ABSTRACT

Communication between computer system needs an effort to keep the secrecy and data safety. One of the alternatives is to keep data using cryptography. Cryptography is a discipline that studies about how to send a message secretly. With cryptography, simple data (Plaintext) are trransformed into blocks data (ciphertexts) which cannot be comprehended so that they are unable to be read or resolved by third party. Those transformed data (Ciphertexts) can only be seen by the ones who are legitimate to open it with the key, that eventually can change the chipertext into the simple data.

This final project studies and implements cryptographic algorithm in data encryption, using SAFER+ Algorithm. SAFER+ is one of the candidates of Advanced Encryption Standard (AES) which are well preprared to displace Data Encryption Standard (DES)

In this final project, too, there is also an analysis about the strong and weak points of SAFER+ algorithm and also a result comparison with other algorithms (CAST-256 and LOKI97). Hence, we will therefore be able to consider the possibilities of uses met the requirements. Or as alternative of other algorithms. The parameters are time and avalanche effect. Eventually, pertaining to the research outcome, it is found that CAST-256 generally performs better

Keywords :

- Block cipher
- SAFER+
- cryptography.