PENGAMANAN FILE MENGGUNAKAN KRIPTOGRAFI DENGAN METODE AES-128 BERBASIS WEB DI KOMITE NASIONAL KESELAMATAN TRANSPORTASI

Dian Widyawan[1)], **Imelda**[2)]
[1]Program studi, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : dianwidyawan@gmail.com [1)], imelda@budiluhur.ac.id [2)]

Abstrak

Pesatnya perkembangan teknologi informasi dan telekomunikasi yang memudahkan manusia untuk melakukan aktifitas dalam bentuk file ataupun data yang bersifat rahasia, oleh karena itu dibutuhkan pengamanan data untuk mengamankan file yang bersifat rahasia. Data adalah catatan atas kumpulan fakta atau suatu variable yang berbentuk berupa kata- kata, citra dan angka. Namun, terkadang data yang bersifat private sering terjadinya kebocoran dan kehilangan data. Penggunaan komputer menjadi suatu kebutuhan yang tidak dapat dipisahkan lagi untuk disetiap kegiatan, tidak terkecuali dalam Komite Nasional Keselamatan Transportasi bekerja dibidang investigasi. Demi kelancaran dalam melakukan investigasi untuk itu dibutuhkan suatu aplikasi yang dapat menjaga kerahasiaan data tersebut. Penelitian ini bertujuan untuk menghasilkan aplikasi untuk membantu dalam proses pengamanan data. Teknik kriptografi yang di gunakan adalah metode Advanced Encryption Standard (AES) Aplikasi ini rancang dengan salahsatu dari macam – macam metode, yaitu metode Waterfall, pada tahap perancangan aplikasi keamanan file menggunakan bahasa pemograman php berbasis web dengan menggunakan database MySQL. Metode Advanced Encryption Standard (AES) merupakan standar enkripsi dengan kunci-simetris dengan ukuran kunci yang beragam seperti 128 bit, 192 bit, dan 256 bit. Dari hasil implementasi diperoleh kesimpulan bahwa aplikasi mampu mengamankan file investigasi dari yang semula berbentuk plaintext menjadi chipertext dengan hasil akhir file yang tidak dapat dimengerti lagi maknanya.

Kata kunci: Kriptografi, *Advanced Encryption Standard*, *File*

1. PENDAHULUAN

1.1 Latar Belakang

Pesatnya perkembangan teknologi informasi dan telekomunikasi yang memudahkan manusia untuk melakukan aktifitas bertukar informasi dalam bentuk *file* ataupun data yang bersifat rahasia. Oleh karena itu dibutuhkan pengamanan data untuk mengamankan *file* yang bersifat rahasia. Salah satu ilmu sekaligus seni untuk pengamanan data berupa *file* yang terkenal adalah kriptografi.

Komite Nasional Keselamatan Transportasi (KNKT) adalah sebuah lembaga non struktural Indonesia untuk melakukan investigasi sebuah kecelakaan, penelitian kecelakaan dan membuat laporan hasil investigasi dalam rangka mencegah terjadinya kecelakaan transportasi dengan penyebab yang sama. Pada saat ini pengamanan *file* investigasi dilakukan secara manual, yaitu menyimpan *file* investigasi kedalam arsip tempat penyimpanan, hal itu bisa membuat *file* investigasi kondisinya sering terjadi kehilangan atau bocornya *file* penting karena kemudahan untuk mengakses *file* tersebut. Keamanan dan kerahasiaan data adalah salah satu aspek yang sangat penting dalam dunia teknologi pada saat ini. Disebabkan munculkan ilmu pengetahuan yang memungkinkan Teknik – teknik untuk melakukan kejahatan pada informasi, sehingga dapat merugikan pemiliki informasi.

Karena itu muncul suatu idea yang tertuju dari permasalahan yang ada, yaitu untuk memrancang sistem keamanan yang dapat digunakan untuk melindungi data berupa *file* dengan teknik kriptografi. Salah satu metode yang dapat digunakan untuk mengimplementasikan Teknik kriptografi adalah metode *AES-128 bit*.

Penelitian terdahulu telah membahas enkripsi kriptografi dengan metode AES-128 berbasis desktop dari "Agustan Latif" [3] dengan judul "Implementasi Kriptografi menggunakan metode *Advanced Encryption Standard* (AES) yang bertujuan untuk Pengamanan Data teks" pada penelitian ini kontribusinya mengamankan *file* berbasis *web* menggunakan metode AES-128 bit di Komite Nasional Keselamatan Transportasi. Sehingga muncul untuk membuat aplikasi untuk mengamankan *file* dengan metode AES-128 berbasis *web*. Perbedaan dari jurnal diatas, yaitu ada pada format yang bisa dienkripsi dan pada basis program.

1.2 Rumusan Masalah

Rumusan masalah yang akan dibahas adalah bagaimana cara mengamankan file supaya file tidak disalahgunakan oleh pihak yang tidak

bertanggungjawab di Komite Nasional Keselamatan Transportasi.

1.3 Tujuan Penelitian

Berdasarkan permasalahan dari rumusan masalah yang ada, maka tujuan yang diharapkan dari penulisan penelitian ini adalah :

a. Untuk menerapkan algoritma *AES-128* pada aplikasi enkripsi berbasis *web*.
b. Untuk mengamankan *file* berupa informasi dapat terlindungi dengan baik.

1.4 Langkah – Langkah Penelitian

Penelitian harus berasal dari sumber data yang lengkap dan terpercaya untuk memperoleh informasi yang diperlukan dalam memecahkan masalah yang ingin diselesaikan. Metodologi pengembangan sistem ini merujuk pada model waterfall, adapun metodologinya menurut Sommerville (2011) sebagai berikut:

a. Metode kepustakaan
   Pengumpulan data dilakukan dengan membaca jurnal pada internet. Jurnal tersebut menjelaskan mulai dari cara kerja Enkripsi metode AES-128 sampai dengan kelebihan yang dimilikinya.
b. Mengumpulkan data
   Mengumpulkan data mengenai Enkripsi metode AES-128, dari proses tahap penyeleksian dan juga batasan-batasan penyelesaian yang ditanamkan dalam metode tersebut.
c. Analisa data
   Data yang diperoleh kemudian dianalisa setelah itu dipelajari untuk mengetahui bentuk sistem cara kerja yang akan dibuat.
d. Membuat rancangan system
   Membuat rancangan sistem sesuai hasil analisa yang dilakukan dengan membuat rancangan layar, flowchart dan lain-lain.
e. Implementasi
   Rancangan sistem yang sudah dibuat diimplementasikan berdasarkan hasil analisa. Dan hasil analisa dapat dituangkan dalam code program dengan menggunakan bahasa pemrograman tertentu. Pada penerapan ke dalam program akan digunakan bahasa pemrograman Php.
f. Uji coba system
   Setelah sistem selesai dibuat maka dilakukan uji coba terhadap sistem yang buat.

2. LANDASAN TEORI

2.1 Definisi Kriptografi

Kata kriptografi berawal dari bahasa Yunani, "*kryptos*" yang berarti menyembunyikan dan "*graphein*" yang berarti tulisan. Kriptografi merupakan ilmu yang mempelajari cara untuk mengamankan yang berhubungan dengan aspek keamanan informasi seperti antektikasi, kerahasiaan data, keabsahan data dan data integritas. Kriptografi juga dapat disimpulkan sebagai seni untuk menjaga kerahasiaan pesan. Suatu pesan atau data yang masih asli dan belum mengalami perubahan dengan kriptografi dikenal dengan istilah *plaintext*. Kemudian setelah disamarkan dengan sebuah kriptografi, maka *plaintext* ini disebut sebagai *ciphertext*.

2.2 Tujuan Kriptografi

Ada 5 tujuan dari kriptografi yaitu sebagai berikut :

a. *Privacy / Confidentiality*
   Privacy lebih kearah data yang sifatnya rahasia, sedangkan *confidentiality* adalah hubungan antara data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diizinkan untuk keperluan tertentu.
b. *Integrity*
   Aspek ini menekan bahwa informasi tidak boleh diubah tanpa seizin pemilik informasi. Informasi yang diterima harus sesuai dan sama persis seperti saat informasi dikirimkan. Jika terdapat perbedaan antara informasi atau data yang dikirim dengan diterima maka aspek *integrity* tidak tercapai.
c. *Authenticity*
   Aspek ini berhubungan dengan metode atau cara untuk menyatakan bahwa informasi betul-betul asli, orang yang mengakses atau memberikan informasi adalah betul-betul orang yang di maksud.
d. *Availability*
   Aspek ini berhubungan dengan ketersediaan data dan informamsi. Data dan informasi yang berbeda dalam suatu sistem komputer tersedia dan dapat dimanfaatkan oleh orang yang berhak.
e. *Access Control*
   Aspek ini berhubugnan dengan cara pengaturan akses kepada informasi. Hal ini biasanya berhubungan dengan klasifikasi data, mekanisme autentikasi dan juga *privasi*. *Access control* sering kali digunakan untuk melakukan kombinasi *user id/password* atau dengan menggunakan mekanisme lain.

2.3 *Algoritma Advance Encryption Standard(AES)*

Algoritma AES adalah merupakan cara enkripsi yang di terbitkan pada tahun 2001 oleh NIST(National Institute of Standard and Technology) untuk menggantikan algoritma DES yang dianggap kuno dan sangat gampang dibobol, sehingga algoritma AES dijadikan standard untuk mengamankan data untuk

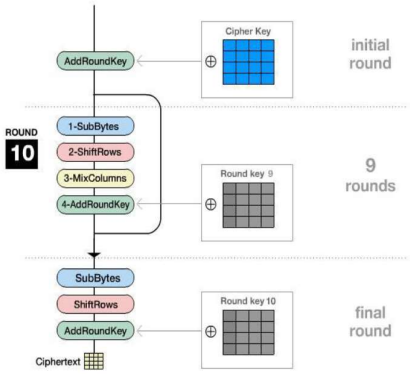
menggantikan algoritma DES. Algoritma AES termasuk jenis *block cipher* yang memiliki panjang kunci sebesar 128 bit, 192 bit, dan 256 bit. Urutan dari algoritma AES dalam suatu kelompok 128 bit disebut blok data atau biasa yang sering disebut plaintext yang selanjutnya akan dienkripsi menjadi *ciphertext*. Perbedaan panjang kunci tersebut nantinya mempengaruhi jumlah putaran pada algoritma AES ini.

Tabel 1. Jumlah Putaran AES [5]

Tipe	Jumlah Key (Nk)	Besar Blok (Nb)	Jumlah Round (Nr)
AES-128	4	4	10
AES-192	5	4	12
AES-256	6	4	14

2.4 Proses Enkripsi Advance Encryption Standard (AES)

AddRoundKey, SubBytes, ShiftRows, dan *Mixcolumns* adalah 4 jenis transformasi *bytes* pada proses enkripsi algoritma AES. Awal proses enkripsi , input yang disalin ke *state* akan mengalami transformasi *byte* berupa *AddRoundKey*. Setelah itu, *state* akan mengalami transformasi *byte SubBytes*, *ShiftRows*, *MixColumn* dan *AddRounKey* secara berulang sebanyak Nr. Proses ini disebut *round function*. Hanya saja pada perulangan terakhir tidak terjadi tranformasi *MixColumn*. Garis besar algoritma AES yang beroperasi pada blok 128-bit dengan kunci 128-bit adalah sebagai berikut (diluar proses pembangkitan *round key*): Proses putaran enkripsi AES-128 dikerjakan sebanyak 10 kali (Nr=10) yaitu seperti pada gambar 1.

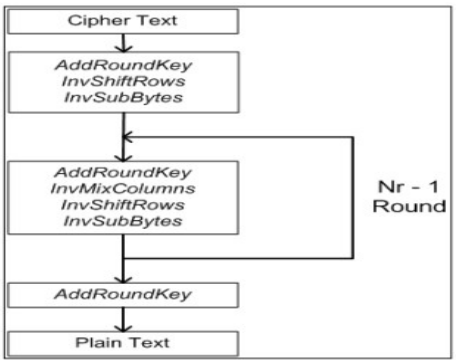


Gambar 1. Skema Proses Enkripsi AES-128 bit [5]

a. *Addroundkey* adalah meng-XOR-kan antara Plainteks (State awal) dengan *cipher key*. Tahap ini disebut juga *initial round.*
b. Algoritma aes ini mempunyai putaran sebanyak Nr-1 kali, proses putaran ini meliputi sebagai berikut: *SubByte, ShiftRows, MixColumns, dan AddRoundKey*.
c. Final Round, adalah proses putaran untuk putaran terakhir yang meliputi *SubBytes*, *ShiftRows*, dan *AddRoundKey*.

2.5 Proses Dekripsi Advanced Encryption Standard (AES)

Transformasi *cipher* dapat dibalikkan dari proses enkripsi dan diimplementasikan dalam arah yang berlawanan untuk mendapatkan *inverse cipher* yang mudah dimengerti untuk algoritma AES. Transformasi *byte* yang dipakai pada *invers cipher* yaitu *invShiftRows*, *InvSubBytes, InvMixColumns,* dan *AddRoundKey* seperti pada gambar 2.



Gambar 2. Skema Dekripsi AES-128 [5]

2.6 *Contoh Alur Algoritma Enkripsi AES*

Berikut ini adalah contoh dari alur Advanced Encryption Standard, Misalkan akan mengirim sebuah plainteks yang berisi 128 bit atau 16 karakter seperti berikut.

a. Plainteks : abcd
b. Kunci : dian

Maka plainteks dan kunci ini dapat dibuat menjadi state seperti pada tabel 2 dan 3.

Tabel 2. Plainteks

a	b	c	d
(null)	(null)	(null)	(null)
(null)	(null)	(null)	(null)
(null)	(null)	(null)	(null)

Tabel 3. Tabel Kunci

d	i	a	n
(null)	(null)	(null)	(null)
(null)	(null)	(null)	(null)
(null)	(null)	(null)	(null)

Karena Advanced Encryption Standard menggunakan representasi byte maka akan

menggunakan bilangan hexadecimal. Sehinggal teks diatas akan di konversikan menjadi bilangan hexadecimal dengan melihat kode ASCII, maka akan didapat seperti tabel 4 dan 5.

Tabel 4. Konversi Plainteks

61	62	63	64
00	00	00	00
00	00	00	00
00	00	00	00

Tabel 5. Konversi Kunci

44	69	61	6E
00	00	00	00
00	00	00	00
00	00	00	00

Proses untuk mencari RoundKey 1 sampai dengan 10 sebagai berikut.

Tabel 6. Mencari w[4]

44	69	61	6E	
00	00	00	00	
00	00	00	00	
00	00	00	00	
W[0]	W[1]	W[2]	W[3]	W[4]

Untuk mencari w[4] adalah seperti berikut.
W[i] = w[i-4] ⊕ Subword(rotword(W[3])) ⊕ RC[1].

Tabel 7. Proses Mencari W[4]

6E		00		63	⊕	01	⊕	44		26
00	➡	00	➡	63	➡	00	➡	00	➡	63
00		00		63		00		00		63
00	1	6E	2	9F	3	00	4	00	5	9F

Keterangan
1. W[3] Melakukan pergeseran 1 kali.
2. Melakukan subtitusi pada S.box.
3. Melakukan XOR dengan tabel Rcon.
4. Melakukan XOR dengan W[0].
5. Hasil W[4].

Tabel 8. Mencari W[5]

44	69	61	6E	26	
00	00	00	00	63	
00	00	00	00	63	
00	00	00	00	9F	
W[0]	W[1]	W[2]	W[3]	W[4]	W[5]

Untuk mencari W[5] adalah sebagai berikut.
W[i] = W[i-4] ⊕ W[i-1].

Tabel 9. Proses Mencari W[5]

69	⊕	26		4F
00	➡	63	➡	63
00		63		63
00	1	9F	2	9F

Keterangan
1. Melakukan XOR W[1] dan W[4].
2. Hasil W[5].

Hasil dari perhitungan untuk round key 1 sampai 10.

Tabel 10. Round key 1 Sampai 10

KUNCI				Round Key 1					Round Key 10			
44	69	6E	29	26	4F	2E	40		2E	D7	09	A4
00	00	00	00	63	63	63	63		94	65	71	B3
00	00	00	00	63	63	63	63	➡	2B	16	6A	35
00	00	00	00	9F	9F	9F	9F		41	47	81	95
W[0]	W[1]	W[2]	W[3]	W[4]	W[5]	W[6]	W[7]		W[40]	W[41]	W[42]	W[43]

Proses Enkripsi
Hal pertama yang harus dilakukan adalah melakukan XOR antara plainteks dan kunci, seperti berikut.

Tabel 11. Proses XOR Plainteks dan Kunci

Plain Teks	Kunci	Hasil

61	62	63	64	⊕	44	69	61	6E	=	25	0B	02	0A
00	00	00	00		00	00	00	00		00	00	00	00
00	00	00	00		00	00	00	00		00	00	00	00
00	00	00	00		00	00	00	00		00	00	00	00

Ronde 1

a. Hasil proses subbyte dengan menggunakan tabel s-box.

Tabel 12. Proses Subtitusi Dengan S-Box

25	0B	02	0A	➡	3F	2B	77	67
00	00	00	00		63	63	63	63
00	00	00	00		63	63	63	63
00	00	00	00		63	63	63	63

b. Transformasi shiftrows

Tabel 13.Shiftrows

3F	2B	77	67	➡	3F	2B	77	67
63	63	63	63		63	63	63	63
63	63	63	63		63	63	63	63
63	63	63	63		63	63	63	63

c. Proses MixColumns

Proses ini merupakan proses terbanyak dari pada proses proses lain setiap rounde. Proses mixColumns menjadi 4 bagian untuk sebuah matriks atau state karena dikerjakan untuk setiap kolom sebagai berikut.

1. Proses MixColumn untuk kolom pertama.

Tabel 14. Proses MixColumns

S'(0,1)	=	02	03	01	01	*	3F	2B	77	67
S'(1,1)		01	02	03	01		63	63	63	63
S'(2,1)		01	01	02	03		63	63	63	63
S'(3,1)		03	01	01	02		63	63	63	63

HASIL			
DB	F3	4B	6B
3F	2B	77	67
87	BB	5F	6F

Pada ronde pertama didapat Cipherteks yang akan menjadi masukan atau input untuk ronde kedua, begitu juga cipherteks yang didapat pada ronde kedua akan digunakan menjadi inputan pada ronde ketiga. Proses ini berlangsung hingga ronde kesepuluh. Pada ronde kesepuluh didapat hasil enkripsi sebagai berikut.

Ronde-10 :

Tabel 15. Proses Ronde ke-10 Sub-byte

66	05	8B	CD
10	3C	D9	02
0C	25	3A	52
4B	2B	3E	A3

Tabel 16. Proses Ronde ke-10 Shift Rows

66	05	8B	CD
3C	D9	02	10
3A	52	0C	25
A3	4B	2B	3E

Tabel 17. Proses Ronde ke-10 Add Round Key

48	D2	82	69
A8	BC	73	A3
11	44	66	10
E2	0C	AA	AB

Pada ronde 10 transformasi yang dilakukan hanya 3 transformasi yaitu subbyte , shiftrows, Addroundkey. Dan didapat cipherteks yang sesungguhnya yaitu.

Tabel 19. Hasil Ronde 10

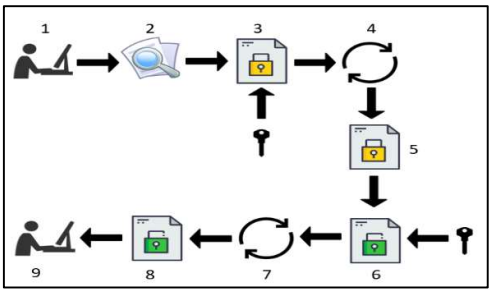
48	D2	82	69
A8	BC	73	A3
11	44	66	10
E2	0C	AA	AB

Jika didalam bentuk ASCII maka didapat cipherteks **: H Ò R i ¨ ¼ s £ [DC1] D f [DLE] â [FF] ª «**

3. ANALISIS MASALAH DAN PERANCANGAN SOLUSI

3.1 Arsitektur Aplikasi

Aplikasi Pengamanan pada file di Komite Nasional Keselamatan Transprotasi berbasis Web dapat diakses oleh orang tertentu saja. Kemudian cara aplikasi ini dimulai dengan *login* aplikasi pengamanan file pada *Web*.



Gambar 2. Alur Kerja Aplikasi

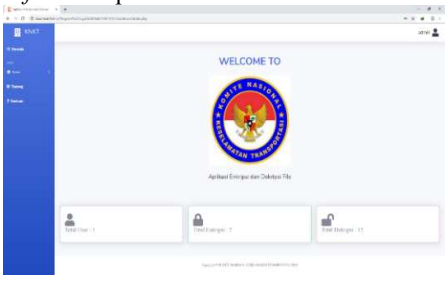
3.2 Tampilan Halaman Login

Saat Aplikasi dijalankan, maka yang pertama kali tampil adalah halaman login. Dimana user harus menginput username dan password untuk masuk ke halaman beranda. Di dalam login terdapat textfield untuk memasukan username dan password dan tombol login untuk memproses username dan password, jika benar akan masuk ke halaman beranda jika tidak akan kembali ke halaman login.

Gambar 3. Tampilan Halaman Login

3.3 Tampilan Halaman Beranda

Pada halaman beranda ini terdapat menu – menu *Form*, Tentang, Bantuan. Terdapat 3 submenu dari *Form* yang isinya adalah *Form* Enkripsi, *Form* Dekripsi, dan *Form* Data Informasi. didalam menu beranda terdapat beberapa fitur yang dapat menampilkan jumlah user yang dapat *login*, jumlah *file* enkripsi dan jumlah *file* dekripsi.

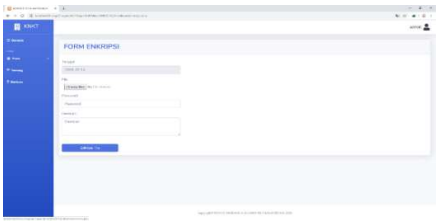


Gambar 4. Tampilan Halaman Beranda

3.4 Tampilan Halaman Form Enkripsi

Pada halaman form enkripsi terdapat textfield tanggal, tombol choose file, textfield password, textfield dekripsi. textfield tanggal adalah , tombol choose file adalah untuk memilih file yang akan dienkripsi, textfield password adalah untuk memasukan password atau kunci pada file, textfield dekripsi adalah untuk membuat informasi kepada file tersebut.

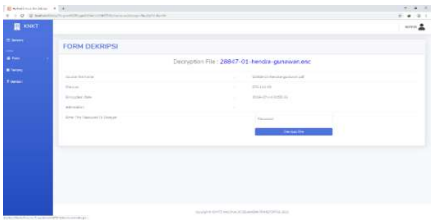
.



Gambar 5. Halaman Form Enkripsi

3.5 Tampilan Halaman Form Dekripsi

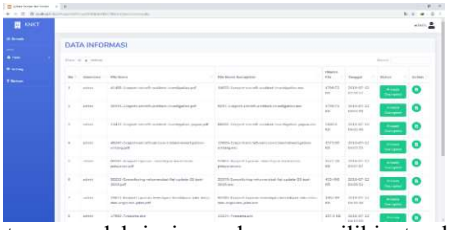
Pada halaman dekripsi terdapat text untuk menampilkan informasi file , textfield password untuk memasukan password yang sesuai dengan memasukan password enkripsi, dan tombol dekripsi file untuk proses dekripsi file tersebut.



Gambar 6. Tampilan Halaman Form Dekripsi

3.5 Tampilan Halaman Data Informasi

Pada halaman Data Informasi terdapat tabel yang berisikan semua data yang terenkripsi



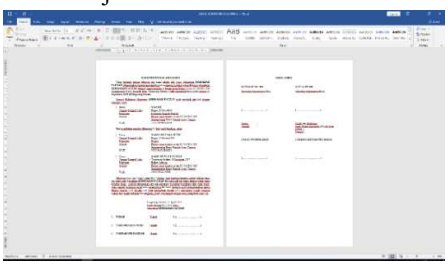
ataupun dekripsi , dan memiliki tombol download untuk mendownload file yang terenkripsi ataupun dekripsi.

Gambar 7. Tampilan Halaman Data Informasi

3.6 Uji Coba Pada File

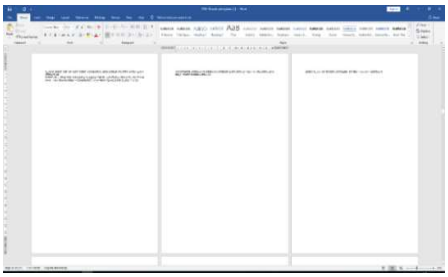
Dalam Pengujian aplikasi ini, dilakukan terhadap hasil pengujian *file* yang asli dengan *file* yang telah dienkripsi menggunakan aplikasi ini dengan kebutuhan yang telah terpenuhi baik spesifikasi *software* maupun spesifikasi *hardware. File* yang akan di coba meliputi format *.doc, *.pdf, *.xls.

a. Uji Coba file *.doc



Gambar 8. File *.doc sebelum enkripsi

Setelah file *.doc dienkripsi maka file akan berubah seperti gambar berikut.



Gambar 9. File *.doc sesudah enkripsi

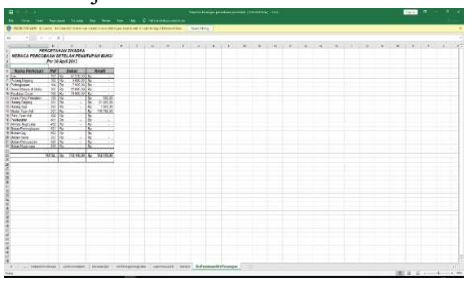
b. Uji Coba File *.Pdf

Gambar 10. File *.pdf sebelum enkripsi

Setelah file *.pdf dienkripsi maka file akan berubah seperti gambar berikut

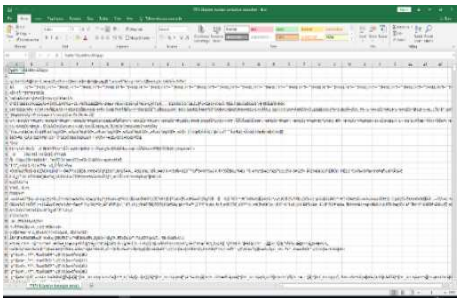
Gambar 11. File *.pdf sesudah enkripsi

c. Uji Coba File *.xls



Gambar 12. File *.xls sebelum enkripsi

Setelah file *.xls dienkripsi maka file akan berubah seperti gambar berikut.



Gambar 13. File *.xls sesudah enkripsi

3.7 Tabel Pengujian

Dalam tabel Pengujian ini akan dibahas perbandingan antara proses enkripsi dan dekripsi file. File yang diuji meliputi format *.doc, *.docx, *.pdf, *.xlsx, *.xls, *.pptx, *.ppt. Pengujian ini dilakukan untuk melihat perbandingan antara file asli dengan file setelah di enkripsi serta waktu proses enkripsi dan dekripsi.

Tabel 20. Pengujian

Nama File	Ukuran File			Waktu (Detik)	
	Asli	Enkripsi	Dekripsi	Enkripsi	Dekripsi
Report Aircraft Accident Investigation.pdf	1.800 KB	1.799,72 KB	1.800 KB	80.4526	79.3247
Report-Aircraft Accident Investigation-papua.pdf	2.486 KB	2.485,8 KB	2.486 KB	110.9472	108.6355
laporan-keuangan-perusahaan-percetakan.xls	872 KB	871,5 KB	872 KB	38.9759	38.3819
Minggu10_PowerPoint.ppt	1.521 KB	1.519 KB	1.521 KB	68.613	67.1862
Surat Pernyataan.doc	20 KB	19,57 KB	20 KB	0.9395	0.8771

3.8 Kelebihan Aplikasi

Berdasarkan hasil uji coba program yang dilakukan beberapa sampel maka dapat

disimpulkan kelebihan dari aplikasi tersebut sebagai berikut:

a. Program aplikasi ini sangat mudah digunakan dan isi filenya terjamin keamananya.
b. Ukuran setelah didekripsi kembali ke ukuran *file* awal.

3.9 Keterbatasan Aplikasi

Berdasarkan hasil uji coba program yang dilakukan beberapa sampel maka dapat disimpulkan keterbatasan dari aplikasi tersebut sebagai berikut:

a. Hanya mengenkripsi *file* dari Word, Excel, PowerPoint, *Text*, dan Pdf.
c. Maksimal file hanya 5MB
d. Semakin besar file yang di enkripsi, maka semakin lama prosesnya.

4. KESIMPULAN

Dari hasil analisis masalah yang telah dijabarkan dan juga aplikasi yang dibuat, maka dapat ditarik kesimpulan sebagai berikut:

a. Dengan adanya aplikasi kriptografi dengan metode AES ini dapat mengamankan dokumen penting yang ada di Komite Nasional Keselamatan Transportasi .
b. Algoritma AES-128 bit ini berhasil diterapkan pada Komite Nasional Keselamatan Transportasi.
c. Untuk mengamankan file dilakukan enkripsi sehingga hanya orang mempunyai kunci yang dapat mendekripsi file tersebut.

Beberapa saran yang diberikan untuk pengemanban selanjutnya dengan harapan menghasilkan penelitian yang lebih baik lagi, berikut saran yang dapat diberikan :

a. Pada penelitian selanjutnya dapat dikembangkan metode kriptografi lain atau menggabungkan 2 metode sampai 3 metode kriptografi agar lebih aman.
b. Penelitian ini dapat juga ditambahkan metode steganografi untuk menyembunyikan data dari pihak yang tidak bertanggungjawab.
d. Penelitian selanjutnya dapat menambahkan format music, gambar, dan video.
e. Waktu proses diharapkan dapat lebih cepat walapun dengan ukuran file yang besar.

5. DAFTAR PUSAKA

[1]. Arif, A. and Mandarani, P. (2016). Rekayasa Perangkat Lunak Kriptografi menggunakan Algoritma Advanced Encryption Standard (AES) 128 bit pada sistem keamanan *Short Message Service* (SMS) berbasis Android. Jurnal TEKNOIF, 4(1), pp. 84-93.

[2]. Harahap, Muh. K. (2016). Analisis Perbandingan Algoritma kriptografi Klasik Vigenere Cipher dan One Time Pad. Jurnal Nasional Informatika dan Teknologi Jaringan, 1(1), pp. 61-64.

[3]. Latif, A. (2015). Implementasi Kriptografi Menggunakan Metode Advanced Encryption Standar (AES) untuk pengamanan data teks. Jurnal Ilmiah Mustek Anim Ha, 4(2), pp. 163-172.

[4]. Muharram, F., Azis, H. and Manga, A. R. (2018). Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES). Prosiding Seminar Nasional Ilmu Komputer dan Teknologi Informasi, 3(2), pp. 112-115.

[5]. Nurnaningsih, D. and Permana, A. A. (2018). Rancangan Aplikasi Pengamanan Data Dengan Algoritma Algoritma Advanced Encryption Standard (AES). *JURNAL TEKNIK INFORMATIKA*, 11(2), pp. 177-186.