ABSTRACT

Issues of security and confidentiality of data is one of important aspects in terms of information exchange. One of the solutions to maintain the security and confidentiality of the data transmission process is the encryption technique. Encryption is the process of transforming data from which can be understood to be unreadable.

GOST is one block cipher encryption algorithm that uses a 32 round Feistel network structure and 256-bit key. With a Feistel structure, the encryption algorithm has the same structure as the decryption. The difference lies only in the sub-key is used. Sub-key generated from the key scheduling process (key-schedule). Key scheduling algorithm in the GOST is very simple, so that in certain circumstances this causes vulnerable to related-key attack.

One approach to preventing that attacks is to maximize the avalanche on the key that is by passing through a strong hash function before the key is expanded to the key scheduling algorithm.

In this final project, the key scheduling was design by adding one-way hash function, HAVAL and SHA-256, to improve security againts related key attack. From the tests performed that has been done, it was concluded that the related key attack is no longer applicable and obtained an increase in the value of the avalanche effect from the modification of algorithm GOST.

***Keywords**: GOST, block cipher, Feistel Network, sub-key, key-schedule, related-key attack.*