ABSTRACT

Sending information through socket programming is basically not equipped with adequate security, so it is vulnerable to wiretapping or data theft by irresponsible parties. To overcome this, we need a cryptographic method to guarantee the security of the data to be sent. There are several cryptographic methods including Advanced Encryption System (AES-256), Data Encryption Standard (DES), and International Data Encryption Algorithm (IDEA). The three cryptographic methods are symmetric algorithms which have advantages in terms of efficiency in encryption and message delivery, compared to asymmetric cryptography. However, based on the studies that have been conducted, the performance of the three algorithms is unknown when applied to socket programming. To answer this, in this study an experiment was conducted to implement the three algorithms in socket programming. To find out the performance of each algorithm, an experiment was conducted to send files in Txt, Docx, Pdf, Rar, Jpg, Mp3, and MP4 formats, which were encrypted using the AES-256, DES, and IDEA algorithms. From the test results it was found that the AES-256 algorithm has the best performance in terms of encryption and decryption speed, so the time required is shorter. While the DES algorithm has an advantage in the size of the encrypted file which does not increase in size.

.

Keywords: AES-256, DES, IDEA, Socket Programming