ABSTRACT

Cryptography is the practice that studies mathematics techniques related to information security aspects i.e. data validation, data integration and data authentication. It also can be defined as the art of protecting information. When a message transferred from a source to another, contain of the message could be seen by other people whom improper to see it. To secure it, the message could be transformed into codes which cannot be translated by any other person.

Noekeon algorithm is the algorithm that uses block-cipher scheme which same keys for each round. In this final project, the scheduling key process is used so that different kind of keys happen in each round is shown.

From the experiments conducted suggest that the modification algorithms performed no better than Noekeon algorithm itself. This is evidenced from the calculation speed of time, the avalanche effect, and the probability of characteristics differential attack shows the modified Noekeon algorithm undervalues the Noekeon algorithm method itself.

Keywords: Cryptography, Noekeon Algorithm, Block-cipher.