**1. LCG, MT 이외의 난수 생성 방식**

**1. Xorshift 생성기**

Xorshift 생성기는 조지 마스카리아스(George Marsaglia)가 개발한 난수 생성 알고리즘으로

기본 원리는 초기 상태를 가지고 비트 **XOR 연산**과 **시프트 연산**을 반복하여 새로운 값을

생성하는 것이다.코드가 매우 간단하고 빠른 연산 속도를 가지는 장점이 있지만

다른 난수 생성기에 비해비교적 짧은 주기를 가지고 있어 난수의 패턴이 반복될 수 있다.

**2. WELL 생성기**

WELL 생성기는 메르센 트위스터(MT)의 단점을 보완하기 위해 프랑스의 Pierre L’Ecuyer와

그의 연구진이 개발한 난수 생성 알고리즘으로 난수가 균등하게 분포되도록 설계되어

특정 초기 상태에서 편향 문제를 줄이며, 고품질의 의사 난수를 생성할 수 있다.

초기 상태가 균등하지 않아도 안정된 난수 품질을 보장하지만 알고리즘이 비교적 복잡하여

단순히 구현하기 어려울 수 있다.

**3. 역 합동 생성기(Inverse Congruential Generator)**

역 합동 생성기는 역함수를 사용하여 난수를 생성하는 알고리즘으로 이 알고리즘은 기존의

LCG와 비슷하지만, 중요한 차이는 현재 상태의 역원을 계산하여 다음 값으로 사용하는 것이다.

다음과 같은 수식을 기반으로 한다:

역원의 사용으로 인해 더 복잡한 패턴의 난수를 생성할 수 있고, LCG보다 균일한 분포를 생성하는 경향이 있지만 modular 역원 계산은 일반적인 곱셈이나 덧셈보다 계산 비용이 크다.

또한 a, c, m같은 파라미터가 적절히 선택되지 않으면 주기가 짧아질 수 있다.

**4. 블럼-블럼-샙(Blum-Blum-Shub, BBS)**

블럼-블럼-샙(BBS)은 두 큰 소수의 곱을 기반으로 하여 예측이 불가능한 비트 스트림을

생성하는 난수 생성 알고리즘이다. 높은 보안성과 예측 불가능성이 있지만

다른 난수생성기에 비해 속도가 느리고 초기 설정이 복잡하다는 단점이 있다.