Abstract

Technological developments in terms of data security on systems have developed very rapidly. There are 2 important aspects, namely security and confidentiality of information data, therefore before sending it must do encryption first. In this case, the application of information data security is not only done with one security technique, but can be done in a combination. This study aims to create a security system that can be used to improve information data security. By implementing lattice-based cryptography, namely NTRU, which will be combined in the AES algorithm. The lattice-based cryptography used in this study is NTRU because NTRU performs an encryption scheme while for other lattice-based uses mix key encaps and signatures. In addition, the NTRU algorithm survives for NIST round 3. The NTRU algorithm is also a symmetric cryptography that can be used to generate random numbers. The combination of these algorithms will be carried out in a file transfer protocol designed to establish a connection between the server and the client, which can then send files from the server to the client. The File Transfer Protocol that has been created will be applied to the TLS version 1.2 protocol because until now in August 2020 there were 98.4% using TLS version 1.2 support where the data source was taken from SSL Pulse. SSL Pulse is a dashboard that monitors the quality of SSL / TLS support. On the other hand, previously there were frequent attacks on the TLS version 1.2 protocol. So this study confirms that the implementation of the NTRU cryptographic algorithm in the TLS 1.2 version protocol can be used to increase security.

Kata kunci: Random Polynomial, NTRU Cryptography, Lattice Based