Abstract

Random key bit generators are used in statistically secured stream ciphers. In stream ciphers pseudorandom key bits are XORed with non-random text bits to generate random cipher bits. In practice, it is impossible to get a Random Bit Generator (RBG) that can be used for encryption as well as for decryption. The solution is to search for a suitable Pseudo Random Bit Generator (PRBG). In this paper, a comparative study of randomness of RC4 is made with that of six set of pseudorandom 8-bit sequences generated by introducing some variations in BBS and PM algorithms. In RC4, the given key randomizes an 8-bit identity S-Box in 256 rounds. The BBS and PM require an initial seed to be given as key. In the study, one algorithm generates 167800 pseudorandom 8-bit key sequences for a given key. For each of the seven sets, 300 such sequences are generated using 300 different given keys. The randomness of 300 sequences for each set are tested using three test modules.

References

- L. Schrage, A More Portable Fortran Random Number Generator, ACM Transactions on

**Index Terms**

Computer Science

Security

**Keywords**

NIST Statistical Tests  Pseudorandom Bit Generator  Statistical Randomness Test  Stream Cipher.