IMPLEMENTASI ALGORITMA *ADVANCED ENCRYPTION STANDARD* (AES) SEBAGAI SISTEM PENGAMANAN DATA PENGARSIPAN PADA PERPUSTAKAAN DIGITAL DI PUSLITBANG GEOLOGI KELAUTAN

Zaenal Firdaus[1] Didit Andri Jatmiko[2]

[1]Teknik Informatika-Universitas Komputer Indonesia
Jalan Dipatiukur No 112-116 Bandung. 40312
E-mail :jenalfirdaus@email.unikom.ac.id[1] didit@email.unikom.ac.id[2]

ABSTRAK

Puslitbang Geologi Kelautan merupakan Pusat Penelitian dan Pengembangan Geologi Kelautan yang di kelola instansi pemerintah di bawah departemen ESDM. Pada awal berdirinya, PPGL didukung oleh empat bidang teknis, yaitu : Bidang Geologi Kelautan, Bidang Geofisika Kelautan, Bidang Sarana Operasi Kelautan, Bidang Manajemen Informasi dan Bagian Umum, dengan jumlah sumber daya manusia 222 orang. Sarana dan prasarana yang dimiliki sebagian berasal dari P3G.

Beberapa permasalahan yang terjadi di Puslitbang Geologi Kelautan adalah keamanan data. Data-data hasil laporan penelitian lapangan maupun data penting lainnya mudah diakses oleh semua bagian dalam perusahaan yang tidak mempunyai hak untuk mengetahuinya. Oleh karena itu dibutuhkan suatu sistem untuk melindungi data dari pihak-pihak yang tidak bertanggung jawab.Kriptografi merupakan salah satu teknik untuk mengamankan data. Kriptografi menggunakan algoritma *Advanced Encryption Standard* memiliki ukuran blok dan kunci yang sama, yaitu 128 *bit*, 192 *bit*, dan 256 *bit* untuk proses enkripsi dan dekripsi.Sistem keamanan data ini dibangun untuk membantu melindungi data-data penting perusahaan, seperti data hasil laporan penelitian lapangan maupun data pribadi perusahaan. Kesimpulan yang diperoleh berdasarkan implementasi dan pengujian yang dilakukan kepada pengguna, sistem ini mampu memberikan pengamanan yang kuat pada data, melindungi data dan mudah digunakan.

Kata Kunci : ***Kriptografi, Advanced Encryption Standard, Algoritma, Enkripsi, Dekripsi***

PENDAHULUAN

1.1 Latar Belakang

Puslitbang Geologi Kelautan merupakan Pusat Penelitian dan Pengembangan Geologi Kelautan yang di kelola instansi pemerintah di bawah departemen ESDM. Pada awal berdirinya, PPGL didukung oleh empat bidang teknis, yaitu : Bidang Geologi Kelautan, Bidang Geofisika Kelautan, Bidang Sarana Operasi Kelautan, Bidang Manajemen Informasi dan Bagian Umum, dengan jumlah sumber daya manusia 222 orang. Sarana dan prasarana yang dimiliki sebagian berasal dari P3G.

Perpustakaan digital di Pulitbang salah satunya bagian sarana pelayanan publik yang berada di tempat instansi perusahaan puslitbang geologi kelautan khususnya pengarsipan, proses pengarsipan dilakukan secara manual/konvensional, misalnya dengan menyimpan laporan-laporan dalam sebuah map yang kemudian disimpan di dalam lemari arsip. Tentunya cara seperti ini tidak efektif dan efisien karena semakin banyak laporan yang akan diarsipkan maka akan semakin besar juga ruang yang dibutuhkan untuk menyimpan arsip tersebut.

Pada saat ini di P3GL menghadapi masalah dalam keamanan laporan, laporan bebas diakses oleh berbagai pihak dan tidak ada pengamanan dalam laporan laporan antara lain laporan penelitian, pemetaan, inventaris, dan penyelidikan sehingga orang bisa membaca dan merubah karna belum ada aplikasi untuk mengenkripsi file,maka dari itu diperlukan suatu keamanan yang baik sehingga laporan yang terdapat pada komputer menjadi lebih aman.

Berdasarkan permasalahan yang ada maka diperlukan sebuah aplikasi untuk mengamankan laporan pengarsipan di instansi P3GL tersebut. Dalam hal ini khususnya untuk membatasi pihak lain untuk melihat laporan agar mengurangi penggunaan tanpa izin oleh P3GL. Salah satu caranya adalah membuat data informasi tersebut tidak terbaca / tidak dapat dimengerti oleh pihak lain. Untuk hal itu penelitian kali ini akan

menggunakan pengamanan dengan teknik kriptografi yang dapat membuat data informasi digital tidak terbaca menggunakan algoritma *Advanced Encryption Standard* (AES).

Dengan demikian maka penelitian ini akan berfokus untuk membangun aplikasi keamanan sistem yang berjudul "Implementasi Algoritma Advanced Encryption Standard (AES) Sebagai Sistem Pengamanan Data Pengarsipan Pada Perpustakaan Digital di Puslitbang Geologi Kelautan".

1.2 Identifikasi Masalah

Dari latar belakang yang telah dijabarkan di atas masalah yang dihadapi yaitu :

1. Belum ada pembatasan hak akses untuk melihat pengarsipan data digital.
2. Bagaimana menerapkan algoritma *Advanced Encryption Standard* (AES) dalam pengenkripsian data rahasia sehingga data yang telah dienkripsi tidak dapat dibaca atau dimengerti oleh pihak lain.

1.3 Maksud dan Tujuan

Berdasarkan penelitian yang dibahas, maka maksud dari penulisan tugas akhir ini yaitu menerapkan algoritma advanced encryption standard (AES) sebagai sistem pengamanan data pengarsipan pada perpustakaan digital. Sedangkan tujuan dari penelitian ini adalah

1. Membuat pembatasan hak akses untuk melihat pengarsipan data digital.
2. Membuat sebuah aplikasi yang dapat melakukan enkripsi dan dekripsi data dengan menggunakan algoritma *Advanced Encryption Standard* yang akan digunakan untuk mengamankan data penting sebuah instansi pemerintahan di Puslitbang Geologi Kelautan.

1.4 Batasan Masalah

Dalam penyelesaian proposal tugas akhir ini diberikan batasan masalah agar tujuan dan sasaran yang diinginkan dapat tercapai. Adapun batasan masalah sebagai berikut :

1. Format Laporan yang bisa dilakukan enkripsi yaitu .pdf
2. Sebelum data disembunyikan terlebih dahulu dilakukan penyandian dengan password yang dikonversi menjadi byte menggunakan SHA-1 kemudian file dienkripsi menggunakan algoritma AES (Advance Encryption Standard) 128 bit.
3. Proses otentikasi password menggunakan fungsi hash SHA-1.
4. Sistem ini akan menghasilkan sebuah chipertext dengan format file .pdf.
5. Sistem berbasis *website.* Menggunakan PHP, Html dan *library* pembuatan web lainnya.

2. ANALISIS PERANCANGAN DAN IMPLEMENTASI

2.1 Analisis Sistem

Analisis sistem merupakan suatu tahapan yang bertujuan untuk mengetahui dan mengamati apa saja yang terlibat dalam suatu sistem. Pembahasan yang ada pada analisis sistem ini yaitu analisis masalah, analisis algoritma, analisis kebutuhan non-fungsional, dan analisis kebutuhan fungsional.

2.1.1 Analisis Masalah

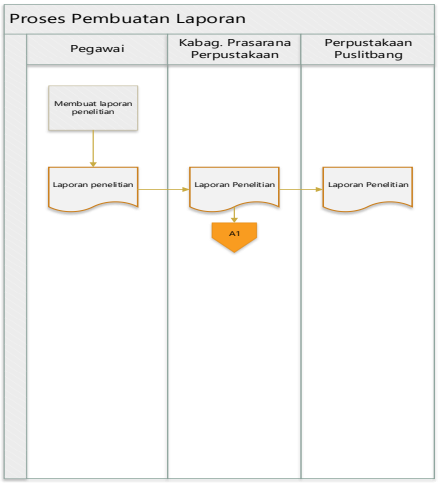
Analisis masalah adalah tahap penjabaran masalah yang ada sebelum sistem ini dibangun dan bertujuan untuk membantu pembangunan aplikasi kriptografi ini. Berikut adalah penjabaran dari masalah – masalah yang ada antara lain sebagai berikut :

1. Belum terdapat pembatasan hak akses untuk melihat data file laporan pengarsipan hasil penelitian dari pihak Puslitbang Geologi Kelautan. Hal ini mengakibatkan orang lain yang tidak memiliki kepentingan dapat melihat dan menyalahgunakan data file laporan tersebut.
2. Sebuah file laporan asli yang diserahkan tentu bisa dilihat berkali-kali dan ini mengakibatkan orang lain yang tidak bertanggung jawab dapat menyalahgunakan laporan tersebut.

2.1.2 Analisis Sistem yang Sedang Berjalan

Berdasarkan hasil pengamatan dan wawancara langsung didapatkan prosedur yang dilakukan Puslitbang Geologi Kelautan dalam sistem pengamanan data laporan pengarsipan pada Perpustakaan Digital. Secara garis besar terdapat beberapa tahapan yang dilakukan seperti berikut :

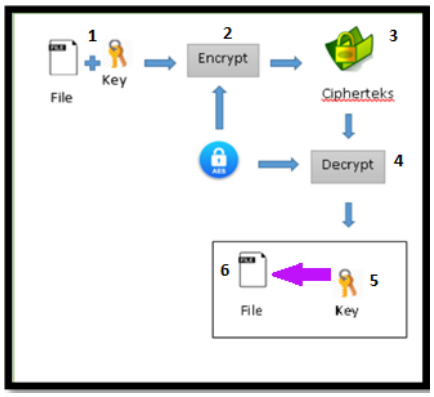
1. Pegawai puslitbang membuat hasil laporan penelitian yang telah dikerjakan selama bertugas diluar kota bandung.
2. Dokumen hasil laporan penelitian tersebut di cetak untuk diarsipkan ke Perpustaakan di Puslitbang Geologi Kelautan.
3. Pegawai puslitbang menyerahkan dokumen hasil laporan penelitian ke perpustakaan Puslitbang Geologi Kelautan.
4. Kabag prasarana Perpustakaan Puslitbang menerima dokumen laporan penelitian tersebut.



Gambar 1. Analisis Sistem yang sedang berjalan

2.1.3 Analisis Sistem yang dibangun

Sistem yang dibangun adalah sebuah sistem yang dapat melakukan kriptografi terhadap file dokumen. Proses kriptografi ini dilakukan agar file dokumen hasil laporan penelitian tidak bisa dilihat/dibaca menggunakan sistem pembuka file. Hal ini bisa dilakukan dengan asumsi bahwa setiap file dokumen yang akan telah dikenakan algoritma kriptografi akan mengalami pertambahan nilai sehingga file tidak dapat dibaca oleh sistem pembuka file biasa. Untuk lebih jelasnya proses yang akan terjadi dalam aplikasi yang akan dibangun adalah sebagai berikut :



Gambar 2. Analisis Sistem yang dibangun

Analisis sistem yang dibangun merupakan gambaran lengkap Analisis sistem yang akan dibangun. Sistem yang dibangun adalah sebagai berikut:

1. Pegawai puslitbang membangkitkan kunci privat dan kunci publik. Kunci privat disimpan pegawai dan kunci privat harus dijaga dengan baik karena kunci ini akan digunakan untuk proses dekripsi. Jika kunci ini berhasil didapatkan oleh pihak lain maka file akan mudah didekripsi sehingga laporan penelitian bisa dilihat oleh pihak yang tidak berkepentingan.
2. Kunci publik yang telah dibangkitkan ditahap pertama akan dikirimkan ke kabag prasarana puslitbang. Kunci ini berguna untuk melakukan proses enkripsi file dokumen. Pengiriman ini bisa dilakukan melalui jaringan lain diluar aplikasi. Kunci ini sifatnya aman karena jika kunci publik berhasil diambil maka pihak lain tidak dapat melakukan proses dekripsi karena proses dekripsi hanya menggunakan kunci privat.
3. Tahapan ketiga adalah ketika kunci publik telah didapatkan oleh kabag prasarana puslitbang akan melakukan pencarian file dokumen.
4. Setelah file dan kunci siap maka keduanya akan dimasukkan kedalam sistem enkripsi. Pada proses ini akan file dienkripsi dengan menyisipkan nilai pembatas dekripsi pada salah satu indeks *array byte*. Pada proses enkripsi ini akan menghasilkan suatu file dengan format .pdf.
5. Ketika proses enkripsi telah dilakukan dan menghasilkan file terenkripsi maka selanjutnya pihak perusahaan akan mengirimkan file terenkripsi tersebut kepada kabag prasarana puslitbang.
6. File terenkripsi yang telah sampai pada kabag prasarana puslitbang akan digunakan pada proses dekripsi. Dengan menggunakan kunci privat yang telah disimpan sebelumnya dan file terenkripsi tersebut maka proses dekripsi dapat dilakukan. Proses dekripsi ini akan mengembalikan file terenkripsi menjadi file dokumen semula.

2.1.4 Analisis Proses Enkripsi *Advanced Encryption Standard*(AES)

Proses enkripsi algoritma *AES* pada ronde 0 dan ronde 1. Misalkan plainteks dan kunci yang digunakan adalah contoh kasus seperti berikut yang sudah ditambahkan data *dammy*:

Plainteks : “UNIKOM9807645317”
Kunci : “ADMIN09512345678”

Langkah pertama yang dilakukan adalah mengubah plainteks dan kunci diatas menjadi bentuk *hexadecimal* dimana proses selanjutnya semua akan menggunakan bentuk *hexadecimal*. Hasil konversi akan menjadi seperti ini:

Plainteks : “40 45 44 49 20 41 4C 59 41 4E 54 4F 32 30 31 36”
Kunci : “52 49 4A 4E 44 41 45 4A 31 32 33 34 35 36 37 38”

Setelah menkonversi plainteks dan kunci ke dalam hexadecimal, maka kita akan susun plainteks dan kunci ke dalam bentuk matriks 4x4 seperti gambar dibawah:

44	20	41	32
45	41	4E	30
44	4C	54	31
49	59	4F	36

52	44	31	35
49	41	32	36
4A	45	33	37
4E	4C	34	38

Sebelum memasuki initial round atau round 0, kita terlebih dahulu harus mencari round key untuk tiap - tiap ronde. Pada ronde 0, subKey-nya sama dengan kunci yang pertama kali diinput. Pada ronde 0 plainteks akan melalui proses AddRounKey dimana pada tahap ini terjadi perhitungan XOR antara plainteks dengan kunci.
Proses XOR terjadi terhadap masing - masing cell pada matriks diatas, contoh matriksTeks[1,1] XOR matriksKunci[1,1] dan matriksTeks[2,1] XOR matriksKunci[2,1], dan seterusnya. Dibawah ini akan disimulasikan proses XOR antara baris ke-1 kolom ke-1 pada masing - masing matriks.

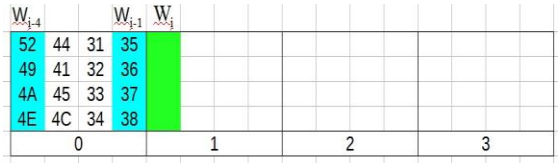
Baris ke-1 kolom ke-1 dari matriks plainteks : 44

Baris ke-1 kolom ke-1 dari matriks kunci : 52

Untuk melakukan XOR terlebih dahulu ubah bentuknya dari hexa ke bentuk biner sehingga seperti dibawah ini.
Baris ke-1 kolom ke-1 dari matriks plainteks (biner 8 bit) : 01000100
Baris ke-1 kolom ke-1 dari matriks kunci (biner 8 bit) : 01010010
Selanjutnya membandingkan kedua parameter tersebut *bit* per *bit* sesuai dengan dijelaskan pada tabel 2.2 sehingga menghasilkan

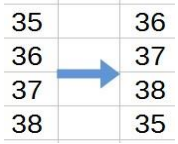
0	1	0	0	0	1	0	0	
0	1	0	1	0	0	1	0	⊕
0	0	0	1	0	1	1	0	

Gambar 3. Analisis Matrik AES



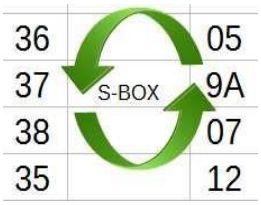
Gambar 4. Analisis Matrik AES2

Untuk memperoleh kolom ke-i dari matriks 4x4 diperlukan kolom ke i-4 dan i-1 dari *round key* yang telah ada. Seperti pada tabel diatas, untuk memperoleh kolom pertama dari *subKey* ke-1 diperlukan kolom pertama dan ke-4 dari *subKey* ke-0.
Cara mendapatkannya adalah seperti berikut:
Khusus kolom pertama pada tiap *round key* cara perhitungannya berbeda dengan cara perhitungan pada kolom 2, 3 dan 4. Pertama, ambil kolom W_{i-1} kemudian *cell* paling atas dipindah ke *cell* paling bawah atau istilah *RotWord*.



Gambar 5. Analisis Matrik AES3

Setelah itu hasilnya disubsitusi dengan S-Box dimana tata cara substitusinya sudah dijelaskan pada bagian 3.1.2.1. Hasil substitusi dengan S-Box menjadi seperti berikut :



Gambar 6. Analisis Matrik AES4

Setelah disubstitusi, maka hasil tersebut akan di-XOR dengan kolom W_{i-4} dan kolom pertama dari tabel *Rcon* dimana terdapat pada bagian 3.1.2.5. Tentunya tata cara XOR juga *cell* terhadap *cell* yang urutan baris dan kolomnya sama. Hasil XOR terlihat pada gambar dibawah.

52		05		01		56
49	⊕	9A	⊕	00	→	D3
4A		07		00		4D
4E		12		00		D8

Gambar 7. Analisis Matrik AES5

Setelah diperoleh kolom pertama dari *subKey* ke-1 maka tabel *subKey* akan terlihat seperti berikut.

W_{i-4}				W_{i-1}	W_i		
52	44	31	35	56			
49	41	32	36	D3			
4A	45	33	37	4D			
4E	4C	34	38	D8			
0				1		2	3

Gambar 8. Analisis Matrik AES6

Sekarang kita akan mencari kolom ke-2 dari *subKey* ke-1, dimana juga diperlukan kolom i-1 dan i-4 dari tabel *subKey*. Cara mencari kolom ke-2 lebih sederhana dibandingkan dengan cara mencari kolom pertama, cukup men-XOR-kan kolom i1 dan i-4 saja. Hasilnya akan seperti ini.

56		44		12
D3	⊕	41	→	92
4D		45		08
D8		4C		94

Gambar 9. Analisis Matrik AES7

Seterusnya untuk mendapatkan kolom ke-3 dan ke-4 caranya sama dengan kolom yang ke-2. Sehingga hasil keseluruhannya akan seperti ini.

52	44	31	35	56	12	23	16				
49	41	32	36	D3	92	A0	96				
4A	45	33	37	4D	08	3B	0C				
4E	4C	34	38	D8	94	A0	98				
0				1				2		3	

Gambar 10. Analisis Matrik AES8

Setelah selesai mendapatkan *subKey* untuk ronde ke-1 kita akan lanjut ke proses *subBytes.* Pada bagian ini kita melakukan proses substitusi *S-Box* terhadap hasil *addRoundKey* pada ronde ke-0. Dimana hasilnya adalah sebagai berikut.

16	64	70	07	S-BOX	47	43	51	C5
0C	00	7C	06		FE	63	10	6F
0E	09	67	06		AB	01	85	6F
07	15	7B	0E		C5	59	21	AB

Gambar 11. Analisis Matrik AES9

Selanjutnya adalah proses *addRoundKey*, sama dengan *addRoundKey* yang terjadi pada ronde ke-0, pada proses ini hasil *mixColumns* yang diperoleh diatas di-XORkan dengan *subKey* ronde ke-1 yang kita telah peroleh tadi. Hasilnya adalah seperti berikut.

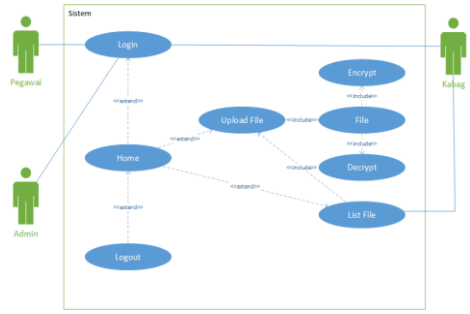
05	1C	E1	A8		56	12	23	16		53	0E	C2	BE
BE	17	30	00	⊕	D3	92	A0	96	→	6D	85	90	96
D3	D9	98	5A		4D	08	3B	0C		9E	D1	A3	56
62	2B	85	E9		D8	94	A0	98		BA	BF	25	71

Gambar 12. Analisis Matrik AES10

Berikut merupakan hasil dari ronde ke-1, untuk ronde ke-2 sampai ke-9 ulangi saja proses diatas, dan untuk ronde terakhir atau ronde ke-10, lewati proses *mixColumns.* Setelah itu, kita akan mendapatkan hasil enkripsi dari plainteks yang di-*input*.

2.1.5 Use case Diagram

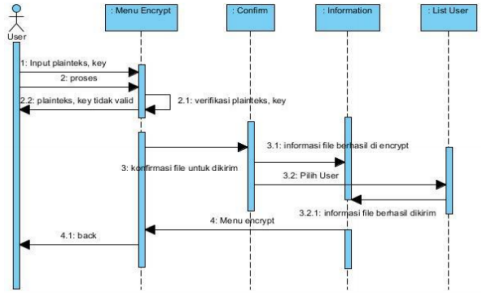
Use case diagram adalah diagram yang menunjukkan fungsionalitas suatu sistem atau kelas dan bagaimana sistem tersebut berinteraksi dengan dunia luar dan menjelaskan sistem secara fungsional yang terlihat oleh pengguna. Dari identifikasi aktor yang terlibat di atas maka *use case* diagram dapat dilihat pada Gambar 13.



Gambar 13. *Use case Diagram*

2.1.6 *Sequence Diagram* Enkripsi File

Interaksi antara aktor User dengan *use case* Enkripsi dijelaskan dalam *Sequence Diagram* pada Gambar 14 sebagai berikut:

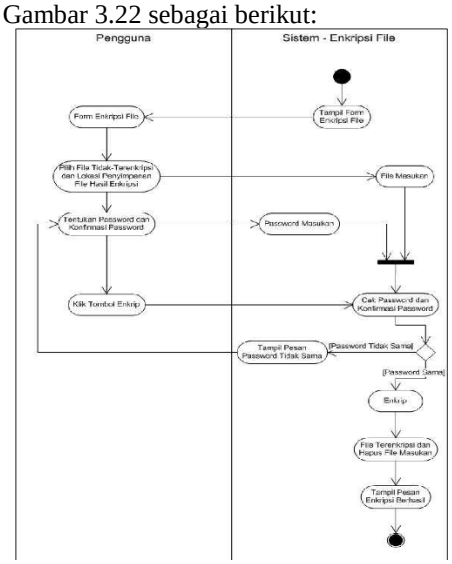


Gambar 13. *Sequence Diagram Enkripsi File*

.

2.1.7 *Aktivity Diagram Enkripsi File*

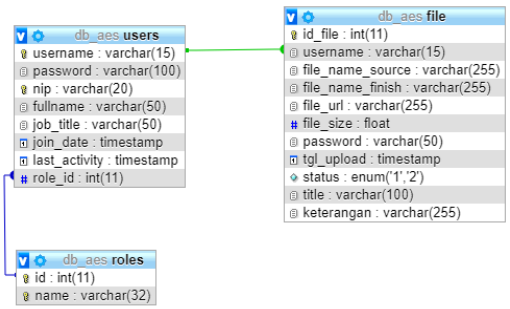
Interaksi antara aktor pengguna dengan *use case* Enkripsi File dijelaskan dalam *activity diagram* pada Gambar 3.22 sebagai berikut:



Gambar 14. *Aktivity Diagram Enkripsi File*

2.1.8 Skema Relasi

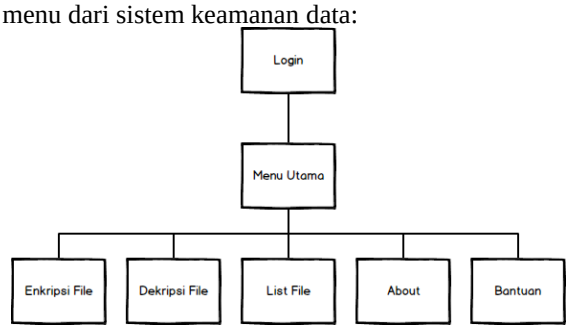
Tabel Relasi Database menggambarkan relasi antar tabel yang ada di dalam database penelitian ini. Berikut Tabel Relasi Database.



Gambar 15. Skema Relasi

2.1.9 Struktur Menu

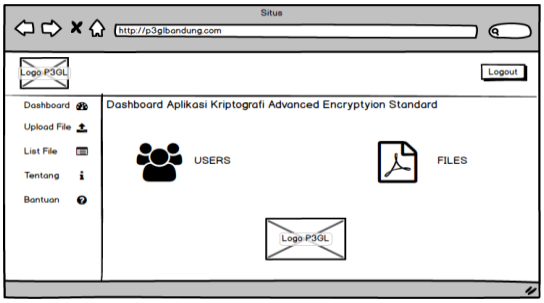
Pada Gambar 16 di bawah ini merupakan struktur menu dari sistem keamanan data:



Gambar 16. Struktur Menu

2.1.10 Perancangan Antarmuka

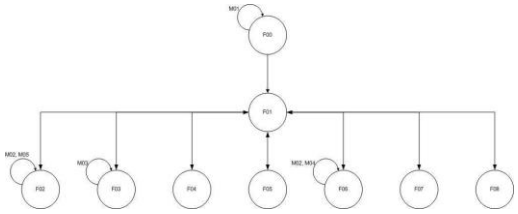
Perancangan antarmuka dibuat untuk memberi konsep pada implementasi pembuatan suatu antarmuka nantinya pada sistem. Berikut adalah gambaran dari perancangan antarmuka di sistem keamanan data:



Gambar 17. Antarmuka AES

2.1.11 Jaringan Semantik Menu

Jaringan semantik adalah gambaran pengetahuan grafis yang menunjukkan hubungan antar berbagai objek, terdiri dari lingkaran-lingkaran yang dihubungkan dengan anak panah yang menunjukkan objek dan informasi tentang objek-objek tersebut. Berikut ini adalah Gambar 18 yang menjelaskan tentang jaringan semantik di dalam sistem keamanan data:



Gambar 18. Jaringan Semantik

2.1.12 Implementasi Antar Muka

Pada bagian ini, akan diuraikan mengenai tampilan antar muka aplikasi ini mulai dari pertama kali dijalankan sampai selesai dijalankan. Berikut ini akan diberikan penjelasan dan gambar mengenai tampilan-tampilan yang ada pada aplikasi ini.

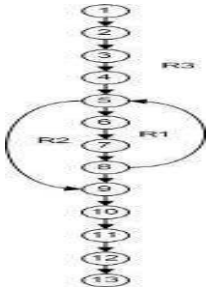
Gambar 19. Implementasi Antarmuka AES

3.HASIL DAN DISKUSI

3.1 Pengujian Alpha

Pengujian *alpha* digunakan untuk menguji aplikasi dengan berbagai kondisi, metode yang digunakan pada pengujian *alpha* adalah metode *white-box*. Pengujian *white-box* digunakan untuk meyakinkan semua perintah dan kondisi pada implementasi algoritma AES.

Berikut ini adalah *flow graph* enkripsi AES yang terlihat pada Gambar 20



Gambar 20. *Flow Graph AES*

3.2 Pengujian Beta

Pengujian *beta* dilakukan melalui pengujian performansi atau uji coba langsung kepada pengguna untuk mencoba sistem yang baru dan hasil dari percobaan tersebut dicatat untuk mengetahui tingkat keakuratan dan kecepatan system.

No.	Nama *File*	Rincian *File*	Ukuran *File* (KB)	Waktu Enkrip (detik)	Ukuran *File* Hasil (KB)	Rasio
1	Potensi Energi.pdf	Teks, Gambar	18.358	3,18	18.358	100%
2	Buku Panduan emonDAK SDA.pdf	Teks, Gambar	21.512	3,24	21.512	100%
3	DAK 26 JANUARI 2012 SDA BANDUNG.pdf	Teks, Gambar	38.212	5,52	38.212	100%
4	emondak_bg3.pdf	Teks, Gambar	19.574	2,76	19.574	100%
5	eMonDAK2012.pdf	Teks	21.532	3,17	21.532	100%
6	Sebaran_Sedimen.pdf	Teks	35.131	5,14	35.131	100%
7	Laporan-P3GL.pdf	Teks, Gambar	26.228	3,78	26.228	100%
8	Dokumen-Atlas.pdf	Teks, Gambar	22.893	3,24	22.893	100%
9	ymsgr1150_0192.pdf	Teks	18.920	2,69	18.920	100%

Tabel 1. Pengujian Beta

4.KESIMPULAN DAN SARAN

4.1 Kesimpulan

Berdasarkan dari hasil penelitian, analisis sistem, perancangan sistem, implementasi sistem, dan pengujian sistem, maka dapat diambil kesimpulan sebagai berikut:

1. Sistem yang dapat dimanfaatkan untuk proses enkripsi dan dekripsi file dengan berbagai macam ukuran dan jenis file, menggunakan algoritma AES.
2. Ukuran file lampiran hasil enkripsi tidak dipengaruhi oleh format file lampiran, tetapi dipengaruhi oleh ukuran awal file lampiran. Semakin besar ukuran file dan semakin panjang kunci AES yang digunakan maka semakin besar ukuran file enkripsi yang dihasilkan.
3. Pada saat proses dekripsi maka memerlukan komputasi lebih banyak jika dibandingkan dengan proses enkripsi, sehingga kebutuhan waktu proses dekripsi menjadi lebih lama dibandingkan dengan proses enkripsi.

4.2 Saran

Sistem Kriptografi AES ini dapat dikembangkan lebih lanjut, oleh karena itu saran dan kritik yang membangun menyarankan beberapa perbaikan pada sistem sebagai berikut:

1. Untuk file yang berukuran relatif besar sebelum proses enkripsi akan lebih baik apabila dikompres terlebih dulu, hal ini berguna untuk mempercepat proses enkripsi dan dekripsi menggunakan algoritma AES.

5. DAFTAR PUSTAKA

[1] Daemen, J; V, Rijmen. 2002. “The Design of Rijndael.” AES—Advanced Encryption Standard. Information Security and Cryptography. SpringerVerlag, Berlin, Heidelberg, New York.

[2] Handayani, Dewi. 2001. *Sistem Berkas*. Yogyakarta: J&J.

[3] Menezes, A.; van Oorschot, P.; Vanstone, S. 1996. *Handbook of Applied Cryptography*. Canada: CRC Press.

[4] Surakhmad, Winarno. 1980. *Pengantar Penelitian Ilmiah: Dasar, Metode, dan Teknik*. Bandung: Tarsito.

[5] Sommerville, Ian. 2001. *Software Engineering 6th*. Addison Wesley.

[6] Munir, Rinaldi. (2004). *Bahan Kuliah IF5054 Kriptografi*. Departemen Teknik Informatika: Institut Teknologi Bandung.

[7] Schneier, Bruce. 1996. *Applied Cryptography 2nd Edition*. Fusionopolis Walk: John Wiley & Sons.

[8] Nechvatal, James, dkk. 2000. *Report on the Development of the Advance Encryption Standard (AES)*. NIST.

[9] Kurniawan, Yusuf. 2004. Kriptografi Keamanan Internet dan Jaringan Komunikasi. Bandung: Informatika.

[10] Rosa A.S dan M.Shalahuddin, "Rekayasa Perangkat Lunak", Bandung, *Informatika, 2013*.

[11] M. K. MZ, "Pengujian perangkat lunak metode black-box berbasis equivalence partitions pada aplikasi sistem informasi sekolah," *Jurnal Mikrotik* , vol. 6, p. 3, 2016.

[12] Sukrisno, et. al., 2007, Implementasi Steganografi Teknik EOF Dengan Gabungan Enkripsi Rijndael, Shift Cipher Dan Fungis Hash MD5, tersedia pada:http://p3m.amikom.ac.id/p3m/TEKNIK%20EOF.pdf -., tanggal akses : 24 Februari 2019.

[13] Rifki Sadikin, 2012, Kriptografi Untuk Keamanan Jaringan, Penerbit ANDI, Yogyakarta.