Abstract

In the latest past, research work has been done in the region of steam ciphers and as a answer of which, several design models for stream ciphers were projected. In Order to appreciate a international standard for data encryption that would prove good in the due course of time, endure the action of cryptanalysis algorithms and reinforce the security that will take longer to be broken, this research work was taken up. There is no standard model for Stream cipher and their design, in comparison to block ciphers, is based on a number of structures. We would not try to evaluate the different designs taken up by various stream ciphers, different attacks agreed out on these stream ciphers and the result of these attacks. During this exercise we would also have a better idea of the latest stream ciphers designs.

References

- Mantin, I. and Shamir, A. “A Practical Attack on Broadcast RC4”.
- Mossel, E., Peres, Y. and Sinclair, A. 2004 “Shuffling by semi random transporting”.
- Babbage, S., Canniue, C. D., Lano, J., Preneel, B., and Vandewalle, J. Distinguishing attacks on SOBER-t32.
- Wikipedia, the free Encyclopedia.

**Index Terms**

Computer Science

Security

**Keywords**

Attacks stream cipher AES LFSR