

## ABSTRACT

The security of voice communication in the Internet network is not yet guaranteed. Though, the use of voice communication has been widely used. This Final Project will discuss the solutions of voice mail security using encryption. Encryption means perform encoding voice messages for unauthorized parties can not understand it.

The encryption algorithm used on this final project is Cipher block Mars Algorithm. Cipher block algorithm will cause greater delay than the stream cipher algorithm. Therefore, the implementation of Mars algorithm should be adjusted so that the delay that appears is small. In this final project, the changes are done by using the counter operation mode that able to change the efficiency of a block cipher becomes similar to stream cipher.

Analysis of a security subsystem is done based on several parameters, namely time processing, comparison of input and output files, avalanche effect, brute force attack, variance, comparison with other algorithms and MOS.

From the test results can be concluded the system can be realized by generating a time delay between blocks is 0.2667 ms, the ratio of input and output files the same. Value avalanche effect by changing 1 bit key reaches 51.25%, while based on 1 bit plaintext change the amount of 0781%. Time to make Bruce force attack is  $2:28 \times 10^{25}$  years and for quite excellent MOS rating for data encryption and decryption fine for data results.

**Keywords: Encryption, Block Cipher, Mars, time processing, file input and output, avalanche effect, brute force attack, MOS**