IN
REVIEW

ENKRIPSI DAN DEKRIPSI UNTUK KEAMANAN FILE MENGGUNAKAN ALGORITMA RIJNDAEL

TUGAS AKHIR

Arip Pebruano
41516320012

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2018

ENKRIPSI DAN DEKRIPSI UNTUK KEAMANAN FILE MENGGUNAKAN ALGORITMA RIJNDAEL

Tugas Akhir

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:
Arip Pebruano
41516320012

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2018

LEMBAR PERNYATAAN ORISINALITAS

Yang bertanda tangan dibawah ini:

NIM	: 41516320012
Nama	: Arip Pebruano
Judul Tugas Akhir	: Enkripsi Dan Dekripsi Untuk Keamanan File Menggunakan Algoritma Rijndael

Menyatakan bahwa Laporan Tugas Akhir saya adalah hasil karya sendiri dan bukan plagiat. Apabila ternyata ditemukan didalam laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Bekasi, 27 Desember 2018

Arip Pebruano

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR

Sebagai mahasiswa Universitas Mercu Buana, saya yang bertanda tangan di bawah ini :

Nama Mahasiswa	:	Arip Pebruano
NIM	:	41516320012
Judul Tugas Akhir	:	Enkripsi Dan Dekripsi Untuk Keamanan File Menggunakan Algoritma Rijndael

Dengan ini memberikan izin dan menyetujui untuk memberikan kepada Universitas Mercu Buana **Hak Bebas Royalti Noneksklusif** (*None-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul diatas beserta perangkat yang ada (jika diperlukan).

Dengan Hak Bebas Royalti/Noneksklusif ini Universitas Mercu Buana berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat dan mempublikasikan tugas akhir saya.

Selain itu, demi pengembangan ilmu pengetahuan di lingkungan Universitas Mercu Buana, saya memberikan izin kepada Peneliti di Lab Riset Fakultas Ilmu Komputer, Universitas Mercu Buana untuk menggunakan dan mengembangkan hasil riset yang ada dalam tugas akhir untuk kepentingan riset dan publikasi selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Bekasi, 29 Desember 2018

Arip Pebruano

SURAT PERNYATAAN LUARAN TUGAS AKHIR

Sebagai mahasiswa Universitas Mercu Buana, saya yang bertanda tangan di bawah ini :

Nama Mahasiswa	:	Arip Pebruano
NIM	:	41516320012
Judul Tugas Akhir	:	Enkripsi Dan Dekripsi Untuk Keamanan File Menggunakan Algoritma Rijndael

Menyatakan bahwa Luaran Tugas Akhir saya adalah sebagai berikut :

No	Luaran	Jenis			Status	
1	Publikasi Ilmiah	Jurnal Nasional Tidak Terakreditasi		✓	Diajukan	✓
		Jurnal Nasional Terakreditasi				
		Jurnal International Tidak Bereputasi			Diterima	
		Jurnal International Bereputasi				
	Disubmit/dipublikasikan di :	Nama Jurnal	: Jurnal Ilmiah Teknik Informatika Format			
		ISSN	: ISSN : 2089 - 5615			
2	Kertas Kerja, Merupakan material haasil penelitian sebagai kelengkapan Artikel Jurnal. Terdiri dari (minimal 4)	Literatur Review				[✓]
		Hasil analisa & perancangan aplikasi				[✓]
		Source code				[✓]
		Data set				[ ]
		Tahapan eksperimen				[✓]
		Hasil eksperimen seluruhnya				[✓]
		....				
3	HAKI Disubmit / Terdaftar	HKI			Diajukan	
		Paten			Tercatat	
		No & Tanggal Permohonan	:			
		No & Tanggal Pencatatan	:			

Demikian pernyataan ini saya buat dengan sebenarnya.

Bekasi, 27 Desember 2018

Arip Pebruano

LEMBAR PERSETUJUAN

Nama Mahasiswa	:	Arip Pebruano
NIM	:	41516320012
Judul Tugas Akhir	:	Enkripsi Dan Dekripsi Untuk Keamanan File Menggunakan Algoritma Rijndael

Tugas Akhir ini telah diperiksa dan disetujui

Bekasi, 27 Desember 2018

Menyetujui,

(Sri Dianing Asri, ST, M.Kom)
Dosen Pembimbing

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41516320012
Nama	:	Arip Pebruano
Judul Tugas Akhir	:	Enkripsi Dan Dekripsi Untuk Keamanan File Menggunakan Algortima Rijndael

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 2 Februari 2019

(Diky Firdaus, S.Kom, MM)
Ketua Penguji

(Nur Ani, MMSI)
Anggota Penguji 1

(Umniy Salamah, MMSI)
Anggota Penguji 2

LEMBAR PENGESAHAN

NIM	:	41516320012
Nama	:	Arip Pebruano
Judul Tugas Akhir	:	Enkripsi Dan Dekripsi Untuk Keamanan File Menggunakan Algortma Rijndael

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 2 Februari 2019

Menyetujui,

(Sri Dianing Asri, ST, M.Kom)
Dosen Pembimbing

Mengetahui,

(Diky Firdaus, S.Kom, MM)	(Desi Ramayanti, S.Kom, MT)
Koord. Tugas Akhir Teknik Informatika	Ka. Prodi Teknik Informatika

ABSTRAK

Nama	:	Arip Pebruano
NIM	:	41516320012
Pembimbing TA	:	Sri Dianing Asri, ST, M.Kom
Judul	:	Enkripsi Dan Dekripsi Untuk Keamanan File Menggunakan Algoritma Rijndael

Banyak data informasi yang penting berbentuk file. Hal ini tentunya sangat diperlukan keamanan terhadap data tersebut agar tidak dapat dibaca oleh sebarang orang. Teknik pengamanan dapat dilakukan dengan kriptografi. Salah satu metode yang digunakan adalah Rijndael, Rijndael Adalah algoritma yang beroperasi dalam byte Algoritma ini mampu melakukan enkripsi terhadap plain text sebesar 16 byte atau 128 bit. Selain itu, algoritma ini juga menggunakan kunci sebanyak 16 byte. Dengan kunci sepanjang 128 bit, maka terdapat 2128 = 3,4 x 1038 kemungkinan kunci. Dengan demikian, waktu yang dibutuhkan untuk menebak kunci yang ada dengan komputer yang cepat pun membutuhkan 1018 tahun. Selain panjang kunci yang lumayan banyak, kunci internal pada algoritma ini juga selalu berubah pada setiap putarannya. Kunci internal ini disebut dengan round key menggunakan kunci simetris. Dimana proses enkripsi dan dekripsi nya menggunakan kunci yang sama. Algoritma rijndael didesain oleh Vincent Rijmen dan John Daemen asal Belgia keluar sebagai pemenang kontes algoritma kriptografi pengganti DES yang diadakan oleh NIST (National Institutes of Standards and Technology) milik pemerintah Amerika Serikat pada 26 November 2001. Algoritma Rijndael inilah yang kemudian dikenal dengan Advanced Encryption Standard (AES). Setelah mengalami beberapa proses standardisasi oleh NIST, Rijndael kemudian diadopsi menjadi standard algoritma kriptografi secara resmi pada 22 Mei 2002.

Kata kunci:

rijndael, kriptografi, ilmu komputer, universitas mercu buana

ABSTRACT

Name	:	Arip Pebruano
Student Number	:	41516320012
Counsellor	:	Sri Dianing Asri, ST, M.Kom
Title	:	Encryption And Decryption For Secure File Using Rijndael Algorithm

File can contain data and information that is important,it must be secured so other people can't read it. criptograpy can be an option to secure it,rijndel is one of the method that we can use,rijndel operate in byte,this algorithm can encrypt the plain text up to 16 byte or 128 bit, otherwise this algorithm use a lock/key up to 16 byte with the length of the the lock/key up to 128 byte,it has a 2128 = 3.4 x 1038 possible lock/key and its need 1018 years even with a super fast computer. Besides the length of the key,every spin in this algorithm it's always change,this internal key called a round key using a simetis key.the proses encrypt and decrypt have a same lock key. The rijndel algorithm it design by vincent rijmen and john daemen from belgium. After win an algorithm cryptography contest that replace DES algorithm organised by NIST that belong to american government 26 nov 2001 rijndael algorithm now is known as an advanced encrypt standard. After through many adjusment by NIST, and then rijndael adapted to be official standard algorithm cryptography at 22 mei 2002.

Key words:

rijndael, kriptografi, computer science, universitas mercu buana

KATA PENGANTAR

Puji syukur kita panjatkan kehadirat Allah S.W.T yang telah memberikan limpahan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan tugas akhir yang berjudul **Enkripsi Dan Dekripsi Untuk Keamanan File Menggunakan Algoritma Rijndael** dapat penulis selesaikan sesuai dengan rencana karena dukungan dari berbagai pihak yang tidak ternilai besarnya. Oleh karena itu penulis menyampaikan terima kasih kepada:

1. Prof. Dr. Ngadino Surip, selaku Rektor Universitas Mercu Buana Jakarta
2. Desi Ramayanti, S.Kom., MT, selaku Ketua Program Studi Teknik Informatika
3. Sri Dianing Asri, ST, M.Kom, selaku dosen pembimbing yang telah memberikan bimbingan kepada penulis dalam penyusunan laporan tugas akhir ini.
4. Ibu saya yang tidak pernah lelah memberikan doa serta dukungan kepada penulis untuk maju dan terus berusaha.

Semoga laporan tugas akhir ini dapat memperluas wawasan dan pengetahuan yang bermanfaat dan berguna sebagaimana fungsinya.

Bekasi, 29 Desember 2018

Arip Pebruano

DAFTAR ISI

NASKAH JURNAL

ENKRIPSI DAN DEKRIPSI UNTUK KEAMANAN FILE MENGGUNAKAN ALGORITMA RIJNDAEL

Arip Pebruano
Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana
Jl. Raya Meruya Selatan, Kembangan, Jakarta, 11650
arif.februano@gmail.com

Abstract - File can contain data and information that is important,it must be secured so other people can't read it.criptograpy can be an option to secure it,rijndel is one of the method that we can use,rijndel operate in byte,this algorithm can encrypt the plain text up to 16 byte or 128 bit, otherwise this algorithm use a lock/key up to 16 byte with the length of the the lock/key up to 128 byte,it has a 2128 = 3.4 x 1038 possible lock/key and its need 1018 years even with a super fast computer. Besides the length of the key,every spin in this algorithm it's always change,this internal key called a round key using a simetis key.the proses encrypt and decrypt have a same lock key. The rijndel algorithm it design by vincent rijmen and john daemen from belgium. After win an algorithm cryptography contest that replace DES algorithm organised by NIST that belong to american government 26 nov 2001 rijndael algorithm now is known as an advanced encrypt standard. After through many adjusment by NIST, and then rijndael adapted to be official standard algorithm cryptography at 22 mei 2002.

Keywords: cryptography, rijndael, AES

Abstrak - Banyak data informasi yang penting berbentuk file. Hal ini tentunya sangat diperlukan keamanan terhadap data tersebut agar tidak dapat dibaca oleh sebarang orang. Teknik pengamanan dapat dilakukan dengan kriptografi. Salah satu metode yang digunakan adalah Rijndael, Rijndael Adalah algoritma yang beroperasi dalam byte Algoritma ini mampu melakukan enkripsi terhadap plain text sebesar 16 byte atau 128 bit. Selain itu, algoritma ini juga menggunakan kunci sebanyak 16 byte. Dengan kunci sepanjang 128 bit, maka terdapat 2128 = 3,4 x 1038 kemungkinan kunci. Dengan demikian, waktu yang dibutuhkan untuk menebak kunci yang ada dengan komputer yang cepat pun membutuhkan 1018 tahun. Selain panjang kunci yang lumayan banyak, kunci internal pada algoritma ini juga selalu berubah pada setiap putarannya. Kunci internal ini disebut dengan round key menggunakan kunci simetris. Dimana proses enkripsi dan dekripsi nya menggunakan kunci yang sama. Algoritma rijndael didesain oleh Vincent Rijmen dan John Daemen asal Belgia keluar sebagai pemenang kontes algoritma kriptografi pengganti DES yang diadakan oleh NIST (National Institutes of Standards and Technology) milik pemerintah Amerika Serikat pada 26 November 2001. Algoritma Rijndael inilah yang kemudian dikenal dengan Advanced Encryption Standard (AES). Setelah mengalami beberapa proses standardisasi oleh NIST, Rijndael kemudian diadopsi menjadi standard algoritma kriptografi secara resmi pada 22 Mei 2002.

Kata kunci: ***kriptografi, rijndael, AES***

I. PENDAHULUAN

Di era modern seperti saat ini, teknologi sangat erat kaitannya dengan komputer. Komputer sudah menjadi bagian penting dalam kehidupan manusia, penggunaan komputer sendiri sudah menjadi kebutuhan primer. Tak dipungkiri lagi, semua orang yang melakukan komunikasi atau pertukaran data serta informasi dengan pihak lainnya melalui internet ataupun mengcopy data menggunakan media penyimpanan secara manual. Data dan informasi akan disimpan pada komputer atau laptop pribadi. Data penting yang berada dalam komputer perlu dijaga kerahasiaannya, karena data tersebut bisa saja menjadi target pihak yang tak berwenang, terutama data dan informasi yang sifatnya sangat rahasia.

Untuk menjamin keamanan pertukaran informasi data dapat diatasi dengan implementasi kriptografi atau pengacakan terhadap informasi. Sehingga pesan tersebut tidak dapat dipahami oleh pihak lain. Kriptografi memiliki dua konsep yang penting, yaitu enkripsi dan dekripsi[1]. Enkripsi mengubah informasi atau data menjadi bentuk yang hampir tidak dikenali seperti informasi awal menggunakan algoritma tertentu, sedangkan dekripsi mengubah bentuk tersamar tersebut menjadi informasi awal[2].

Berdasarkan permasalahan yang ada, maka penelitian ini akan mencoba membuat perangkat untuk mengamankan semua file windows 7 dengan menerapkan kriptografi rijndael 256 bit menggunakan Visual Studio 2010.Perangkat lunak ini bertujuan untuk mengamankan dokumen sebelum mengirim melalui jaringan internet atau penyimpanan external, sehingga hanya orang yang berkepentingan yang mengetahui isi dari file tersebut.

II. LANDASAN TEORI

A. Rindael

Rijndael adalah salah satu algoritma AES yang sifatnya simetris dan block cipher. Dengan demikian algoritma ini menggunakan kunci yang sama saat enkripsi dan dekripsi. Rijndael mendukung berbagai variasi ukuran blok dan kunci yang akan digunakan. Namun Rijndael mempunyai ukuran blok dan kunci yang tetap sebesar 128, 192, 256 bit. Pemilihan ukuran blok data dan kunci akan menentukan jumlah proses yang harus dilalui untuk proses enkripsi dan dekripsi[3]. Barulah kemudian blok itu akan diproses dengan metode yang akan dijelaskan.

B. Proses Enkripsi

Pada proses enkripsi ada 4 jenis transformasi bytes, yaitu SubBytes, ShiftRows, MixColumns, dan AddRoundKey. Pada awal proses enkripsi, input yang diberikan ke dalam state akan mengalami transformasi byte AddRoundKey. Setelah itu, state akan mengalami transformasi SubBytes, ShiftRows, MixColumns, dan AddRoundKey secara berulang-ulang sebanyak Nr. Proses ini dalam algoritma AES disebut sebagai round function. Round yang terakhir agak berbeda dengan round-round sebelumnya dimana pada round terakhir, state tidak mengalami transformasi MixColumns.

C. Sub-bytes

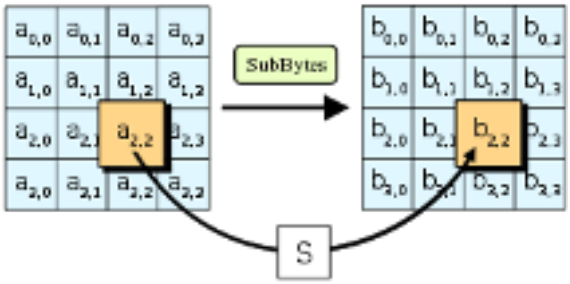
Proses SubBytes Proses SubBytes memetakan setiap byte dari array State dengan menggunakan tabel substitusi S-Box. Tidak seperti Des S-box berbeda pada setiap putaran, AES hanya mempunyai satu buah S-Box. Tabel yang digunakan adalah seperti pada gambar 2.2.

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	0a
dx	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Gambar 2.2 Tabel s-box

Dikutip dari : https://en.wikipedia.org/wiki/Rijndael_S-box

Dalam langkah SubBytes, setiap byte dalam array diperbarui menggunakan 8-bit substitusi kotak, Rijndael S-box. Proses SubBytes adalah operasi yang akan melakukan substitusi tidak linear dengan cara mengganti setiap byte statedengan byte pada sebuah tabel yang dinamakan tabel SBox. Sebuah tabel S-Box terdiri dari 16x16 baris dan kolom dengan masing-masing berukuran 1 byte [4]

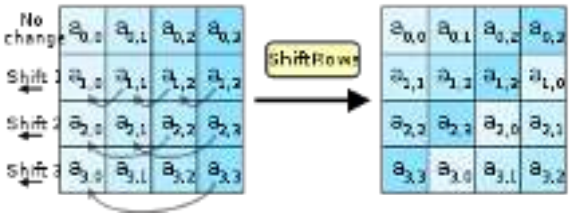


Gambar 2.3 SubBytes

Dikutip dari : https://id.wikipedia.org/wiki/Berkas:AES-SubBytes.svg

D. ShiftRows

Proses ShiftRows ini adalah proses yang sangat sederhana. Pada ShiftRows melakukan pergerseran wrapping pada 3 baris terkhir dari array state. putaran menggeser byte di setiap baris dengan offset tertentu. Untuk AES baris pertama tidak mengalami pergeseran dan Setiap byte dari baris kedua bergeser satu ke kiri. Demikian pula, baris ketiga dan keempat dialihkan oleh offset masing-masing dari dua dan tiga.

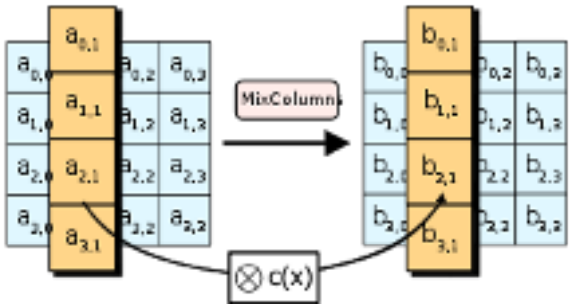


Gambar 2.4 table ShiftRows

Dikutip dari : https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

E. MixCollums

Dalam langkah MixColumns, empat byte dari setiap kolom state digabungkan dengan menggunakan transformasi linier invertible. Fungsi MixColumns mengambil empat byte sebagai masukan dan keluaran empat byte, dimana setiap masukan byte mempengaruhi semua keluaran empat byte. Dengan ShiftRows, MixColumns memberikan difusi dalam sandi. Dalam langkah MixColumns, masing-masing kolom negara dikalikan dengan tetap polinomial c (x) lihat gambar 2.5.

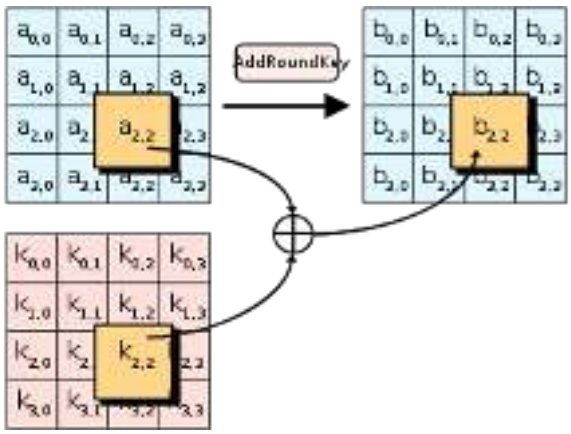


Gambar 2.5 MixColumns

Dikutip dari : https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

F. AddRounKey

Dalam AddRoundKey langkah, subkey dikombinasikan dengan state. Untuk setiap putaran, sebuah subkunci berasal dari kunci utama menggunakan Rijndael.. Subkunci ditambahkan dengan menggabungkan setiap byte dari state sesuai dengan byte dari subkey menggunakan bitwise XOR. pada gambar 2.6 langkah AddRoundKey setiap byte dari state dikombinasikan dengan byte dari subkunci putaran menggunakan operasi XOR (⊕) .



Gambar 2.6 proses AddRound key

Dikutip dari : https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

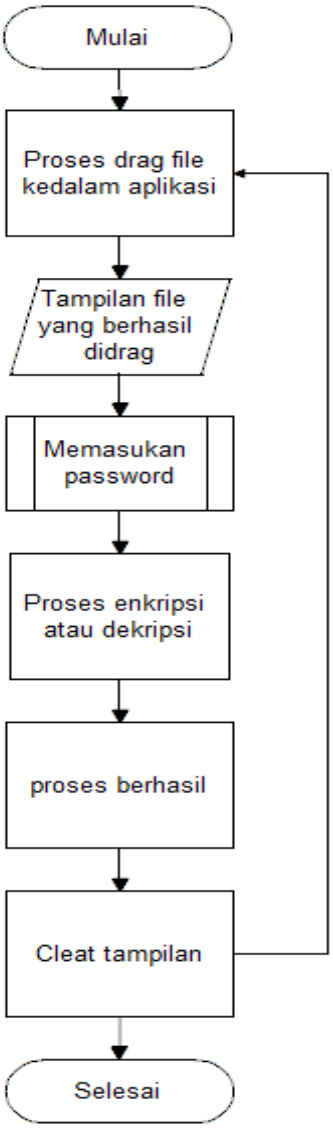
G. Proses Dekripsi

Metode dekripsi hanyalah kebalikan dari sistem enkripsi. Namun, dalam proses dekripsi input yang digunakan adalah ciphertext yang diperoleh selama proses enkripsi. Mirip dengan proses enkripsi, dekripsi memulai XOR antara ciphertext dengan cipherkey. Terdapat 13 kali putaran dalam proses dekripsi. Langkah proses dekripsi

a) melakukan AddroundKey
b) melakukan proses Inverse ShiftRow, Inverse SubBytes, AddRoundKey dan Inverse MixColumns sebanyak sembilan kali putaran.
c) Pada putaran terakhir atau putaran ke sepuluh terjadi proses InvShiftRows, InvSubBytes dan proses InvMixColums

III. DESAIN PENELITIAN

1. FLOWCHART APLIKASI



Gambar 3.1 flowchart aplikasi

Pada gambar 3.1 flowchart aplikasi terdapat 4 langkah, langkah pertama file yang akan diproses di drag kedalam aplikasi, langkah kedua yaitu masukan password, langkah ketiga klik tombol enkripsi/dekripsi, pada langkah keempat clear tampilan untuk mereset tampilan aplikasi untuk memproses file lain.

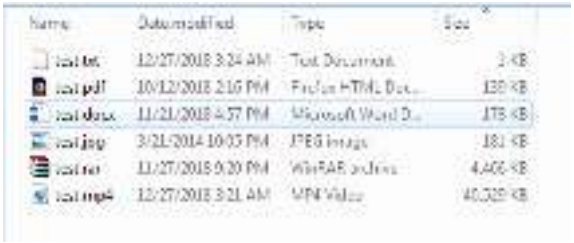
A. Desain aplikasi

Perancangan desain pada aplikasi menggunakan visual studio 2010 dan diberi nama ”Kriptografi rijndael”. Terdapat 1 Listview yaitu berfungsi untuk drag file ke aplikasi dan menampilkan file yang akan diproses, pada aplikasi terdapat 3 button yaitu button enkripsi yang berfungsi untuk melakukan proses enkripsi, button dekripsi untuk melakukan proses dekripsi, dan button clear untuk meriset kolom yang ada diaplikasi, salain itu juga terdapat 2 label yang berfungsi memberi keterangan memaksukan password dan keterangan file yang akan diproses harus digrag atau drop ke dalam aplikasi, 1 Textbox untuk memasukan password sebelum file diproses, dan 1 progressbar untuk menampilkan proses status.

Gambar 2.19 Tampilan antarmuka program

B. Implementasi dan pengujian

Pengujian program pada tahap ini dilakukan dengan drag beberapa file ke dalam aplikasi, ada beberapa format file diantaranya txt, docx, pdf, jpg, mp4 dan rar. Pada gambar 4.1 dapat dilihat file yang akan di drag kedalam aplikasi.



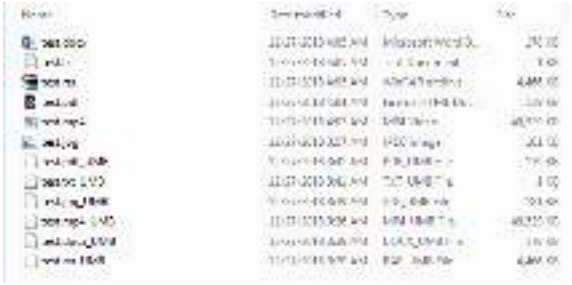
Gambar 4.1 List file

Gambar 4.2 file yang berhasil didrag

Pada proses drag file memerlukan waktu proses memindahkan file atau menyalin file kedalam aplikasi, waktu yang dibutuhkan dalam proses drag file tergantung besar ukuran file tersebut, semakin besar ukuran file yang akan di drag maka semakin lama program dapat menampilkan file tersebut.

C. Proses enkripsi

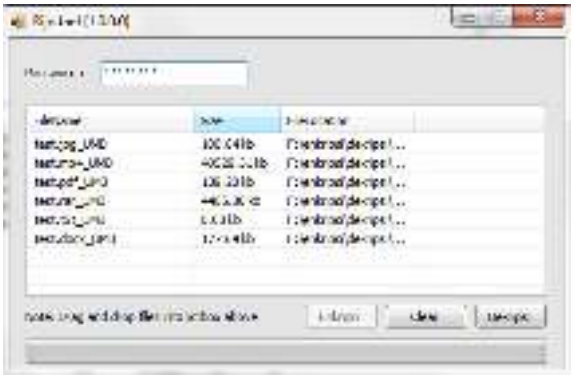
Tahap pengujian berikutnya adalah tahap enkripsi file yang sudah didrag kedalam aplikasi akan dienkripsi dengan kunci ”rijndael” (8 karakter), dapat dilihat pada gambar 4.3 hasil dari proses enkripsi menghasilkan file chiper dan format file berubah menjadi _UMB.



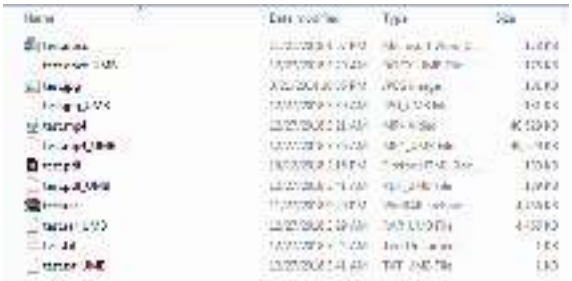
Gambar 4.3 Hasil Enkripsi

D. Proses dekripsi

Pengujian pada tahap ini adalah proses dekripsi dengan kata kunci yang sama saat proses enkripsi yaitu ”rijndael”, pada tahap ini file asli tidak bisa disatukan kedalam 1 folder dengan file hasil enkripsi dikarenakan pada proses dekripsi file akan disimpan kedalam folder yang sama dan nama yang sama, jadi penguji tidak bisa mengetahui apakah proses dekripsi berhasil atau tidak. Pada gambar 4.4 file yang akan didekripsi didrag kedalam aplikasi dan pada gambar 4.5 proses dekripsi berhasil.



Gambar 4.4 file enkripsi yang akan didekripsi



Gambar 4.5 hasil dekripsi

Hasil pengujian proses enkripsi dan dekripsi dalam aplikasi ini berhasil bagi documen yang memiliki tipe .txt, .mp4, .rar, .docx, .jpg, .pdf.

IV. KESIMPULAN

Kesimpulan dari penelitian ini adalah :

1. Hasil dari proses enkripsi tidak sama sekali merubah ukuran file, hanya merubah bytes sehingga file tidak dapat dikenali oleh komputer.
2. Aplikasi yang dikembangkan dapat melakukan enkripsi dan dekripsi file dengan berbagai macam ukuran dan jenis file dalam satu proses.
3. Algoritma rijndael dapat dijadikan alternatif untuk proses keamanan data dalam hal ini enkripsi dan dekripsi file dokumen.

V. DAFTAR PUSTAKA

[1] Dan, P., Performansi, A., Algoritma, M., Dan, A. E. S., Yang, A. E. S., & Berbasis, T. (2015). ANDROID COMPARATION AND ANALYSIS OF PERFORMANCE OF ENCRYPTION- DECRYPTION OF TEXT USING AES ALGORITHM AND MODIFIED AES BASED ON ANDROID, *2*(2), 3022–3030.

[2] Yulianingsih, P., Hamdani, & Maharani, S. (2014). Aplikasi Chatting Rahasia Menggunakan Algoritma Vigenere Cipher. *INFORMATIKA Mulawarman*, *9*(1), 1–4.

[3] Santoso, K. I., & Habibi, R. (2014). Kriptografi Pada Aplikasi Komunikasi Data Dengan Algoritma AES 256. *Seminar Nasional Ilmu Komputer*, (Snik), 1–10. Retrieved from https://ejournal.stmikbinapatria.ac.id

[4] Abidin, A. M., Hardianti, F., & Setiani, I. N. (2016). Analisa Dan Implementasi Proses Kriptografi Encryption-Decryption Dengan Algoritma Advanced Encryption Standard (Aes-128). *Jurnal Sarjana Teknik Informatika, Keamanan Komputer*, `1-20.

[5] Wikipedia. 2017. Daftar pustaka. https://id.wikipedia.org/wiki/CRC . 12 desember 2018. (15:28)

[6] Wikipedia. 2018. Daftar Pustaka. https://en.wikipedia.org/wiki/Advanced_Encryption_Standard . 11 desember 2018 (23:37)

[7] Pardosi, I. A., Megawan, S., Sembiring, N. P., Mikroskil, S., & No, J. T. (2015). Aplikasi Penyembunyian Pesan pada Citra dengan Metode AES Kriptografi dan Enhanced LSB Steganografi, *16*(2), 135–144.

[8] Dan, P., Performansi, A., Algoritma, M., Dan, A. E. S., Yang, A. E. S., & Berbasis, T. (2015). ANDROID COMPARATION AND ANALYSIS OF PERFORMANCE OF ENCRYPTION-DECRYPTION OF TEXT USING AES ALGORITHM AND MODIFIED AES BASED ON ANDROID, *2*(2), 3022–3030.

[9] Nandar Pabokory, F., Fitri Astuti, I., & Harsa Kridalaksana, A. (2015). *IMPLEMENTASI KRIPTOGRAFI PENGAMANAN DATA PADA PESAN TEKS, ISI FILE DOKUMEN, DAN FILE DOKUMEN MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD*. *Jurnal Informatika Mulawarman* (Vol. 10).

[10] Nandar Pabokory, F., Fitri Astuti, I., & Harsa Kridalaksana, A. (2015). *IMPLEMENTASI KRIPTOGRAFI PENGAMANAN DATA PADA PESAN TEKS, ISI FILE DOKUMEN, DAN FILE DOKUMEN MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD*. *Jurnal Informatika Mulawarman* (Vol. 10).

[11] Mankar, M., Kshirsagar, R. V, & Vyawahare, M. V. (2015). International Journal on Recent and Innovation Trends in Computing and Communication Encryption and Decryption Using Rijndael Algorithm. Retrieved from http://www.ijritcc.org

[12] Anwar, S., Nugroho, I., & Ahmadi, A. (2015). Implementasi Kriptografi Dengan Enkripsi Shift Vigenere Chiper Serta Checksum Menggunakan CRC32 Pada Data Text. *Jurnal Sistem Informasi*, *2*.

[13] Latif, A. (2015). Implementasi Kriptografi Menggunakan Metode Advanced Encryption Standar (Aes) Untuk Pengamanan Data Teks. *Jurnal Ilmiah Mustek Anim Ha*, *4*(2), 163–172.

[14] Tullah, R., Dzulhaq, M. I., & Setiawan, Y. (2016). Perancangan Aplikasi Kriptografi File Dengan Metode Algoritma Advanced Encryption Standard (AES), *6*(2).

[15] K, G. G. P. U., & Erlanshari, A. (2016). IMPLEMENTASI METODE A DVANCED ENCRYPTION STANDARD (AES) DAN MESSAGE DIGEST 5 (MD5) PADA ENKRIPSI DOKUMEN (STUDI KASUS LPSE UNIB), *4*(3), 277–287.Indonesia, U. U. (2016). Jurnal Rekayasa Elektrika, *12*(1). https://doi.org/10.17529/jre.v12i1.2896

[16] Tulloh, A. R., Permanasari, Y., & Harahap, E. (2016). Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen Cryptography Advanced Encryption Standard (AES) for File Document Encryption sebagai agensi departemen perdagangan AS menetapkan sebuah standard kriptografi Standard (AES). *Prosiding Matematika*, *2*(2460–6464), 118–125.

[17] Mamun, A. A.-, Rahman, S. S. M., & Shaon, T. A. (2017). S ECURITY ANALYSIS OF AES AND E NHANCING ITS S ECURITY BY M ODIFYING S-B OX WITH AN A DDITIONAL B YTE, *9*(2), 69–88. https://doi.org/10.5121/ijcnc.2017.9206

[18] Rahman, M. T., Pinandito, A., & Pramukantoro, E. S. (2017). Perbandingan Performansi Algoritme Kriptografi Advanced Encryption Standard (AES) dan Blowfish pada Text di Platform Android, *1*(12), 1551–1559.

[19] Kunci, K. (2017). Aplikasi Enkripsi Pesan Teks Dengan Metode Advanced Encryption Standard Pada Ponsel Berbasis Android, 29–31.

KERTAS KERJA

Langkah-langkah dalam penelitian ini meliputi pengembangan perangkat lunak yang dijelaskan sebagai berikut yaitu:

1. Literatur Review
   Pada bagian ini penulis mereview tentang teori, temuan, dan bahan penelitian lainnya yang diperoleh dari bahan acuan untuk dijadikan landasan kegiatan penelitian untuk menyusun kerangka pemikiran yang jelas dari perumusan masalah yang ingin diteliti terdapat 10 artikel jurnal nasional, 5 artikel jurnal internasional dan 4 artikel prosiding internasional.
1. Analisi dan perancangan
   Bab ini membahas implementasi dan pengujian dan analisa hasil pengujian atau penelitian terhadap aplikasi Kriptografi Rijndael. Sehingga dapat diketahui apakah sistem tersebut mampu menyelesaikan permasalahan yang dihadapi dan sesuai dengan tujuan dari penelitian tugas akhir ini.
2. Source code
   Bab ini menjelaskan secara ringkas Bahasa pemrograman, lingkungan (system operasi) dan library yang dibutuhkan untuk eksekusi.
3. Skenario pengujian
   Pengujian sistem pendukung keputusan berikut menggunakan data uji berdasarkan data yang telah didapat dari aplikasi
4. Tahapan eksperimen
   Dalam tahap ini penulis melakukan pengujian dari aplikasi yang dibuat terhadap data yang telah disiapkan.
5. Hasil Semua Eksperimen
   Pengujian software Visual Studio dilakukan dengan menguji kinerja dari program penjadwalan apakah telah berfungsi sesuai dengan harapan dan juga memperlihatkan apakah telah layak sebagai user interface