ABSTRACT

Context free grammars present the desirable cryptographic property that it is easy to generate and validate strings from a given grammar; however it is hard to identify a grammar given only the strings generated by it. There is no theoretical study which proves that, given a set of strings from a language how difficult it is to generate another string which belongs to the same language.

Due to this unique property of CFG the proposed idea is to develop a CFG based cryptosystem to provide security for text files. This cryptosystem is a symmetric key encryption technique which consists of various modules: key generation, encryption and decryption at sender and receiver side.