Muhammad Rafay

20P-0018.

Information Security

The Blum Blum Shub (BBS) generator is a pseudorandom number generator that uses two secret large prime numbers to create a sequence of random bits. It's secure because breaking it requires factoring a semiprime numbers, which is hard problem.

However, it's slow and not commonly used in modern cryptography.

//Code.

```
Impoot Math

def is_prime(num):
    if num < 2:
        return False

    For i in range (2, int (math.sqrt(num)) +1):
        if num % i == 0:
            return False
    return True
```

```
def generate_bbs_sequence(p, q, seed, length):
    N = p * q
    X = seed
    result = []

    for _ in range(length):
        X = (X * X) % N
        result.append(X % 2)

    return result

# Choose large primes p & q.
p = 499
q = 503
# Choose a random seed (Must be relatively prime to N)

Seed = 12345
Length = 10.
sequence = generate_bbs_sequence(p, q, seed, length)
print(sequence)
```