ABSTRACT

Technology has been used in various aspects, both offline and online. The increase of its usage, especially in online storage data with cloud system, makes data security become one of the most important requirements for the user. There are many ways to protect the data, one of them is with data encryption. Encryption is a process to convert data or information into a new form that can be read only by the recipient chosen by the sender. The recipient should have the key to open it, it is called as decryption process. The utilization of the technology in the election process has been carried out in the electronic voting system (e-voting system). But the high risk of security problem makes data encryption applied in the e-voting system. Thus, the ballot won't be interrupted by the insider or the outsider.

In this final project we designed security system of e-voting using Paillier homomorphic encryption algorithm. With homomorphic property, the system can calculate the sum of votes without revealing which vote is voting for which candidate. It can avoid the action of people who intends to cheat on the election process.

Based on the test result the system that has been built shows it can perform encryption and decryption process in a homomorphic way to the data with processing time 3652319 nanoseconds or 0.003651 seconds for encryption and 1499519 nanosecond or 0.001499 seconds for decryption process. The resulting ciphertext values will be different each other even though the same plaintext is encrypted, with a size of 4 times larger than the plaintext size. The success ratio for the system is 100%, with the maximum number of messages that can be processed is 3.287.973.778 messages.

Keywords: Encryption, Paillier, Homomorphic, E-voting, Security