 번째 난수 생성 방식으로는 중앙 제곱법이 있다. 1949 년에 폰 노이만이 고안한 의사 난수법으로 이전의 생성한 난수를 제곱하고, 그 결과에서 가운데의 n 개를 추출하여 다음 난수를 생성하는 방식이다. 난수 하나를 알게 되면 그 이후의 값들도 연산을 통해 쉽게 예측할 수 있는 방식이므로 보안에는 적절하지 않은 방식이다. 이 알고리즘이 고안되었던 당시에는 컴퓨터의 성능이 좋지 않아 이렇게 간단한 방식을 통해 난수를 생성하였고 최근에는 거의 사용되지 않는다고 한다.

두 번째 난수 생성 방식은 XOR shift 방식이다. 메르센 트위스터와 같이 bit shift 연산을 사용하여 난수를 발생시킨다. 구조상 현대의 컴퓨터에서 연산 속도가 매우 빠르고 품질도 선형 합동법에 비해 좋아 자주 사용된다고 한다. XOR shift 알고리즘에는 종류가 여러 개 있는데, 이 때 32 bit, 64 bit, 128 bit 의 수를 사용하며 그 주기는 각각 $2^n - 1$과 같은 형태의 메르센 수 난수 반복 주기를 갖는다.

마지막으로는 양자 난수 생성 방식이 있다. 이 난수 생성기는 패턴을 분석할 수 없는 순수 난수를 만드는 장치이다. 양자역학적 성질을 이용하여 특정 제한 조건에 따라 일련의 난수를 발생시키며 통신 네트워크를 통한 외부 위협으로부터 원천 봉쇄할 수 있다고 한다. 양자역학 현상들로부터 발생하는 무작위성에 의존하기 때문에 순수 난수를 생성하고 이로 인해 안정성 관련 문제를 해결할 수 있어 보안 분야에 사용하기 적합하다. 하지만 실제 응용에서는 값이 편향될 수 있고, 비트를 빠르게 산출하지 못한다는 단점이 있다.