

## **KOMPRESI MENGGUNAKAN ALGORITMA HUFFMAN UNTUK OPTIMASI FILE TEKS PADA PROSES ENKRIPSI ALGORITMA AES**

**MUHAMMAD NOFIYANTO**

(Pembimbing : Aisyatul Karima, S.Kom, MCS)

*Teknik Informatika - S1, FIK, Universitas Dian Nuswantoro*

*www.dinus.ac.id*

*Email : 111201206946@mhs.dinus.ac.id*

### **ABSTRAK**

Dengan semakin berkembangnya teknologi membuat pertumbuhan data terutama file berbasis teks semakin besar serta kebutuhan keamanan yang handal guna mencegah hilangnya informasi. Perlu cara dalam pengamanan data dan memperkecil ukuran data untuk efisiensi ukuran data dapat dilakukan dengan menerapkan kompresi dan dari segi keamanan dengan kriptografi. Algoritma kompresi Huffman dapat memperkecil ukuran file teks, algoritma AES (Advanced Encryption Standard) untuk pengamanan karena teruji dalam menahan serangan kriptanalisis. Implementasinya program melakukan kompresi pada file teks (.txt, .doc) kemudian diubah menjadi file terkompresi (.hsf) dan dilakukan proses enkripsi (.enc). Agar dapat digunakan kembali dilakukan proses dekripsi pada file (.enc.dec) dan file tersebut didekompresi menghasilkan file teks semula. Tahap pengujian dilakukan dalam 3 cara yaitu rasio kompresi, pengujian recovery, dan pengujian Brute Force. Dari ketiga tahap pengujian didapatkan hasil rasio kompresi terbaik mencapai 47,27% artinya ukuran file lebih kecil dari ukuran asli dan terburuk 2688% artinya file lebih besar dari file asli. Pada pengujian recovery seluruh isi dapat dikembalikan seperti semula. Pada tahap brute force dalam durasi terpendek 2 jam lebih hingga telama 1 hari lebih belum dapat membobol file hasil kompresi dan enkripsi.

Kata Kunci : Kompresi, Algoritma Huffman, Kriptografi, Advanced Encryption Standard

## **COMPRESSION USING HUFFMAN ALGORITHM TO OPTIMIZE TEXT FILE IN AES ALGORITHM ENCRYPTION PROCESS**

**MUHAMMAD NOFIYANTO**

(Lecturer : Aisyatul Karima, S.Kom, MCS)

*Bachelor of Informatics Engineering - S1, Faculty of Computer  
Science, DINUS University*

*www.dinus.ac.id*

*Email : 111201206946@mhs.dinus.ac.id*

### **ABSTRACT**

With the rapid development of technology make data especially text-based file grow a much bigger following with security need much stronger to prevent information loss. So need a method in order to secure data and the other to reduce size data can be handled by implementing compression and cryptography. Huffman algorithm can reduce size from a text file, meanwhile, AES (Advanced Encryption Standard) algorithm use to secure text file because this already tested hold any cryptanalysis attack. In implementation compressing text file (.txt, .doc) then become compressed file (.hsf) and then encrypted (.enc). To can be used again file need through decryption process (.enc.dec) then must be decompressed to become original text file. Attesting step there is 3 testing method from ratio compression, recovery testing, and brute force attack. From all these testing step result from the best ratio compression could get is 47.27% mean file have smaller size rather than original and the worst is 2688% mean file bigger than original. Meanwhile, recovery test all character could be retrieved again. At attacking phase brute force from shortest time is 2 hours more to the longest is 1 day more still cannot extract any information from processed file.

**Keyword** : Compression, Huffman Algorithm, Cryptography, Advanced Encryption Standard