ANALISA DAN IMPLEMENTASI ENKRIPSI-DEKRIPSI SUARA MENGGUNAKAN ALGORITMA RIJNDAEL

Iskan Susanto[1], Iwan Iwut Tritoasmoro[2], Tjokorda Agung Budi Wirayuda[3]

[1]Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

Abstrak

Keamanan komunikasi suara dalam jaringan internet belum terjamin. Padahal penggunaan komunikasi suara telah banyak digunakan. Tugas Akhir ini akan membahas tentang solusi pengamanan pesan suara dengan menggunakan enkripsi. Enkripsi berarti melakukan pengkodean pesan suara agar pihak yang tidak berhak tidak dapat memahaminya.

Algoritma enkripsi yang digunakan pada Tugas Akhir ini adalah algoritma enkripsi cipher blok Rijndael. Algoritma cipher blok akan menimbulkan delay yang lebih besar daripada algoritma cipher aliran. Oleh karena itu, penerapan algoritma Rijndael harus disesuaikan agar delay yang ditimbulkan kecil. Pada makalah ini, perubahan tersebut dilakukan dengan menggunakan mode operasi counter yang dikatakan dapat merubah efisiensi cipher blok menjadi menyerupai cipher aliran.

Analisa subsistem security dilakukan berdasarkan beberapa parameter yaitu time processing, perbandingan file input dan output, avallanche effect, brute force attack, dan MOS.

Dari hasil pengujian dapat disimpulkan sistem dapat direalisasikan dengan menghasilkan waktu delay antar blok adalah 1,046 ms, perbandingan file input dan output sama. Nilai avalanche effect berdasarkan perubahan 1 bit kunci mencapai 48,74 % sedangkan berdasarkan perubahan 1 bit plainteks besarnya 0,781 %. Waktu untuk melakukan bruce force attack adalah 1,823 x 1025 tahun dan untuk penilaian MOS tergolong fine

Kata Kunci : Enkripsi, Cipher Block, Rijndael, file input dan output, avallanche effect, brute force attack, MOS

Abstract

Security of voice communication in the Internet network is not yet guaranteed. While the use of voice communication has been widely used. The final project will discusses security solutions with a voice message using encryption. Encryption means to a voice message that the party has no right can not understand it.

Encryption algorithm used on the final project is a block cipher encryption algorithm Rijndael. Block cipher algorithm will cause a delay of more than the stream cipher algorithm. Therefore, the implementation of Rijndael algorithm should be adjusted so that the small delay incurred. The final project, the changes are done by using the counter mode operation can alter the efficiency of a block cipher-like stream cipher.

Analysis of a security subsystem based on several parameters, namely time processing, comparison of input and output files, avallanche effect, brute force attack, and MOS.

From the results of the test can be realized with the system can generate the time delay between the blocks is 1.046 ms, the difference in input and output files the same. Value based on the avalanche effect changes 1 bit key reaches 48.74%, while the changes based on 1 bit plainteks amount of 0.781%. Time to make a bruce force attack is 1,823 x 1025 years for the assessment and fine classified MOS

Keywords : Encryption, Cipher Block, Rijndael, file input and output, avallanche effect, brute force attack, MOS