Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for more Secure Communication

Foundation of Computer Science (FCS), NY, USA

Volume 129 - Number 13

Year of Publication: 2015

Authors:

Atish Jain, Ronak Dedhia, Abhijit Patil

Abstract

Caesar cipher is an ancient, elementary method of encrypting plain text message into cipher text protecting it from adversaries. However, with the advent of powerful computers, there is a need for increasing the complexity of such techniques. This paper contributes in the area of classical cryptography by providing a modified and expanded version for Caesar cipher using knowledge of mathematics and computer science. To increase the strength of this classical encryption technique, the proposed modified algorithm uses the concepts of affine ciphers, transposition ciphers and randomized substitution techniques to create a cipher text which is nearly impossible to decode. It also increases the range of characters which Caesar cipher Algorithm can encrypt by including all ASCII and extended ASCII characters in addition to alphabets. A complex key generation technique which generates two keys from a single key is used to provide enhanced security. This paper aims to propose an enhanced version of Caesar cipher substitution technique which can overcome all the limitations faced by classical Caesar Cipher.
References

2. http://searchsecurity.techtarget.com/definition/cipher

Index Terms
Computer Science
Communications

Keywords
Caesar Cipher, Substitution Cipher, Transposition Cipher, Affine Cipher, Encryption, Decryption, Cryptography, Shift Cipher, Randomized, Plain Text, Cipher Text, Cryptanalysis.