ABSTRACT

With the development of technology, everyone is required to be able to use the internet. One of the good impacts of the development of the internet is that it makes it easier for someone to exchange information and communicate via the internet, the development of the internet also has a negative impact, namely the existence of cybercrime that endangers our personal information. Any data that is private can be seen by unauthorized people. One way to prevent this, by making information that is private cannot be read by unauthorized people with cryptography, cryptography is used to secure information, including maintaining the confidentiality, integrity, and validity of data. Cryptography uses various algorithms such as encryption, hashes, and signatures to achieve information security goals. With encryption, information that was previously easy to read is converted into a collection of incomprehensible writings or called ciphertext. For this reason, an algorithm is needed to encrypt and increase the security of data, the ElGamal algorithm is one of the cryptographic algorithms that can be used to encrypt. The security level of this algorithm is based on the discrete logarithm problem in the group of multiples of integers, modulo, and prime numbers. This research aims to implement the ElGamal algorithm and improve security. The final result of the implementation of the ElGamal algorithm in this study is that the ElGamal algorithm can encrypt messages properly and based on testing the ElGamal computational cost algorithm in terms of memory cost it can be concluded that the use of memory in this message sending application does not require a lot of memory and based on the results of the time cost it is concluded that the time required to perform encryption is small and linear. The results of MITM testing to increase the security of messages sent cannot be read by attackers.

Keywords: *ElGamal, Ciphertext, computation cost, memory cost, time cost, MITM.*