Implementasi Keamanan File dengan Kompresi *Huffman* dan Kriptografi *Advanced Encryption Standart* (AES) pada Pengamanan File Data Antemortem

Rizky Satria Wibowo, Jayanta, Catur Nugrahaeni

Jurusan Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta[1]
Jurusan Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta[2]
Jurusan Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta[3]
Jl. RS. Fatmawati Raya, Pd. Labu, Kec. Cilandak, Kota Depok, Daerah Khusus Ibu Kota Jakarta 12450
E-mail: rizkysw@upnvj.ac.id[1], jayanta@upnvj.ac.id[2], catur.nugrahaeni@upnvj.ac.id[3]

Abstrak

Kombinasi keamanan file dengan kompresi dan kriptografi dibuat untuk memfasiltasi keamanan serta cakupan kapasitas ruang penyimpanan yang besar serta waktu yang cukup besar untuk prosesnya seperti halnya file data antemortem. Kriptografi dan kompresi ini dibuat menggunakan metode *Huffman* untuk kompresi dan *Advanced Encryption Standart (AES)* untuk metode kriptografi sendiri. Proses untuk mendapatkan hasil yang diinginkan, digunakan metode-metode pendukung untuk pemrosesan hasil output dari kombinasi antara kompresi *Huffman* dan Kriptografi *AES.* Percobaan atas kriptografi dan juga kompresi dilaksanakan atas tiga tahapan dimana percobaan tersebut adalah percobaan atas pengamanan, perubahan serta keutuhan file antemortem. Hasil penelitian ini menunjukan bahwa file data antemortem tidak mengalami perubahan atas proses penguncian, hal ini ditunjukan atas percobaan checksum untuk berkas berbasis teks serta *histogram RGB* untuk berkas berbasis citra. Dalam aspek keamanan serta keutuhan diperoleh tingkat keamanan yang baik serta keutuhan atas berkas yang telah dilakukan proses penguncian dengan menggunakan metode AES.

Kata Kunci: AES, Huffman, Kriptografi, Kompresi

I. PENDAHULUAN

Teknologi informasi sekarang ini terus tumbuh semakin pesat, gaya perubahan data serta informasi dapat dilaksanakan dengan cara mudah melalui berbagai macam media yang ada. Keamanan dan penyimpanan menjadi elemen yang sangat penting bagi pemakai teknologi informasi, hal ini tidak lepas bagaimana proses pertukaran data itu dilakukan, dengan semakin banyaknya orang memanfaatkan layanan komunikasi pertukaran data, tentu masalah pun bermunculan, di antaranya adalah kebutuhan akan media penyimpanan yang semakin besar, keamanan pada data rahasia yang tidak boleh didapatkan serta jatuh ke orang lain, kecepatan proses akan pertukaran data, dan permasalahan lainnya. Dari hal tersebut, maka diciptakan sebuah keamanan bagi seluruh elemen-elemennya, terutama informasi-informasi dan aset-aset penting demi mengamankan kerahasian informasi data tersebut. Keamanan serta penyimpanan menjadi fokus serta point penting yang dibangun serta dikembangkan guna menjamin keutuhan data serta kecepatan dalam informasi.

Program pengaman data untuk menghindari penyalahgunaan dan pengubahan data, serta pemampatan sebagai upaya untuk pengefisiensian data. Kemanan ini menggunakan algoritma simetrik *Advanced Encrytption Standart* (AES) sebagai algoritma pengamanan data, algortima *AES* memiliki kunci dengan kombinasi yang serupa dengan

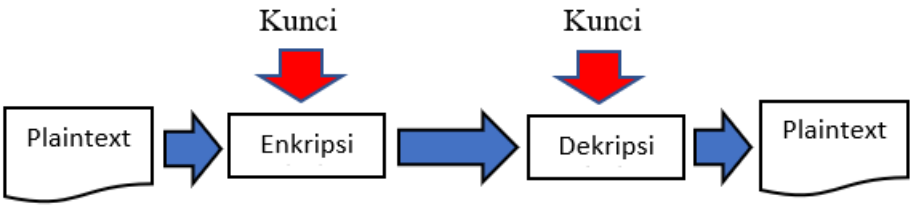
 ISSN : 2086-8251

kunci enkripsi dengan pilihan kunci 128 bit, 192 bit, atau 256 bit . AES Memiliki sifat tidak mengubah sama sekali bentuk dari berkas awal dan akhir dan tentu sangat aman dan lebih cepat hal ini didasari atas kemenanga AES pada NIST. Algortima kemanan data ini lalu dikombinasikan dengan algoritma pemampatan data kompresi *Huffman* guna memperkecil ukuran serta mempercepat pengiriman data penggunaan algoritma ini didasari atas sifat utama dari Huffman yaitu *Losless* atau tidak mengubah sama sekali data yang ada yang sebelumnya ada dan tetap dalam bentuk semula. Dua teknik ini dikombinasikan guna mendapatkan hasil secara maksimal secara efisien maupun keamanan dari data *output* yang kita lindungi yaitu file data antemortem.

II. METODOLOGI PENELITIAN

a. Kriptografi

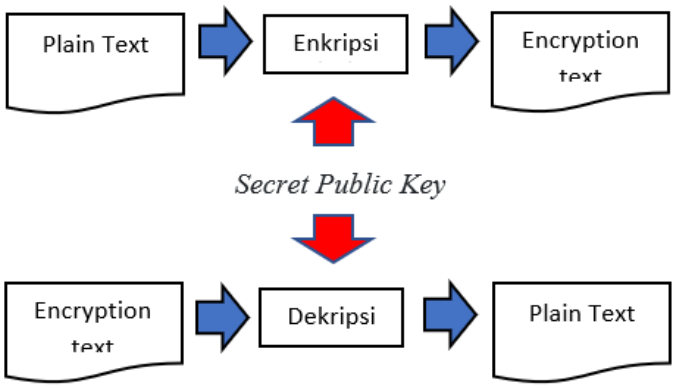
Asal kata kriptografi terdiri atas dua kata didalam bahasa Yunani, yaitu di mana *cryptos* dan *graphen*. *Cryptos* dalam artinya adalah rahasia sedangkan *graphen* dalam artinya disini merupakan sebuah goresan atau tulisan sehingga secara harfiah kriptografi sendiri merupakan tulisan yang dirahasiakan. Menurut istilahnya, kriptografi adalah ilmu yang mempelajari teknik-teknik dimana teknik tersebut berhubungan dengan berbagai aspek keamanan informasi seperti kerahasian, integritas data, serta otentifikasi. Kriptografi pada awalnya dijabarkan sebagai bagaian dari penyembunyian pesan rahasia. Namun saat ini kriptografi tidak hanya untuk menjaga *privacy* atau *confidentiality*, tetapi juga untuk tujuan data *integrity*, *authentication*, dan *non-repudation*.



Gambar 1. Sistem Kriptografi

b. *Advanced Encryption Standart (*AES)

Algoritma Rijndael atau yang lebih dikenal dengan dengan *Advanced Encryption Standart* (AES) beroprasi pada medan *Galois* (2^8), dalam hak ini artinya semua oprasi aritmatika dilakukan pada penggunaan byte berukuran 8 bit didalam matriks. Algoritma AES mendukung panjang kunci 128 bit sampai 256 bit dengan step 32 bit. Algoritma AES merupakan algoritma simetris. Algortima simetris ini merupakan algoritma yang hanya mempunyai satu buah kunci saja yang digunakan untuk kunci publik dan kunci private sehingga algoritma AES masuk kedalam jenis algoritma simetris.



Gambar 2. Sistem Kriptografi AES

c. Kompresi

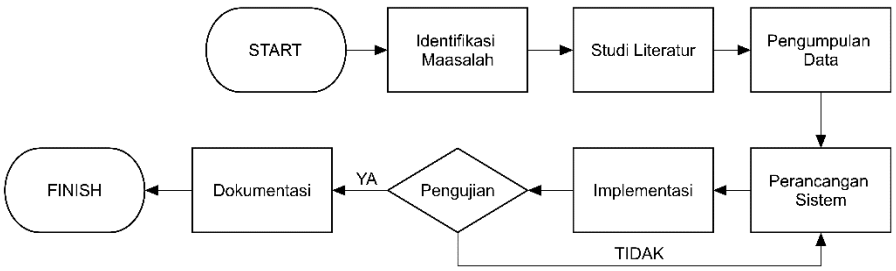
Kompresi data adalah seni atau ilmu untuk merepresentasikan informasi dalam bentuk yang kompak serta dinamis namun tetap effisien. Dalam hal ini diciptakan sebuah representasi kompak dengan mengidentifikasi dan menggunakan struktur yang ada dalam data. Data bisa berupa karakter dalam file teks, angka yang merupakan contoh bentuk gelombang ucapan atau gambar, atau urutan angka yang dihasilkan oleh proses lain.

d. Huffman

Pengkodean *Huffman* adalah metode yang cukup populer untuk teknik kompresi data. Algoritma ini dimulai dengan membuat daftar semua simbol alphabet yang ada secara turun urutan probabilitas mereka dari yang terkecil hingga terbesar. Selanjutnya algoritma ini kemudian membuat pohon biner, dengan atribut di setiap daun, dari bagian bawah ke atas. Ini semua dilaksanakan secara bertahap, di mana pada setiap step terdapat dua simbol dengan yang terkecil probabilitas dipilih, di inputkan ke bagian atas pohon parsial, didelete dari daftar, dan diganti dengan simbol bantu yang mewakili dua simbol asli. Ketika simbol di reduksi menjadi hanya satu simbol bantu (mewakili semua alfabet), pohonnya lengkap. Pohon tersebut selanjutnya dilintasi untuk menetapkan kode-kode simbol yang mengambil dari node atas atau node akar. Dengan kata lain algortima kompresi ini menukar kode dengan yang kecil didalam karakter yang sering diguanakan dan yang lebih besar pada yang jarang digunakan.

e. Flowchart Metode Penelitian

Pada metodologi penelitian ini, tahapan penelitian disajikan dalam bentuk *flowchart* dibawah ini:



Gambar 3. *Flowchart* metodologi penelitian

Uraian proses tahapan penelitian pada gambar 2 adalah sebagai berikut:

a. Identifikasi Masalah, pada tahapan ini penulis mengamati permasalahan yang ada didalam bidang keamanan data, khususnya mengenai pengamanan data antemortem serta pengimplementasiannya nantinya.

b. Studi Literatur, pada tahap studi literatur dilakukan untuk mengumpulkan dan mencari informasi terkait literatur penelitian yang berkaitan tentang kriptografi, kompresi data, pengamanan data antemortem, serta penelitian yang berkaitan tentang algortima *AES* dan kompresi *Huffman*.

c. Pengumpulan Data, tahapan ini merupakan sebuah tahapan selanjutnya setelah tahapan studi literatur selesai. Pada tahapan ini merupakan proses pengumpulan data. Pada penelitian ini data yang dikumpulkan merupakan data antemortem yang terdiri dari data umum, data medis serta data tambahan.

d. Perancangan Sistem, tahap ini akan dilakukan perancangan sistem agar memiliki gambaran bagaimana nantinya sistem akan bekerja dengan berbagai macam permodelan.

e. Pengujian, dalam tahapan selanjutnya yaitu tahapan pengujian sistem, di mana pada tahapan ini dilakukan proses pengujian terhadap aplikasi yang telah dibuat sebelumnya didalam proses implementasi.

f. Implementasi, tahapan implementasi ini dilakukan penerjemahan dari perancangan yang telah dibuat dalam *flowchart* serta desain lain kedalam bahasa pemrograman yang digunakan untuk melakukan pengamanan serta pemampatan pada data antemortem.

g. Dokumentasi, selanjutnya pada tahapan akhir ini dilakukan penarikan kesimpulan akhir serta dokumentasi yang diperoleh setelah melakukan pengujian terhadap sistem yang telah dibuat dengan kompresi *Huffman* dan kriptografi *Advanced Encryption Standart* (AES) pada pengamanan file data antemortem.

III. HASIL DAN PEMBAHASAN

a. Pengumpulan Data

Sampel data yang digunakan pada proses penelitian kali ini bersumber dari rumah sakit serta beberapa bersumber dari internet. Instansi tersebut memberikan beberapa sampel terkait dengan data antemortem serta juga contoh formulir yang digunakan langsung dalam proses identifikasi terkait antemortem. Informasi yang terkandung didalam beberapa objek dari sampel diproses untuk dilakukan proses pengamanan dan reduksi ukuran.

Table 1. Data antemortem

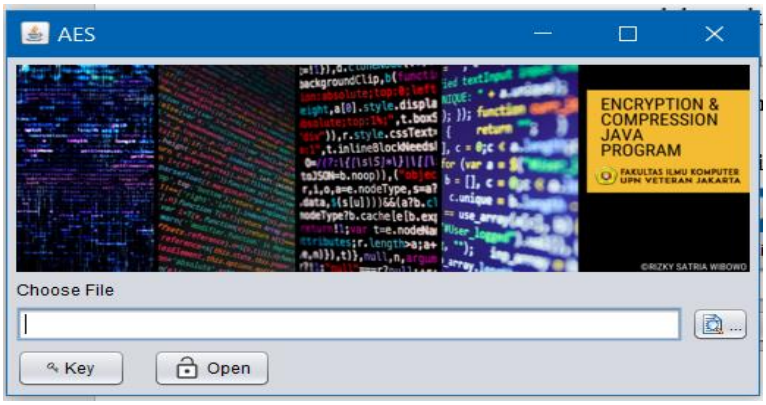
NO	Objek Antemortem
1	Rontgen Dental
2	Dental Picture
3	Sidik Jari
4	Rontgen Cacat Medis

Tabel 1 diatas adalah data sebagian yang digunakan untuk data antemortem yang dipakai dalam proses pengidentifikasian korban suatu bencana atau insiden, yang nantinya akan dilakukan proses pengamanan dan pereduksian ukuran.

b. Perancangan Aplikasi

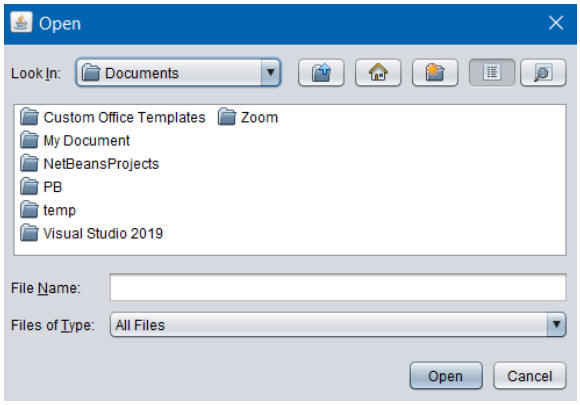
Aplikasi ini dibuat berdasarkan dari rancangan yang sudah disiapkan seperti rancangan *database,* rancangan UML agar aplikasi berjalan sesuai dengan yang diinginkan dan mampu memudahkan *user* menggunakannya. Berikut hasil dari rancangan tersebut.

 ISSN : 2086-8251



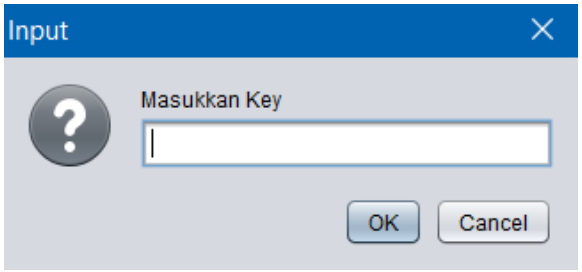
Gambar 4. Menu penguncian & pembukaan

Menu diatas merupakan merupakan menu penguncian & pembukaan yang digunakan untuk proses enkripsi dan kompresi menggunakan algoritma *Advanced Encryption Standart* (AES) & Kompresi *Huffman*.



Gambar 5. Open direktori

Proses pengambilan berkas untuk bisa masuk kedalam proses penguncian.



Gambar 6. Penginputan kunci

Menu penginputan key untuk mengunci berkas atau membuka berkas yang sudah dilakukan proses penguncian sebelumnya.

c. Pengujian Aplikasi

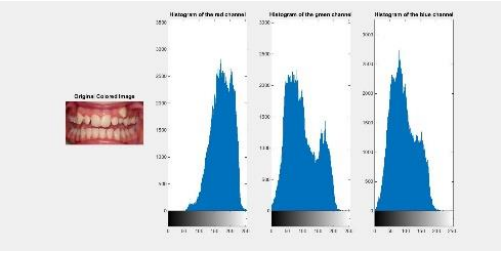
Pengujian aplikasi dilakukan untuk melihat sejauh mana penguncian ini berhasil. Apakah terdapat perubahan dari berkas sesudah dan sebelum proses penguncian atau tidak dan apakah berkas akan aman jika jatuh ketangan orang yang bertanggung jawab.

Table 2. Checksum PDF

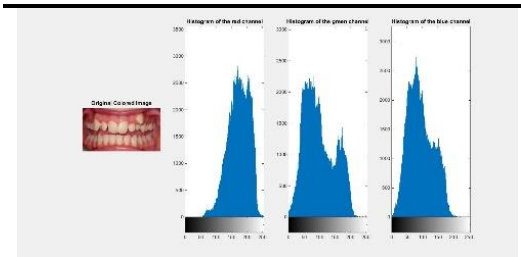
No	Nama Berkas	Keterangan	Nilai Checksum	Keterangan
1	Pasien A.pdf	Berkas Awal	FCAEDA4444F7BE89CF3FE1EB2D31C334	-
		Penguncian	F7051A9C0DCD8708D75653EE2502EAA1	Berbeda
		Pembukaan	FCAEDA4444F7BE89CF3FE1EB2D31C334	Sama
2	Pasien B.pdf	Berkas Awal	360DC4F332605FCF9D03AA8E909FF516	-
		Penguncian	0E1B6F55806488881F947C2272F2649E	Berbeda
		Pembukaan	360DC4F332605FCF9D03AA8E909FF516	Sama
3	Pasien C.pdf	Berkas Awal	DBB0EE300FE13F4AF76382941C1225D1	-
		Penguncian	63B1E7FB2ED657F1EFED75E53731E665	Berbeda
		Pembukaan	DBB0EE300FE13F4AF76382941C1225D1	Sama
4	Pasien D.pdf	Berkas Awal	93422094744A1E13F316F82E7DD279EF	-
		Penguncian	65DC5E859EE2BF11697EB82EC6FCF429	Berbeda
		Pembukaan	93422094744A1E13F316F82E7DD279EF	Sama
5	Pasien E.pdf	Berkas Awal	D19C37C36BC566488D68B818DBCAA53C	-
		Penguncian	C3F23618757603A82E0B982228073D20	Berbeda
		Pembukaan	D19C37C36BC566488D68B818DBCAA53C	Sama
6	Pasien F.pdf	Berkas Awal	ABB4582E3AB55E4692141F89CF4D00FD	-
		Penguncian	E9966F3CE4B01F25B473C6D399C9F275	Berbeda
		Pembukaan	ABB4582E3AB55E4692141F89CF4D00FD	Sama
7	Pasien G.pdf	Berkas Awal	FEEAA89BFF1BC563C989163F603EAEE1	-
		Penguncian	7677DEDD706A98C74241FB58CB382709	Berbeda
		Pembukaan	FEEAA89BFF1BC563C989163F603EAEE1	Sama
8	Pasien H.pdf	Berkas Awal	99AD1A8678BB2253974FA170AD9A7DFD	-
		Penguncian	97BF1E7878C9B3E293A15214C9F91D13	Berbeda
		Pembukaan	99AD1A8678BB2253974FA170AD9A7DFD	Sama
9	Pasien I.pdf	Berkas Awal	0D4F6D35C7A4F3576E48F3FD7AB5B453	-
		Penguncian	2B603B19FB8CA09E8F819B79E3FDDCC8	Berbeda
		Pembukaan	0D4F6D35C7A4F3576E48F3FD7AB5B453	Sama
10	Pasien J.pdf	Berkas Awal	5666B4EA158412488B3E34056115C849	-
		Penguncian	9467C1800205B40E36F0A9D32A6E052E	Berbeda
		Pembukaan	5666B4EA158412488B3E34056115C849	Sama

Tabel. 2 diatas adalah hasil pengujian atas proses penguncian. Di mana pada uji coba checksum ini untuk melihat apakah ada perubahan terkait struktur berkas sebelum dan setelah penguncian.

Table 3. RGB histogram citra

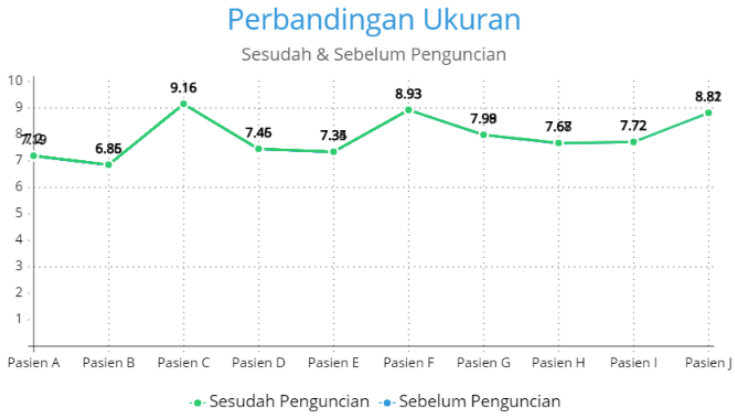
	Histogram Citra	Ukuran Citra
Citra Asli		
		373X673
Citra Hasil Pembukaan		

 ISSN : 2086-8251

	373X673

Tabel 3 adalah tabel percobaan pengecekan terhadap *histogram RGB* yang dihasilkan dari citra asli sebelum penguncian dan citra setelah dilakukan pembukaan. Pengecekan ini dilakukan untuk melihat apakah terdapat perubahan akan struktur dari citra sebelum dan setelah dilakukan proses penguncian.

Analisis ukuran data dilakukan proses penganalisaan atas penguncian kunci data pada algortima yang digunakan. Analisis pengujian ini untuk melihat sejauh mana pertambahan data sesudah dan sebelum dilakukan proses penguncian data.

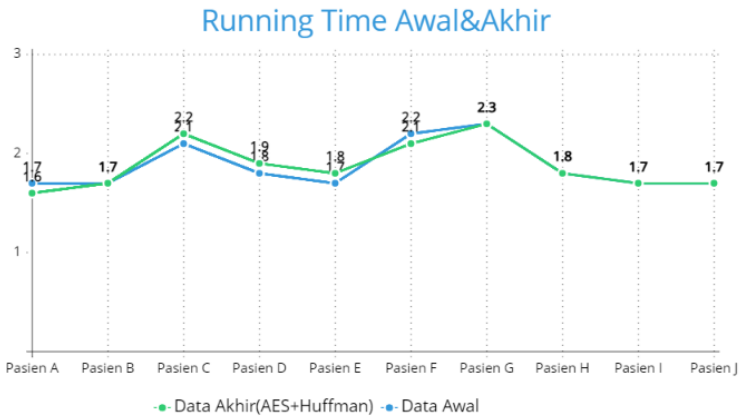


Gambar *7*. Grafik perbandingan ukuran sebelum & sesudah penguncian

Gambar. 7 dari grafik yang digambarkan data cenderung sedikit mengalami perubahan dari segi ukuran sebelum dan sesudah penguncian. Pertambahan ukuran ini disebabkan atas penambahan kunci terhadap proses pengunican *AES.*

Pengujian ini melihat bagaimana waktu perbandingan antara berkas awal dengan berkas yang sudah dilakukan proses penguncian. Dilihat pada hasil diperoleh bahwa range waktu yang dihasilkan tidak terlalu memiliki perbedaan yang terlampau jauh, mengingat ukuran yang dihasilkan tidak terlalu besar.

 ISSN : 2086-8251



Gambar 8. Grafik running time awal & akhir

Gambar 8. Dari grafik yang ditampilkan bisa dilihat bahwa kecenderungan data awal dan data akhir yang telah dilakukan proses *AES* dan *Huffman* memiliki hasil waktu yang tidak jauh berbeda. Hal ini didasari atas ukuran data antara data awal serta data akhir yang telah dilakukan *AES* dan *Huffman* memiliki kesamaan ukuran sehingga waktu yang dicetak juga memiliki kecenderungan.

IV. KESIMPULAN

Berdasarkan hasil dari pembahasan implementasi keamanan file dengan kompresi *Huffman* dan kriptografi *Advanced Encryption Standart* (AES) pada pengamanan file data antemortem, dapat disimpulkan sebagai berikut:

1. Algoritma *Advanced Encryption Standart* (AES) yang dikombinasikan dengan teknik kompresi *Huffman* dapat dipergunakan dalam pengamanan berkas.
2. Kombinasi algoritma *AES* dengan teknik kompresi Huffman dapat digunakan untuk melakukan pengamanan pada berkas tanpa merusak atau merubah berkas yang ada.
3. Hasil running time terhadap percobaan pengiriman data menggunakan kombinasi antara algoritma kriptografi *AES* dan kompresi *Huffman* menunjukan hasil dimana semakin kecil ukuran data semakin cepat juga prosesnya, begitu pula dengan sebaliknya.
4. Kombinasi algoritma *AES* dengan teknik kompresi *Huffman* dapat digunakan untuk melakukan pengamanan pada berkas tanpa merusak atau merubah berkas yang ada.

Refrensi

[1] Ariyus, Doni, *Pengantar ilmu Kriptografi Teori Analisis dan Implementasi*, Yogyakarta, C.V Andi Offset, 2008.

[2] Kemenkes, *Pedoman Teknis Penanggulangan Krisis Kesehatan Akibat Bencana,* Jakarta, Kemenkes RI.

[3] Kromodimoeljo, Sentot, *Teori dan aplikasi Kriptografi*, SPK IT Consulting, 2010

[4] Munir, Rinaldi, *KRIPTOGRAFI*. Bandung, Informatika, 2019.

[5] Sadikin, Rifky, *Kriptografi Untuk Keamanan Jaringan*, Yogyakarta, C.V Andi offset, 2012.

[6] Salomon, David, *Data Compression*, Fourth Edition, London Springer-Verlag, 2007

[7] Sayood, Khalid, *Introduction to Data Compresion*, Fifth Edition, Morgan Kuffman., 2018.

[8] Stinson, 2002, Cryptography: Theory and Practice.Chapman & Hall/CRC.

[9] Waharto, Yudi, Ari Irawan, '*Enkripsi Menggunakan Advanced Encryption*

Standart 256'.Jurnal Kilat, Vol.7,No.2,hh 91-99, 2018.

[10] Yudianto, Ahmad, Pemerikasaan Forensik DNA Tulang dan Gigi : Identifikasi pada DNA Lokus STR CODIS,Y-STRs, dan mtDNA,Sintesa Book, 2020.

[11] Zam, Efvy, *Buku Sakti Hacker*, Jakarta, Mediakita, 2011.