**Security of the BBS Generator-**

**Blum Blum Shub** (**B.B.S.**) is a [pseudorandom number generator](https://en.wikipedia.org/wiki/Pseudorandom_number_generator) proposed in 1986 by [Lenore Blum](https://en.wikipedia.org/wiki/Lenore_Blum), [Manuel Blum](https://en.wikipedia.org/wiki/Manuel_Blum) and [Michael Shub](https://en.wikipedia.org/wiki/Michael_Shub)that is derived from [Michael O. Rabin](https://en.wikipedia.org/wiki/Michael_O._Rabin)'s one-way function.

* It was created by Lenore Blum, Manuel Blum and Michael Shub in 1968. Blum Blum Shub uses the form of xn+1=x2n (modM)

and where x0 is a random seed.

* The value of M is equal to pq, and where p and q are prime numbers. These values of p and q are both congruent to 3 mod 4 (p=q=3(mod4)).
* The security of the method involves the difficulty in factorizing M. It is slow, but is the strongest proven random number generator.
* For each step, we extract some of the information from xn+1, and which is typically the least significant bit. It would not be used within a cipher application, but could be used in key generation.

