KOMPRESI PADA KRIPTOGRAFI FILE SUARA MENGGUNAKAN ALGORITMA MERKLE HELLMAN KNAPSACK DAN HUFFMAN

ABDUL HAFIZ HADRI

11251103254

Jurusan Teknik Informatika

Fakultas Sains dan Teknologi

Universitas Islam Negeri Sultan Syarif Kasim Riau

ABSTRAK

Pertukaran informasi melalui jaringan publik merupakan hal lumrah yang dilakukan saat ini, namun hal ini juga berarti bahwa setiap orang dapat mengakses informasi tersebut. Informasi-informasi yang bersifat rahasia harus dijaga kerahasiaannya agar informasi tersebut tidak jatuh ke pihak yang salah. Teknik kriptografi dapat digunakan untuk memenuhi aspek kerahasiaan informasi yang dikirim, yaitu informasi yang dikirim hanya dapat dibaca oleh pihak yang memiliki hak untuk mengetahui isi informasi tersebut. Algoritma Kriptografi yang digunakan adalah algoritma *Merkle Hellaman Knapsack* yang merupakan algoritma kriptografi asimetris yang menggunakan dua kunci berbeda untuk enkripsi dan dekripsi. Berdasarkan penelitian terdahulu algoritma ini menghasilkan *chipertext* yang besar, pada penelitian ini informasi rahasia berbentuk pesan suara akan diamankan dengan kriptografi dan tentunya menghasilkan data yang besar. Algoritma kompresi data *Huffman* merupakan algoritma umum yang digunakan untuk memperkecil ukuran data. Sitem yang dibagun dengan GUI Matlab merupakan sitem yang digunakan untuk memenuhi proses kriptografi suara dan proses kopresi pada *chipertext.* Berdasarkan hasil pengujian banyaknya data file suara dalam melakukan proses dekripsi membuat waktu yang dibutuhkan sangat lama. Hal ini menujukkan bahwa algoritma *Merkle Hellaman Knapsack* tidak cocok dugunakan untuk mengamankan data dalam jumlah yang banyak.

Kata Kunci : *Huffman*, Keamanan, Kompresi, Kriptografi, Matlab, *Merkle Hellman Knapsack*, Suara.

COMPRESSION ON SOUND FILE CRYPTOGRAPHY USES MERKLE HELLMAN KNAPSACK AND HUFFMAN ALGORITHMS

ABDUL HAFIZ HADRI

11251103254

Informatics Engineering

Faculty of Science and Technology

State Islamic University of Sultan Syarif Kasim Riau

ABSTRACT

Exchange of information trough public networks is a common practice nowdays, but this also means that everyone can access that information. Confidential informatioan must be kept confidential so that the information does not fall to unauthorized parties. Cryptographic techniques can be used to fulfill aspects of confidentiality of information where the information sent can only be read by the recipient that is appropriate for that information. The Cryptographic Algorithm used is the Merkle Hellaman Knapsack algorithm, which is an asymmetric cryptographic algorithm that uses two different keys for encryption and decryption. Based on previous research, the algorithm produced a large size of ciphertext. In this study, confidential information in the form of voicemail will be secured by cryptography and of course produce large data. The Huffman data compression algorithm is a common algorithm used to reduce the size of data. The system is built with the Matlab GUI, this system is used to fulfill sound cryptographic and compression processes in ciphertext. Based on the results of sound files testting in the decryption process, the time needed is very long because of the large amount of data. This shows that the Merkle Hellaman Knapsack algorithm is not suitable to use in securing large amounts of data.

Keyword : *Compression, Cryptography, Huffman, Matlab, Merkle Hellman Knapsack, Secure, Sound.*