Abstract

With growth of networked systems and applications such as e-commerce, the demand for internet security is increasing. Information can be secured using cryptography, anti-virus,
malwares, spywares, firewall etc. In cryptology, cryptanalysis is a discipline where the ciphers are attacked and broke thus enabling the developers to strengthen the cipher. Nowadays cryptanalysis of ciphers is gaining popularity among the research world. One among the ciphers is the knapsack cipher. There are many methods to attack this cipher. One among them is the Genetic Algorithm (GA) approach. Using GA, researchers have attacked the knapsack cipher with a knapsack sequence of size 8. This supports the ASCII representation of the characters. The ASCII representation supports the regional languages like English, numerals and symbols. In this paper we propose the attack on knapsack cipher with knapsack sequence of size 16 using Genetic Algorithm. The increase in knapsack sequence size increases the strength of the knapsack cipher. The increase in knapsack sequence size also supports for Unicode representation. Unicode representation gives hold for many regional languages. Since any language information can be transmitted over the network, this approach supports attack on text of any language. Also there is no constraint on the length of text to be attacked. An analysis on the impact of various GA control parameters viz. initial population size, operators’ type and probability, etc are also carried out in this research work.

References

- Spillman Richard, Cryptanalysis of knapsack ciphers using genetic Algorithms,

Index Terms

Computer Science Security

Keywords

Cryptanalysis Genetic Algorithm (GA)
Knapsack Cipher