IMPLEMENTATION OF MODIFIED CAESAR CIPHER ALGORITHM IN CHAT APPLICATIONS

KANIYA MAHARANI

Informatics Study Program Faculty of Science & Technology
University of Technology Yogyakarta
Jl. Ringroad Utara Jombor Sleman Yogyakarta
E-mail : didik8736@gmail.com

ABSTRACT

Advances in technology, especially communication, make interaction between humans easier in exchanging information through text messages. However, from the many positive sides, the risks and threats of sending messages through the internet and/or Local Area Network (LAN) networks are also great, namely that unauthorized people can read, disseminate and modify the message/information. Chat applications with cryptographic techniques are needed in the process of exchanging messages between two people to maintain confidentiality, data integrity, authenticity and anti-denial of data. The algorithm used in this study is a modified Caesar Cipher, a combination of classical and modern cryptography to encrypt messages (plaintext) into secret information (ciphertext) by converting each character in the plaintext into its ASCII code (American Standard Code for Information Interchange), then calculated using the encryption key provided by the user, after all characters are converted into a new ASCII code, the code is converted again into a character string that matches the ASCII code. There are 95 special characters that will be used by the author (starting from character no.32 to no.127). From the testing process, it is found that the encryption and decryption process can maintain the confidentiality of communication data between two people without being read by other users in the same chatroom. The resulting application is a desktop-based application in a Local Area Network (LAN) with a modified Caesar Cipher algorithm using ASCII characters.

***Keywords**: Chat Application, Caesar Cipher, ASCII, LAN, Chatroom*