

## General Introduction

In today's scenario, people share information to another people frequently using network. Due to this, more amount of information are so much private but some are less private. Therefore, the attackers (or the hackers) take the advantage and start attempting to steal the information since 2001. the symmetric encryption algorithm called 512-bit AES that was designed in 2011 provides high level of security, but it's almost be impossible to be used in multimedia transmissions and mobile systems because of the need for more design area that effect in the use of memory space in each round and the Encryption / Decryption time that it takes.

This work presents an improvement of 512-bit AES algorithm with efficient utilization of resources such as processor and memory space. The proposed approach resists a different encryption analysis and attacks, and provides high security level using a 512-bit size of key block and data block and ameliorates the performance by minimizing the use of memory space and Encryption / Decryption time to be able to work in specific characteristics of resource-limited systems.

The first chapter discuss in detail the technical and applicative aspects of cryptology with its two branches: cryptography and cryptanalysis.

The second chapter is devoted to Mathematical preliminaries required in encryption and decryption methods, and a detailed study of a new variation of the original 128-bit AES algorithm called 512 bit AES that was appeared to provide more security.

The third chapter talks about the proposed algorithm that is given as an alternative to the one that called "512-bit AES" for improving the performance level, explaining its transformations methods including the general architecture and key expansion.

In the fourth chapter, we talk about the environment of the implementation that we have done to make the comparison between algorithms, and the tests that we have done including the results that prove the amelioration of the performance level.

Finally, we conclude the work with a general thought about HLES algorithm as a general conclusion.