Name: Muhammad Sherjeel Akhtar

Roll No: 20p-0101

Section: 7B

Assignment: 03

Submitted To Respected Sir: Dr Muhammad Amin.

7B

BLUM-BLUM-SHUB:

→ The Blum Blum Shub (BBS) algorithm is a pseudo number generator (PRNG) algorithm designed by Lenore Blum.

→ Blum-Blum Shub is categorized due to its simplicity and provable security under certain conditions.

⇒ Algorithm Working:

(1) Choose two large prime numbers, p and q such that $p \equiv q \equiv 3 \pmod{4}$. This congrates (congruence) condition helps ensure the security of the algorithm.

(2) Calculate the modulus $N = p * q$

(3) Choose a random seed value, that is relatively prime to ~~M~~ N. This means that

the greatest common divisor (GCD) of x_0 and N should

be 1.

(4) To generate pseudorandom bits, iterate the following process:

(1) Calculate $x_{i+1} = (x_i)^2 \mod N$, where x_i is the current value

(2) Extract a bit from x_{i+1}, often by taking the least significant bit.

The resultant sequence of bits is considered pseudorandom.

(MDh)

⇒ PYTHON -IMPLEMENTATION:

```
def blum_blub_shub(seed, n):
        p = 499
        q = 547
        x = seed
    result = []
for _ in range(n):
        x = (x*x) % (p*q)
        bit = x % 2
        result.append(bit)
        return result
seed = 123456      #initial seed value
    n=10           #Number of bits to generate
random_bits =blom_blum_shub(seed,n)
    print(random_bits)
```

Scanned with CamScanner

AND

By

Using, this algorithm will generate true random numbers that can be used later on for

ENCRYPTION PURPOSE.