ABSTRACT

IMPLEMENTATION OF SALSA20 TO PROTECT DOCUMENT FILE ON FTP SERVER

By

M. Fikri Aqsha Zulfa Ismail

19102136

File Transfer Protocol (FTP) is a network protocol for sending files between computers. FTP was created with the aim of transmitting files on digital communication networks by considering the aspects of ease of use, speed and efficiency. However, there is one important factor to consider, namely the security of files sent to and stored on the FTP server. This research applies Salsa20 cryptographic algorithm to secure data sent to and stored on an FTP server by designing a Graphical User Interface (GUI) program, Salsa20 was chosen as it is faster than other algorithms such as AES, Blowfish, ChaCha, and RSA in some cases for encrypting files, and there are no known theoretical and practical attack on 20 round of Salsa.. The study results show that the program design by implementing the Salsa20 algorithm to encrypt files was successfully implemented, the program functionality test successfully ran as expected, the results show the average for the encryption process time 15.0 ms and 14.39 ms, decryption 14.3 ms and 22.4 ms, download 3890.7 ms and 4120.3 ms, upload 4796.6 ms, and 3532.5 ms, sniffing attack testing shows that the Salsa20 cipher successfully secures document files, known plaintext testing to prevent implementation errors, unique nonce generation is carried out on each encryption, The avalanche effect shows a percentage that meets the SAC criteria and thereby Salsa20 can be categorized as a strong cipher.

Keywords*: *Cryptography, Data security, File Transfer Protocol, Simteric-key algorithm, Stream cipher, Salsa20