Rancangan Perangkat Lunak Kriptografi Menggunakan Algortima AES dan Transposisi Cipher

Marius Leonardi, I Dewa Ayu Eka Yuliani
STMIK Pontianak;Jl. Merdeka Barat no. 372, (0561) 735555
Jurusan Teknik Informatika, STMIK Pontianak, Pontianak
e-mail: marius.leonardi@outlook.com, ekanesta@gmail.com

Abstrak

Pengaruh perkembangan ilmu komputer telah menjamah berbagai bidang, contohnya dalam bidang keamanan, Pertukaran informasi yang tidak aman dapat meningkatkan kerentanan terhadap akses suatu informasi yang bersifat pribadi atau rahasia. Dalam dunia informasi, terdapat data-data penting dan bersifat rahasia yang tidak boleh diketahui oleh umum. Penyadapan terhadap pesan atau informasi merupakan hal yang sangat merugikan bagi pengguna teknologi informasi saat ini. Enkripsi merupakan salah satu cara melindungi pesan atau data rahasia aman dari pihak tidak bertanggung jawab yang ingin mencuri informasi tersebut. Oleh sebab itu, dibutuhkan sebuah algoritma kriptografi yang kuat dalam menjaga kerahasiaan dan keaslian data.Advanced Encryption Standard (AES) merupakan algoritma kriptografi modern yang saat ini banyak digunakan untuk mengamankan data. AES (Advanced Encryption Standard) adalah lanjutan dari algoritma enkripsi standar DES (Data Encryption Standard) yang masa berlakunya dianggap telah usai karena faktor keamanan. Untuk meningkatkan keamanan maka dilakukan kombinasi enkripsi dengan Transposisi Cipher yang mengacak lagi enkripsi AES sehingga menjadi lebih kuat daripada enkripsi yang tidak memakai kombinasi sama sekali.

Kata kunci*—Enkripsi, AES, Transposisi Cipher*

Abstract

Influence Development of computer science has been touched in various fields, such as Security, Unsecure exchange of information increase chance vulnerability to access some information to be private or confidential is extremely harmful for users of information technology today. In the world of information,there are important data and confidential that should not be known by the public. Tapping on messages or information is very detrimental to current information technology users. Encryption is one way of protecting messages or confidential data safe from irresponsible which trying to steal the information. Therefore, it takes a strong cryptographic algorithms to maintain confidentiality and authenticity data. Advanced Encryption Standard (AES) is a modern cryptographic algorithms that are currently widely used to secure the data. AES (Advanced Encryption Standard) is a continuation of the standard encryption algorithms DES (Data Encryption Standard) that the validity period is deemed to have ended because of the safety factor. To improve the security then a combination of Transposition Cipher encryption with AES encryption that encodes again so that it becomes more powerfull rather than an encryption that don't use a combination at all.

Keywords*—Encryption, AES, Transposition CIpher*

1. PENDAHULUAN

Perkembangan teknologi informasi yang berkembang pesat saat ini salah satunya adalah komputerisasi dalam bidang media komunikasi. Berbagai perusahaan atau pihak-pihak lain telah memanfaatkan teknologi dalam berbagi informasi. Semakin berkembangnya pemanfaatan teknologi informasi maka kerahasiaan dan keamanan sangat penting dalam suatu sistem informasi, Pertukaran informasi yang tidak aman dapat meningkatkan kerentanan terhadap akses suatu informasi yang bersifat pribadi atau rahasia.

Penyadapan terhadap pesan atau informasi merupakan hal yang sangat merugikan bagi pengguna teknologi informasi saat ini. Informasi merupakan data yang telah diolah sehingga mempunyai nilai guna bagi penerimanya. Oleh karena itu sangat penting untuk mencegah pencurian informasi penting oleh pihak-pihak lain yang tidak berkepentingan sehingga adanya kemungkinan penyalahgunaan informasi dapat dihindari. Terdapat berbagai kasus dimana terjadinya penyadapan yang dilakukan oleh pihak tertentu untuk mendapatkan keuntungan dari informasi tersebut. Untuk mengatasi permasalahan tersebut maka informasi perlu di enkripsi untuk mencegah dari penyadapan baik dengan tujuan keamanan bersama, maupun untuk keamanan pribadi. Apabila enkripsi informasi dilakukan, maka keamanan informasi lebih dapat terjamin kerahasiannya. Enkripsi penting karena memungkinkan untuk melindungi informasi yang tidak ingin diakses orang lain. Pebisnis menggunakannya untuk melindungi rahasia perusahaan, pemerintah menggunakannya untuk mengamankan infom rmasi rahasia, dan banyak orang menggunakannya untuk melindungi informasi pribadi untuk menjaga terhadap hal-hal seperti pencurian identitas.

Usaha perlindungan data dapat dilakukan dengan berbagai cara, salah satunya dengan mengaplikasikan bidang kriptografi. Adanya kriptografi, data atau informasi dapat dienkripsi menjadi suatu bentuk yang tidak bisa dibaca atau tidak dimengerti isinya(Chipertext). Kriptografi awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan, namun pada pengertian modern kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data, dan otentifikasi entitas[1]. Ada beberapa metode kriptografi untuk membuat pesan rahasia antara lain mulai dari kriptografi klasik hingga kriptografi modern. Terdapat berbagai algoritma dipakai dalam membuat aplikasi kriptografi salah satunya algoritma AES. AES merupakan algoritma yang dikembangkan untuk menggantikan DES yang lama dan memiliki banyak kelemahan pada stuktur keamanan.

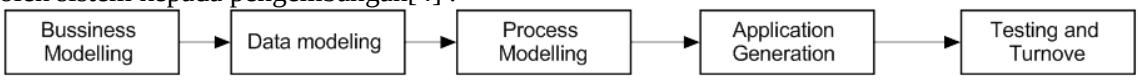
Dalam penelitian ini merancang sebuah perangkat lunak kriptografi algoritma advanced encryption yang dikombinasikan dengan algoritma Transposisi cipher. Advanced Encryption Standard (AES) dipublikasikan oleh National Institute of Standard and Techonology(NIST) pada tahun 2001 untuk menghindari kontoversi mengenai standard yang baru tersebut, sebagaimana pada pembuatan data encryption standard(DES) maka pada tahun 1997 NIST mengadakan sayembara terbuka untuk membuat standard algoritma kriptografi yang baru sebagai pengganti DES. Standard tersebut kelak diberi nama Advanced Encryption Standard(AES)[2]. Ada yang meragukan ketangguhan AES karena semua transformasi yang dilakukan dalam enkripsi AES mempunyai rumus aljabar yang elegan[3].

Pada proses enkripsi dan dekripsi, penulis menggabungkan kedua metode Transposisi Cipher dan AES yaitu pada saat proses pengoperasian enkripsi dan dekripsi algoritma AES disisipkan terlebih dahulu dengan proses algortima Transposisi Cipher kemudian di enkripsi kembali dengan AES. Program ini hanya dapat diakses oleh user kunci atau memiliki hak akses, pihak yang tidak memiliki hak akses tidak akan bisa membaca isi dari dokumen /pesan tersebut.

Dari penelitian ini, diharapkan mampu dapat menghasilkan keamanan yang kuat dan bermanfaat bagi pengguna dari program tersebut.

2. METODE PENELITIAN

Penelitian ini berbentuk eksperimental, yaitu melakukan cara melakukan enkripsi Algoritma AES dan transposisi Cipher. Pengumpulan data dilakukan dengan melakukan studi dokumentasi. Hasil Dari studi dokumentasi akan dipraktekan langsung dalam merancang aplikasi kriptografi. Metode perancangan perangkat lunak menggunakan *RAD (Rapid Application Development)*. Metode RAD memperjelas spesifikasi kebutuhan yang diperlukan oleh sistem kepada pengembangan[4] .

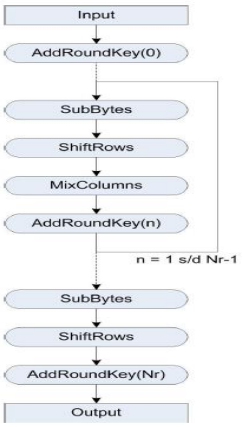


Gambar 1 Langkah-Langkah metode RAD

Metode pengujian yang digunakan adalah metode pengujian *blackbox*, yaitu pengujian yang memungkinkan perekayasa perangkat lunak mendapatkan serangkaian input yang sepenuhnya menggunakan semua persyaratan fungsional untuk suatu program[5]. Pembuatan aplikasi ini menggunakan bahasa pemograman Visual Bacis.NET.

Sistem yang dikembangkan secara garis besar adalah algoritma advanced encryption standard dengan menyisipkan algoritma vigenere cipher. Sebelum melakukan penyisipkan, perlu menganalisa setiap tahapan algoritma. Untuk tahapan algoritma AES adalah sebagai berikut:

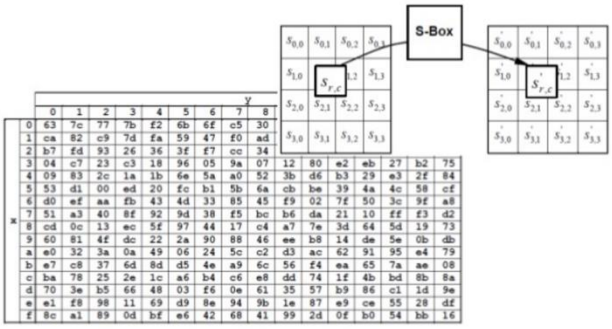
a. Proses Enkripsi AES



Gambar 2. Tahapan AES

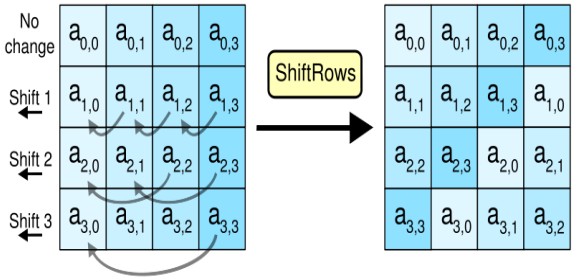
Perhitungan dari setiap tahapan AES adalah sebagai berikut :

a. AddRoundKey, melalukan XOR antara state awal (plainteks) dengan cipher key. Tahap ini juga sebagai initial round.
b. Putaran sebanyak Nr-1 kali. Proses yang dilakukan pada setiap putaran adalah:
   a. SubBytes, adalah subsitusi byte dengan menggunakan tabel subsitusi (S-Box)



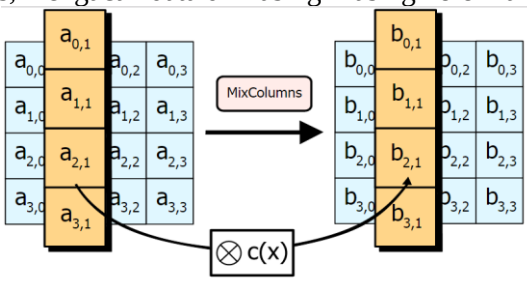
Gambar 3. SubBytes

b. ShiftRow, dilakukan melalui permutasi byte-byte data dari kolom array yang berbeda,



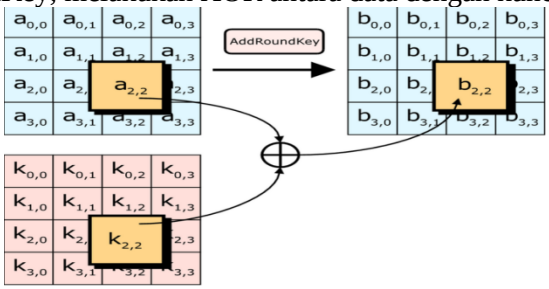
Gambar 4. ShiftRows

c. MixColumns, mengacak data di masing-masing kolom array state.



Gambar 5. MixColumns

d. AddRoundKey, melakukan XOR antara data dengan kunci



Gambar 6. AddroundKey

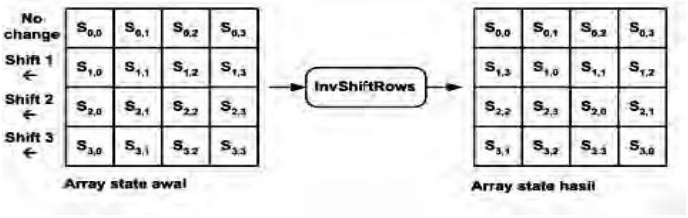
c. Final round, proses untuk putaran terakhir :
   a. SubBytes
   b. ShiftRows
   c. AddRoundKey

b. Proses Dekripsi AES

Transformasi cipher dapat dibalikkan dan diimplementasikan dalam arah yang berlawanan untuk menghasilkan inverse cipher yang mudah dipahami untuk algoritma AES.Transformasi byte yang digunakan pada invers cipher adalah *InvShiftRows*, InvSubBytes, InvMixColumns, dan AddRoundKey. Algoritma dekripsi dapat dilihat pada skema berikut ini :

a. InvShiftRows

InvShiftRows adalah transformasi byte yang berkebalikan dengan transformasi ShiftRows. Pada transformasi *InvShiftRows*, dilakukan pergeseran bit ke kanan sedangkan pada ShiftRows dilakukan pergeseran bit ke kiri. Ilustrasi transformasi *InvShiftRows* terdapat pada gambar berikut.



Gambar 7. InvShiftRows

b. InvSubBytes

InvSubBytes juga merupakan transformasi bytes yang berkebalikan dengan transformasi SubBytes. Pada *InvSubBytes*, tiap elemen pada state dipetakan dengan menggunakan tabel Inverse S-Box. Tabel Inverse S-Box akan ditunjukkan dalam tabel berikut.

HEX		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	52	09	6a	D5	30	36	A5	38	Bf	40	A3	9e	81	F3	D7	Fb
	1	7c	E3	39	82	9b	2f	Ff	87	34	8e	43	44	C4	De	E9	Cb
	2	54	7b	94	32	A6	C2	23	3d	Ee	4c	95	0b	42	Fa	C3	4e
	3	08	2e	A1	66	28	D9	24	B2	76	5b	A2	49	6d	8b	D1	25
	4	72	F8	F6	64	86	68	98	16	D4	A4	5c	Cc	5d	65	B6	92
	5	6c	70	48	50	Fd	Ed	B9	Da	5e	15	46	57	A7	8d	9d	84
	6	90	D8	Ab	00	8c	Bc	D3	0a	F7	E4	58	05	B8	B3	45	06
	7	d0	2c	1e	8f	Ca	3f	0f	02	C1	Af	Bd	03	01	13	8a	6b
	8	3a	91	11	41	4f	67	Dc	Ea	97	F2	Cf	Ce	F0	B4	E6	73
	9	96	Ac	74	22	E7	Ad	35	85	E2	F9	37	E8	1c	75	Df	6e
	a	47	F1	1a	71	1d	29	C5	89	6f	B7	62	0e	Aa	18	Be	1b
	b	fc	56	3e	4b	C6	D2	79	20	9a	Db	C0	Fe	78	Cd	5a	F4
	c	1f	Dd	A8	33	88	07	C7	31	B1	12	10	59	27	80	Ec	5f
	d	60	51	7f	A9	19	B5	4a	0d	2d	E5	7a	9f	93	C9	9c	Ef
	e	A0	E0	3b	4d	Ae	2a	F5	B0	C8	Eb	Bb	3c	83	53	99	61
	f	17	2b	04	7e	ba	77	D6	26	E1	69	14	63	55	21	0c	7d

Gambar 8. InvSuBytes

c. InvMixColumns

Setiap kolom dalam state dikalikan dengan matrik perkalian dalam AES. Perkalian dalam matrik dapat dituliskan :

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 0B & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

Gambar 9. InvMixColumns

Untuk Vigenere Cipher pada penelitian ini bisa mengenkripsi semua karakter pada plaintext dari simbol sampai angka pun juga bisa. Berbeda dengan Vigenere cipher yang lain, vigenere cipher pada penelitian ini digunakan untuk disisipkan ke dalam algoritma Advanced Encryption Standard sehingga diperlukan pengenkripsian semua karakter yang dibutuhkan untuk penggabungan. Setiap huruf disandikan dengan menggunakan baris yang berbeda-beda, sesuai kata kunci yang diulang. Enkripsi (penyandian) dengan Vigenere cipher juga dapat dituliskan secara matematis, dengan menggunakan penjumlahan dan operasi modulus, yaitu:

$C_i = (P_i + K_i) \bmod 256$

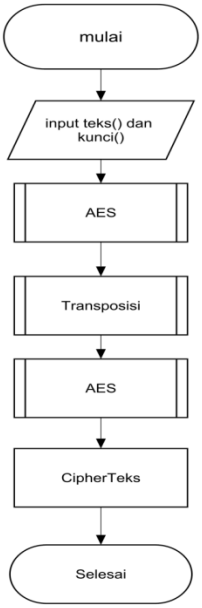
Atau C = P + K kalau jumlah dibawah 256 dan -256 kalau hasil jumlah diatas 256 dan dekripsi,

$C_i = (P_i - K_i) \bmod 256$
Atau P = C- K kalau hasilnya positif dan +256 kalau hasil pengurangan minus
Rumus enkripsi vigenere cipher :
$C_i = (P_i + K_i) \bmod 256$ (1)
Rumus dekripsi vigenere cipher:
$C_i = (P_i - K_i) \bmod 256$ (2)
Dimana:
C_i= nilai decimal karakter ciphertext ke-i
P_i= nilai decimal karakter Plaintext ke-i
K_i= nilai decimal karakter Kunci ke-i

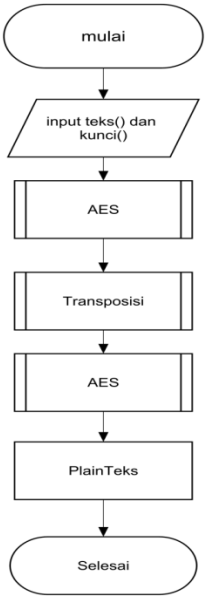
Analisis dan perancangan aplikasi dalam penelitian ini menggunakan model prototipe. Untuk tahap pengumpulan kebutuhan kebutuhan sistem akan dianalisis melalui studi dokumentasi. Perancangan cepat akan dilakukan untuk kemudian dievaluasi apakah sudah memenuhi kebutuhan yang dianalisis sebelumnya. Pengujian yang digunakan adalah pengujian *black-box* yaitu pengujian perilaku yang berfokus pada persyaratan fungsional perangkat lunak[6].

3. HASIL DAN PEMBAHASAN

Berikut adalah penjelasan pada masing – masing bagian yang terdapat dalam sistem: a) pemilihan file yang akan dilakukan enkripsi atau dekripsi; b) jika telah selesai melakukan enkripsi maupun dekripsi, data tersebut dapat disimpan dalam bentuk file. Untuk tahapan enkripsi kriptografi advanced encryption standard yang dikombinasikan dengan Transposisi Cipher adalah sebagai berikut:

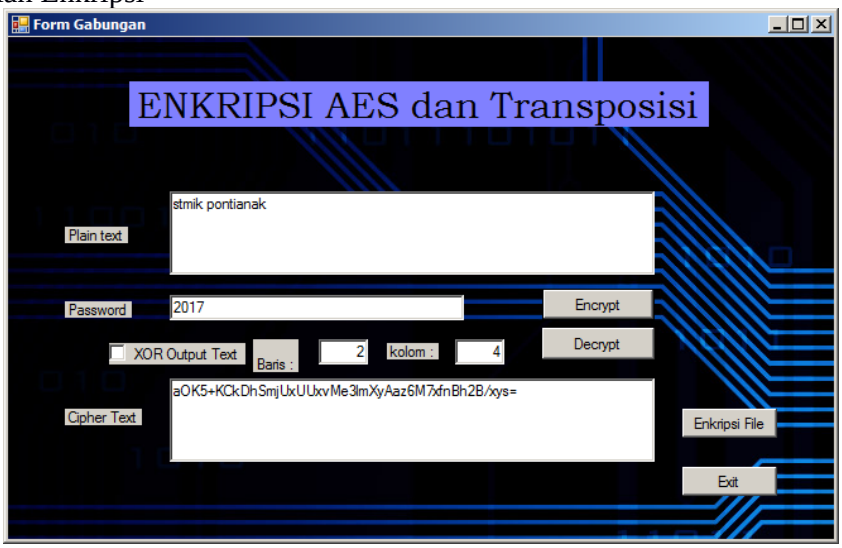


Gambar merupakan tahap enkripsi yang digunakan untuk menghasilkan ciphertext. Proses tersebut dimulai dari pemasukan plaintext dan kunci yang selanjutnya dilakukan enkripsi sesuai urutan fungsi-fungsi yang ada. Untuk hasilnya berupa sebuah ciphertext yang nantinya dapat diterjemahkan kembali kedalam bentuk plaintext. Berikut adalah tahapan kembalinya ciphertext ke plaintext(dekripsi):



Gambar merupakan tahap dekripsi yang digunakan mengembalikan ciphertext ke dalam bentuk yang dapat dibaca.Gambar tahap memiliki tahap terbalik tahap enkripsi.Berikut merupakan flowchart yang menjelaskan proses dari enkripsi dan dekripsi pesan:

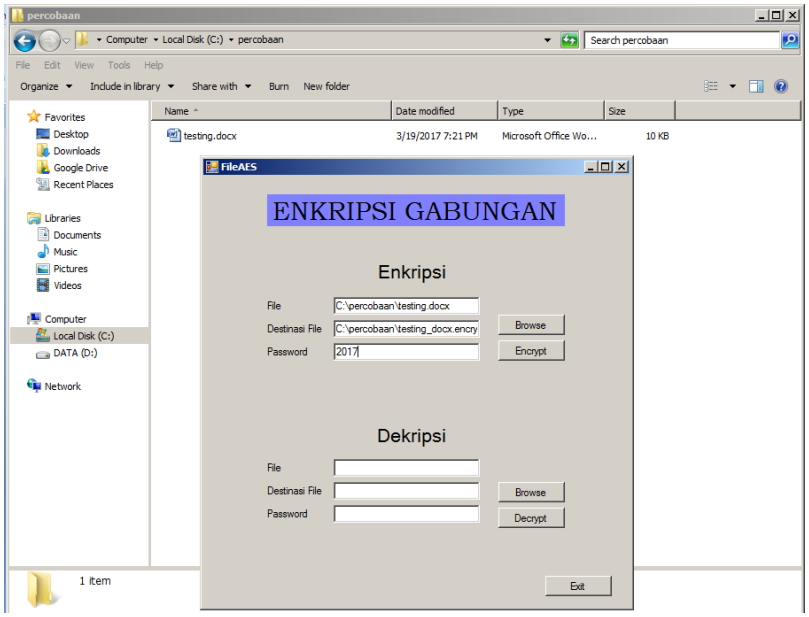
a. Pengujian Enkripsi



Gambar 10. Hasil pengujian Enkripsi Text

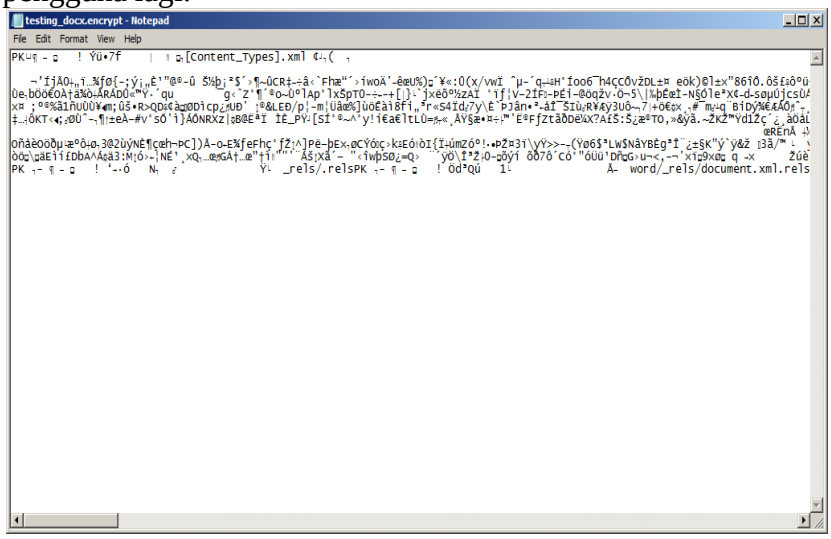
Berikut merupakan hasil dari proses enkripsi: a) Untuk setiap test, akan diambil setiap huruf dan panjang dari test tersebut; b) test tersebut akan dihitung panjang teks. Hasil pengujian digunakan untuk menguji kemampuan sistem untuk melakukan penyandian. Pengujian dapat dilakukan dengan memasukan pesan dan kunci, pesan dan kunci dapat berupa karakter apa saja untuk dilakukan enkripsi

Hasil penelitian ini bukan hanya melakukan enkripsi-dekripsi teks saja melainkan pada file. File terbentuk dari kumpulan byte yang disatukan. Berbeda dengan enkripsi-dekripsi teks, bytes dalam file tersebut dijadikan ke dalam bentuk hexa untuk dilakukan proses penyandian. Byte yang sudah disandikan akan disusunkan kembali ke dalam bentuk file. Berikut adalah pengujian enkripsi file pada file testing.docx:



Gambar 11. Pengujian Enkripsi File

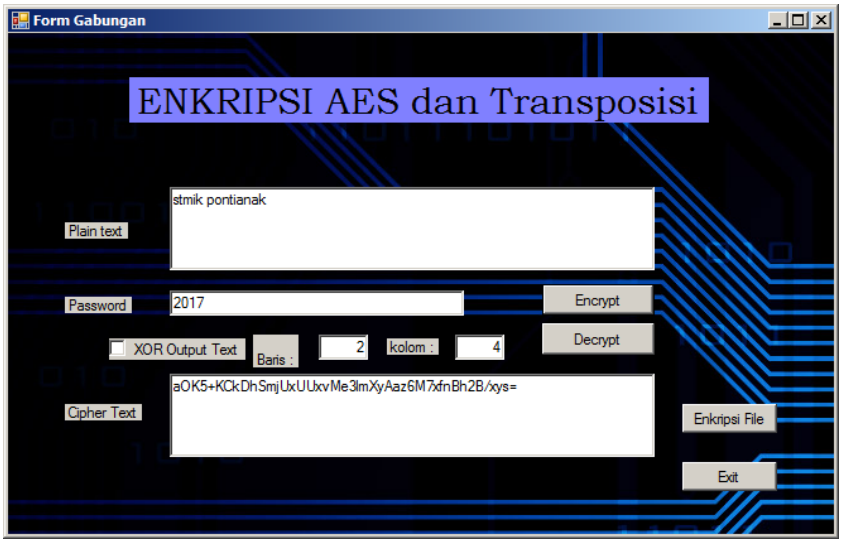
Gambar diatas menunjukkan bahwa ada sebuah file DOCX yang bernama testing.docx yang akan dienkripsi. Berikut ini adalah hasil file testing.Docx. file yang sudah dipilih nantinya akan dienkripsi menjadi file yang berbentuk .encrypt yang tidak dapat lagi dibaca oleh pengguna lagi.



Gambar 12. Hasil Enkripsi File

Gambar merupakan hasil enkripsi file dan dibuka dengan menggunakan notepad. Jika file tersebut diubah menjadi file docx kembali dan dibuka menggunakan Microsoft word dan hasilnya tidak dapat dibuka. File yang dibuka dengan notepad menghasilkan huruf-huruf yang tidak dapat dibaca dari hasil enkripsi file yang menghasilkan huruf seperti gambar diatas.

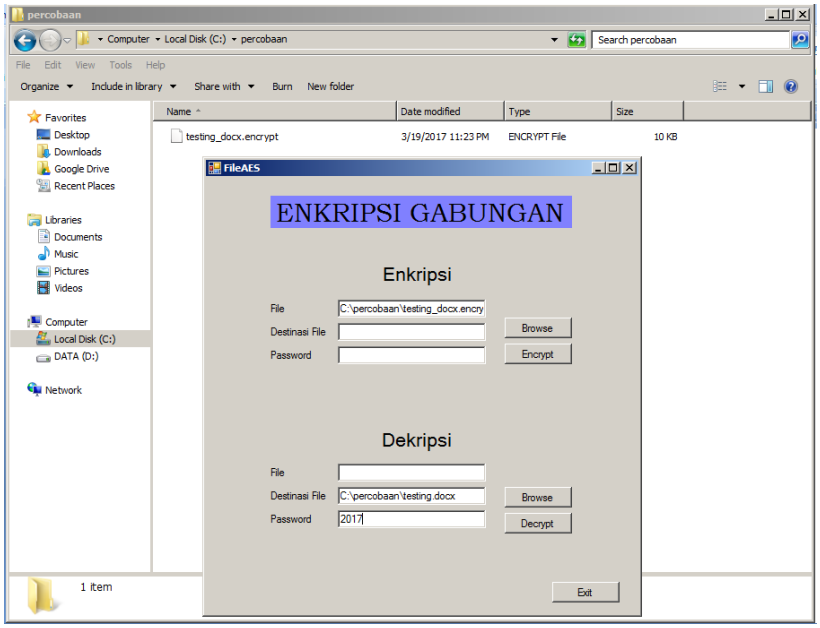
b. Pengujian Dekripsi



Gambar 13. Hasil pengujian Dekripsi Text

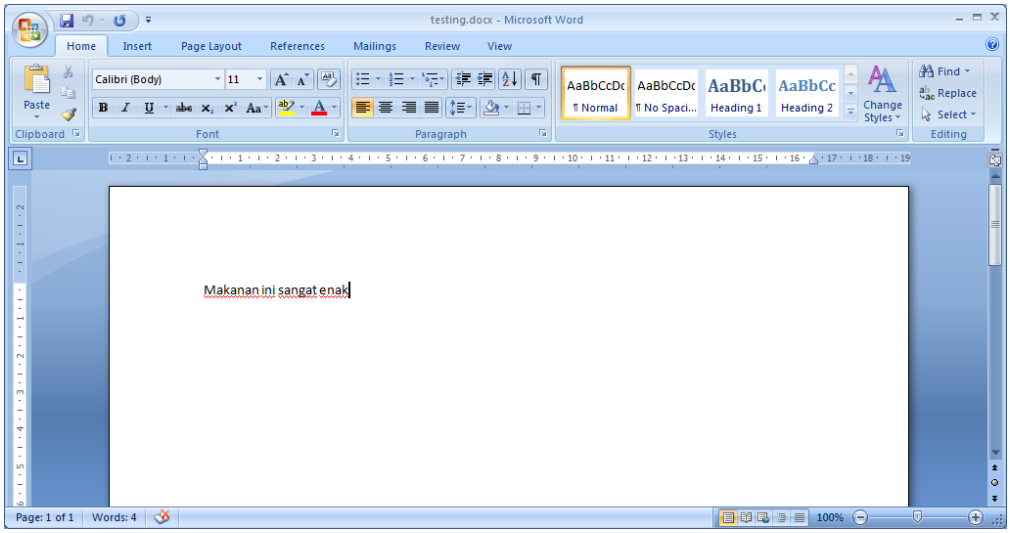
Berikut merupakan penjelasan dari proses dekripsi: a) ciphertext tersebut tersusun atas teks hexa, yang dimana nantinya sistem akan mengambil 2 karakter dari ciphertext tersebut untuk dijadikan hexa; b) selanjutnya, sistem akan mengikuti alur setiap prosesnya. Hanya dengan memberikan kunci yang benar saja maka dekripsi baru bisa dilakukan. Dekripsi dialkukan dengan pertama mengdekripsi dengan algoritma AES, selanjutnya malakukan dekripsi Transposisi cipher dan kemudian didekripsi kembali dengan AES untuk menghasilkan kembali plain teks tersebut

Berikut adalah gambar pengujian dekripsi file pada file testing.docx.encrypt yang akan di dekripsi kembali menjadi file kembali seperti semula dan dapat dibaca kembali oleh pengguna.



Gambar 14. Pengujian Dekripsi File

Gambar diatas menunjukkan bahwa ada sebuah file ENCRYPT yang bernama testing.docx.encrypt yang akan didekripsi. Berikut ini adalah hasil file testing.Docx.



Gambar 15. Hasil Pengujian Dekripsi File

Gambar merupakan hasil dekripsi file dan dibuka dengan menggunakan Microsoft word. Gambar diatas menunjukkan bahwa file tersebut berhasil didekripsi kembali dan tidak mengalami perubahan sama sekali.

Pengujian perangkat dilakukan untuk menunjukkan hasil perancangan. Hasil pengujian ditunjukkan dibawah ini:

Data masukan	Yang diharapkan	Pengamatan	Kesimpulan pengujian
Mencoba semua form pada program	Menampilkan semua form yang dibuka	Semua form pada progam tampil sesuai yang diharapkan	Pass
Pengujian pengisian data pada form transposisi, AES dan Kombinasi pada textbox dan kunci Text : isi Kunci : tidak diisi Text : isi Kunci : isi Text : tidak diisi Kunci : tidak diisi Text : tidak diisi Kunci : diisi	Akan melakukan proses enkripsi maupu dekripsi Menampilkan konfirmasi masukkan kunci. Proses enkripsi maupun dekripsi dilakukan. Tidak terjadi proses apapun. Tidak terjadi proses apapun	Menampilkan proses hasil enkripsi maupun dekripsi Enkripsi berjalan tanpa kunci Enkripsi maupun dekripsi jalan. Terjadi proses enkripsi. Terjadi proses enkripsi.	Pass
Pengujian password dekripsi	Akan Melakukan dekripsi	Menampilkan hasil dekripsi	Pass

Kunci : sesuai Kunci : tidak sesuai	Plainteks muncul Plainteks tidak muncul	Plainteks muncul Plainteks tidak muncul	
Pengujian form about	Menampilkan form about	Menampilkan form about	Pass

4. KESIMPULAN

Berdasarkan dari hasil dan pembahasan yang telah didapatkan maka dapat ditarik kesimpulan bahwa kriptografi AES yang dikombinasikan dengan Transposisi cipher dapat untuk diimplementasikan dalam mengamankan informasi lebih baik disbanding hanya dengan menggunakan AES. Dengan dikombinasikannya kedua algoritma ini maka kekuatan keamanan menjadi lebih baik dari biasanya.

5. SARAN

Sistem untuk kedepannya bisa melakukan penyandian pada data atau pesan yang tidak hanya dikombinasikan dari tetapi menggabungkan kedua algoritma menjadi satu dengan menggabungkan kelebihan-kelebihan kedua algoritma menjadi satu maka akan menjadi lebih kuat dari biasanya yang hanya dikombinasi.

UCAPAN TERIMA KASIH

Terima kasih disampaikan kepada seluruh dosen, teman dan seluruh pihak yang telah memberikan berbagai masukan terhadap penelitian yang sudah dilaksanakan, serta pemberian berbagai ilmu yang sangat bermanfaat. Dan juga tersedianya fasilitas-fasilitas yang ada untuk mendukung terhadap penelitian ini.

DAFTAR PUSTAKA

[1] Rifki Sadikin. 2012. Kriptografi Untuk Keamanan Jaringan. Yogyakarta:Andi
[2] Dony Ariyus. 2008. Pengantar Ilmu Kriptografi. Jogjakarta,Indonesia: Penerbit Andi.
[3] Kromodimoeljo, S. 2010. Teori dan Aplikasi Kriptografi.SPK IT Consulting.
[4] A. S., Rosa dan Shalahuddin, M. 2013. *Rekayasa Perangkat Lunak Terstruktur Dan Berorientasi Objek*. Informatika. Bandung.
[5] A. S., Rosa dan Shalahuddin, M. 2013. *Rekayasa Perangkat Lunak Terstruktur Dan Berorientasi Objek*. Informatika. Bandung.
[6] Shalahudin, A.S. Rosa., 2013, *Rekayasa Perangkat Lunak Terstruktur dan Berorientasi Objek*, Penerbit Informatika, Bandung.