Name: Jawad Ahmed

Roll No: 20P-0165

Section: BCS-7A

Assignment # 03

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 -prime number, which is a hard problem. However, it's slow and not commonly used in modern cryptography.

```
// code
import 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 and q
P = 499
q = 503

# choose a random seed (must be relatively prime to N)
Seed = 12345

# Generate a pseudorandom sequence of length 10
Sequence = generate_bbs_sequence (p, q, seed, 10)
Print (sequence)
```