Abstract

Once an application steps out of the bounds of a single-computer box, its external
communication is immediately exposed to a multitude of outside observers with various intentions, good or bad. In order to protect sensitive data while these are en route, applications invoke different methods. In today’s world, most of the means of secure data and code storage and distribution rely on using cryptographic schemes, such as certificates or encryption keys. Thus, cryptography mechanisms form a foundation upon which many important aspects of a solid security system are built. Cryptography is the science of writing in secret code and is an ancient art. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then; those new forms of cryptography came soon after the widespread development of computer communications. There are two basic types of cryptography: Symmetric Key and Asymmetric Key. Symmetric key algorithms are the quickest and most commonly used type of encryption. Here, a single key is used for both encryption and decryption. There are few well-known symmetric key algorithms i.e. DES, RC2, RC4, IDEA etc. This paper describes cryptography and its types and then proposes a new symmetric key algorithm X-S cryptosystem based on stream cipher. Algorithms for both encryption and decryption are provided here. The advantages of this new algorithm over the others are also explained.

References

Keywords
Cryptography  Encryption  Decryption  X-s Cryptosystem  Pretty Good Privacy
Symmetric Key Algorithm.