Perancangan Aplikasi Kriptografi File Dengan Metode Algoritma *Advanced Encryption Standard* (AES)

Rahmat Tullah[1], Muhammad Iqbal Dzulhaq[2], Yudi Setiawan[3]
[1,2]Dosen STMIK Bina Sarana Global, [3]Mahasiswa STMIK Bina Sarana Global
Email : [1]kanjeng.ratoe@gmail.com, [2]abi.misykat.misbah@gmail.com, [3]abay.yudisetiawan@gmail.com

***Abstrak*— Kriptografi merupakan studi matematika yang mempunyai hubungan dengan aspek keamanan informasi seperti integritas data, keaslian entitas dan keaslian data. Kriptografi menggunakan berbagai macam teknik dalam upaya untuk mengamankan data. Pengiriman data dan penyimpanan data melalui media elektronik memerlukan suatu proses yang dapat menjamin keamanan dan keutuhan dari data yang dikirimkan tersebut. Data tersebut harus tetap rahasia selama pengiriman dan harus tetap utuh pada saat penerimaan di tujuan. Untuk memenuhi hal tersebut, dilakukan proses penyandian (enkripsi dan dekripsi) terhadap data yang akan dikirimkan. Secara garis besar enkripsi yaitu mengubah data asli yang disebut *plaintext* menjadi data rahasia atau *ciphertext*. Enkripsi dilakukan pada saat pengiriman sedangkan dekripsi dilakukan pada saat penerimaan. Jadi selama proses pengiriman, data yang dikirimkan adalah data rahasia sampai kepada proses penerima, sehingga pihak yang tidak berkepentingan tidak akan mengetahui data asli. Maka dari itu, melalui ilmu kriptografi dengan metode algoritma *Advanced Encryption Standard* yang penulis terapkan dalam sebuah aplikasi pengaman data, dapat diimplementasikan dengan sebuah bahasa pemrograman Java serta membantu dalam proses pengamanan data pada bagian akademik di Perguruan Tinggi STMIK Bina Sarana Global.**

***Kata kunci*— Kriptografi, *Plaintext, Ciphertext, Advanced Encryption Standard*.**

VI. PENDAHULUAN

Kemajuan teknologi komputer membantu semua aspek kehidupan manusia, dari hal yang kecil sampai hal yang rumit sekalipun bisa dikerjakan oleh komputer. Kriptografi merupakan studi matematika yang mempunyai hubungan dengan aspek keamanan informasi seperti integritas data, keaslian entitas dan keaslian data. Kriptografi menggunakan berbagai macam teknik dalam upaya untuk mengamankan data. Secara garis besar enkripsi yaitu mengubah data asli yang disebut *plaintext* menjadi data rahasia atau *ciphertext*. Enkripsi dilakukan pada saat pengiriman sedangkan dekripsi dilakukan pada saat penerimaan. Dalam hal ini penulis akan menerapkan algoritma kriptografi simetris dan bersifat *block cipher*.

Teknik kriptografi simetris dipilih karena diharapkan dengan algoritma ini proses enkripsi–dekripsi data dapat dilakukan dengan waktu yang lebih cepat dibandingkan dengan algoritma kriptografi kunci publik (asimetris). *Advanced Encryption Standard* dipublikasikan oleh NIST *(National Institute of Standards Technology*) pada tahun 2001. AES merupakan simetri *block cipher* untuk menggantikan DES (*Data Encryption Standard*).

STMIK BINA SARANA GLOBAL merupakan sebuah Perguruan Tinggi di bidang ilmu komputer dan manajemen, banyak data dan informasi penting yang dibutuhkan kampus tersebut yang harus dijaga kerahasiaan data informasinya, khususnya data-data nilai mahasiswa pada bagian akademik. Maka dari itu melalui ilmu kriptografi yang penulis terapkan dalam implementasi sebuah aplikasi pengaman data, nantinya diharapkan dapat membantu dalam proses pengamanan data pada bagian akademik di Perguruan Tinggi STMIK Bina Sarana Global.

Batasan rancangan pada program aplikasi ini yaitu :

1. Jenis file .txt tidak utuh saat di dekripsi hal ini dikarenakan penggunaan source code yang terbatas.
2. Rancangan program aplikasi ini untuk menyamarkan isi dari file yang akan di enkripsi dan dekripsi.
3. Metode yang digunakan hanya dengan algoritma AES (*Advanced Encryption Standard*).

VII. LANDASAN TEORI

A. Pengertian Aplikasi

Aplikasi berasal dari kata *application* yang artinya penerapan, penggunaan. Secara istilah aplikasi adalah program siap pakai yang direkam untuk melaksanakan suatu fungsi bagi pengguna atau aplikasi yang lain dan dapat digunakan oleh sasaran yang dituju. Perangkat lunak aplikasi adalah suatu perangkat lunak komputer yang memanfaatkan kemampuan komputer langsung untuk melakukan tugas yang diinginkan pengguna. Contoh utama perangkat lunak aplikasi adalah pengolah kata, lembar kerja dan pemutar media. (Sianturi Fricles Ariwisanto. 2013:01).

B. Pengertian UML (Unified Modelling Language)

Rosa A.S dan M.Shalahuddin (2014:133) mengungkapkan "*Unified Modelling Language*" (UML) adalah salah satu standar bahasa yang banyak digunakan di dunia industri untuk mendefinisikan requirement, membuat analisis & desain, serta menggambarkan arsitektur dalam pemrograman berorientasi objek. Jenis-jenis UML diantaranya:

1. *Use Case Diagram*
2. *Activity Diagram*
3. *Sequence Diagram*
4. *Class Diagram*

C. Pengertian Kriptografi

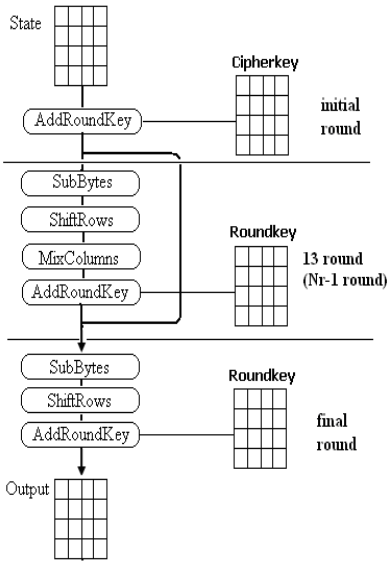
Kriptografi adalah ilmu ataupun seni yang mempelajari bagaimana membuat suatu pesan yang dikirim oleh pengirim dapat disampaikan kepada penerima dengan aman. Kriptografi merupakan bagian dari suatu cabang ilmu matematika yang disebut kriptologi (*cryptologi*). Kriptografi bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah. Perancang algoritma kriptografi disebut kriptografer. (Setyaningsih Emi. 2015:2).

D. Pengertian Advanced Encryption Standard

Setyaningsih Emi (2015:2). *Advanced Encryption Standard* dipublikasikan oleh NIST (*National Institute of Standards Technology*) pada tahun 2001. AES merupakan simetri block cipher untuk menggantikan DES (*Data Encryption Standard*). Input dan output dari algoritma AES terdiri dari urutan data sebesar 128 bit. Urutan data yang sudah terbentuk dalam satu kelompok 128 bit tersebut disebut juga sebagai *block* data atau *plaintext* yang nantinya akan dienkripsi menjadi *ciphertext*. Algoritma AES merupakan algoritma simetris yaitu mengunakan kunci yang sama untuk proses enkripsi dan dekripsi. Algoritma AES memiliki tiga pilihan kunci yaitu tipe: AES-128, AES-192 dan AES-256. Masing-masing tipe menggunakan kunci internal yang berbeda yaitu round key untuk setiap proses putaran. Proses putaran enkripsi AES-128 dikerjakan sebanyak 10 kali (a=10), yaitu sebagai berikut:

1. *Addroundkey*.
2. Putaran sebanyak a-1 kali, proses yang dilakukan pada setiap putaran adalah: *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey*.
3. Final round, adalah proses untuk putaran terakhir yang meliputi *SubBytes*, *ShiftRows*, dan *AddRoundKey*. Sedangkan pada proses dekripsi AES-128, proses putaran juga dikerjakan sebanyak 10 kali (a=10).

Proses enkripsi algoritma AES terdiri dari 4 jenis transformasi *bytes*, yaitu *SubBytes*, *ShiftRows*, *Mixcolumns*, dan *AddRoundKey*. Ilustrasi proses enkripsi AES dapat digambarkan seperti pada Gambar di bawah ini :



Sumber : S.Emi (2015)

Gambar 1. Proses Enkripsi AES

E. Gambaran Umum Objek Yang Diteliti

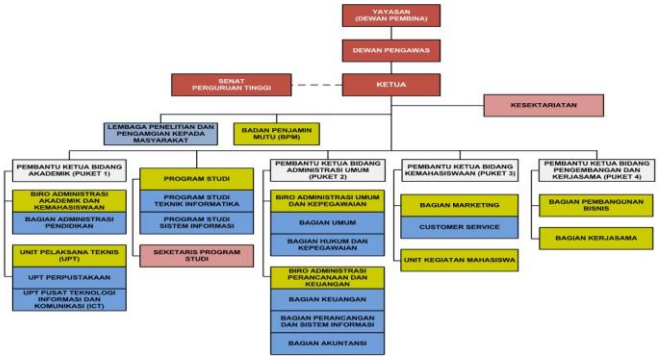
STMIK Bina Sarana Global adalah perguruan tinggi pelopor pendidikan " *Link* & *Match* " yang berada dibawah naungan Direktorat Jenderal Pendidikan Tinggi. Kiprah STMIK Bina Sarana Global diakui oleh masyarakat luas. Pengakuan dari dunia industri tercermin dari banyaknya perusahaan yang merekrut lulusan STMIK Bina Sarana Global, sedangkan pengakuan lain datang dari dunia pendidikan dalam dan luar negeri melalui kerjasama transfer kredit dan konversi mata kuliah.

Adapun wewenang dan tanggung jawab dari Ka.BAAK (ketua biro akademik dan administrasi kemahasiswaan) di STMIK Bina Sarana Global adalah :

1. Melakukan pendataan biodata mahasiswa dan dosen, berikut dokumen kelengkapannya.
2. Menyimpan kelengkapan kegiatan awal perkuliahan, nomor induk mahasiswa, absensi mahasiswa dan dosen, jadwal perkuliahan, biodata dosen dan lain-lain.
3. Menyelenggarakan administrasi mahasiswa.
4. Pemeliharaan biodata mahasiswa.
5. Nomor registrasi.
6. Jadwal kegiatan perkuliahan.
7. Surat keterangan, surat referensi, data nilai, sertifikat mahasiswa.
8. Menyiapkan dan mendaftarkan mahasiswa ke Epsbed.
9. Membuat rekapitulasi mengajar dosen.
10. Menghubungi dosen lain untuk menggantikan dosen yang berhalangan hadir.
11. Menyiapkan sarana dan prasarana untuk kelancaran proses belajar mengajar.
12. Melegalisir ijazah dan memperpanjang izin penyelenggaraan.
13. Menyiapkan KHS dan KRS.
14. Melaksanakan kegiatan lain yang ditugaskan oleh atasannya untuk tugas-tugas penyelenggaraan administrasi pendidikan untuk kepentingan kampus.

F. Struktur Organisasi

Struktur organisasi STMIK Bina Sarana Global pada dasarnya sama seperti struktur organisasi lain, dimana wewenang yang dimiliki oleh atasan diturunkan langsung pada bawahan, dan bawahan bertanggung jawab terhadap atasan.



Sumber : Data Sekunder (2016)

Gambar 2. Struktur Organisasi STMIK Bina Sarana Global

VIII. METODOLOGI PENELITIAN

A. Metode AES

AES termasuk dalam jenis algoritma kriptografi yang sifatnya simetri dan *cipher block*. Dengan demikian algoritma ini mempergunakan kunci yang sama saat enkripsi dan dekripsi serta masukan dan keluarannya berupa *block* dengan jumlah bit tertentu. Contoh Penerapan :

Implementasi dilakukan dengan memasukan sebuah *plaintext* yang memiliki kunci sebagai berikut :

Plaintext : 0 1 2 3 4 5 6 7 8 9 A B C D E F
In HEX : 30 31 32 33 34 35 36 37 38 3 41 42 43 44 45 46
Key : A B C D E F G H I J K L M N O P
In HEX : 41 42 43 44 45 46 47 4849 4A 4B 4C 4D 4E 4F 50

1. AddRound Key

Add Round Key pada dasarnya adalah mengkombinasikan *chipertext* yang sudah ada dengan *chiperkey* yang *chiperkey* dengan hubungan XOR.

30	34	38	43
31	35	39	44
32	36	41	45
33	37	42	46

41	45	49	4D
42	46	4A	4E
43	47	4B	4F
44	48	4C	50

Sumber :S.Emi, kriptografi, 2015

Gambar 3. *AddRounKey*

2. SubBytes

Prinsip dari *SubBytes* adalah menukar isi matriks/tabel yang ada dengan matriks/tabel lain yang disebut dengan S-Box. Di bawah ini adalah contoh *SubBytes* S-Box.

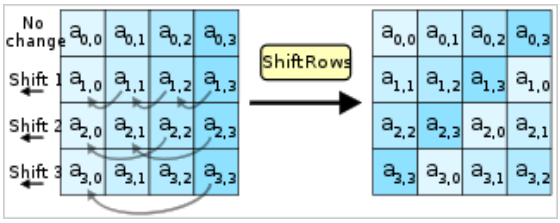
Tabel 1. Tabel S-Box

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

Sumber :S.Emi, kriptografi, 2015

3. ShiftRows

ShiftRows seperti namanya adalah sebuah proses yang melakukan shift atau pergeseran pada setiap elemen *block*/tabel yang dilakukan per barisnya. Yaitu baris pertama tidak dilakukan pergeseran, baris kedua dilakukan pergeseran 1 *byte*, baris ketiga dilakukan pergeseran 2 *byte*.

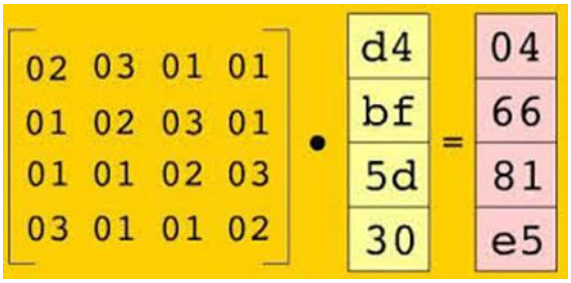


Sumber :S.Emi, kriptografi, 2015

Gambar 4. Proses *ShiftRows*

4. MixColumns

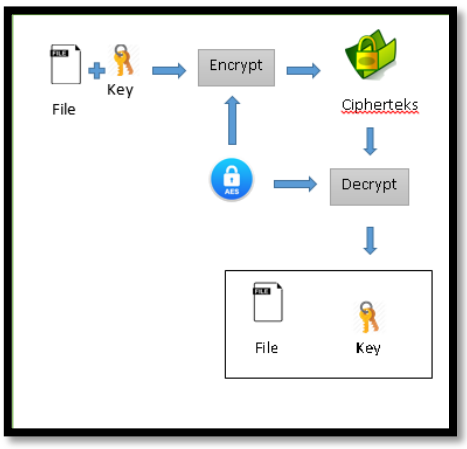
Yang terjadi saat *MixColumns* adalah mengalikan tiap elemen dari *block chiper* dengan matriks yang ditunjukkan pada proses sebelumnya. Tabel sudah ditentukan dan siap pakai. Pengalian dilakukan seperti perkalian matriks biasa yaitu menggunakan dot product lalu perkalian keduanya dimasukkan ke dalam sebuah *block chiper* baru.



Sumber :S.Emi, kriptografi, 2015

Gambar 5. Proses *MixColumns*

B. Alur Proses Aplikasi



Gambar 6. Alur Proses Aplikasi

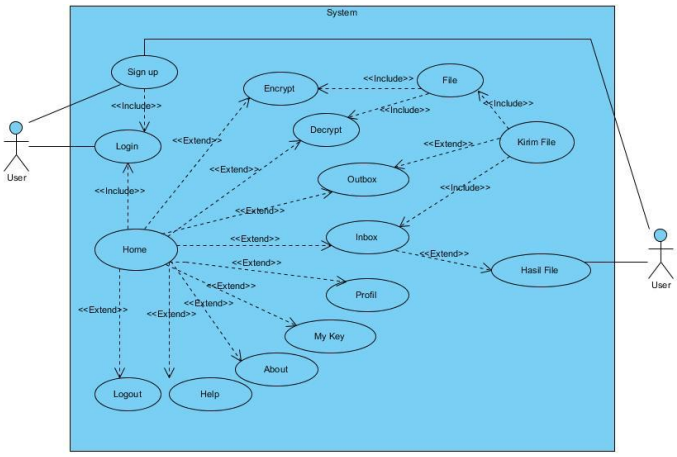
Pada gambar diatas adalah alur proses dari perancangan apikasi yang diberi nama "Global_Crypto". File dan kunci dikirim lalu dienkrip dengan algoritma AES sehingga menghasilkan keluaran berupa *ciphertext*, dan ketika di dekrip kebalikannya dari enkrip *ciphertext* dilakukan proses dekripsi dan menghasilkan keluaran *plaintext* file bersama kuncinya.

5. HASIL DAN PEMBAHASAN

A. Rancangan UML

Pada tahap ini dijelaskan rancangan model diagram yang bersifat pada pendekatan objek dari perancangan aplikasi yang dibuat dengan menggunakan *usecase diagram*, *activity diagram* dan *sequence diagram*.

1. *Use Case Diagram*
   Perancangan aplikasi Global_Crypto diawali dengan membuat rancangan *usecase diagram* seperti gambar dibawah ini:

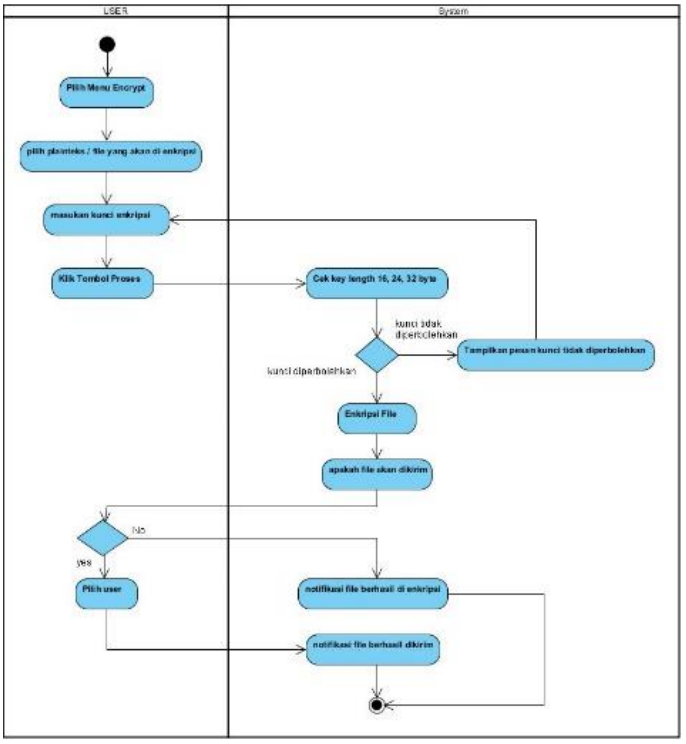


Gambar 7. *Use Case Diagram* Aplikasi Global_Crypto

Pada gambar 7. diatas terdapat beberapa objek diantaranya:

a. 1 (satu) sistem yang merupakan rancangan program aplikasi Global_Crypto.
b. 2 (dua) aktor yang dapat melakukan kegiatan yaitu: User pengirim dan user penerima.
c. 12 (dua belas) *use case* yang dapat dilakukan oleh aktor tersebut yaitu *Login*, *Sign Up*, *Home*, *Encrypt*, *Decrypt*, *Inbox*, *Outbox*, Profil, *My Key*, *About*, *Help*, *Logout*.
d. 6 (enam) *include* yang menjelaskan bahwa *usecase* tersebut berasal dari sumber secara *eksplisit* dari *usecase* sebelumnya.
e. 10 (sepuluh) *extension points*.

2. *Activity Diagram Enkripsi*
   Perancangan yang kedua dari proses ini yaitu menjelaskan bagian dari *activity* pada proses enkripsi. Dalam *activity diagram* enkripsi terdapat dua partition yaitu user dan *system*. User memilih menu *encrypt* dan memasukan inputan file yang akan di enkripsi dan memilih tombol proses maka system akan melakukan verifikasi terhadap kunci yang digunakan apabila sesuai panjang kuncinya maka proses enkripsi akan dilakukan dan system akan mengeluarkan notifikasi "apakah file akan dikirim" jika tidak maka system akan mengeluarkan notifikasi "file berhasil dienkripsi" jika file dikirim maka user harus memilih user mana yang akan dikirim filenya dan *system* akan memberitahu file berhasil dikirim. Seperti ditunjukan pada gambar dibawah ini.



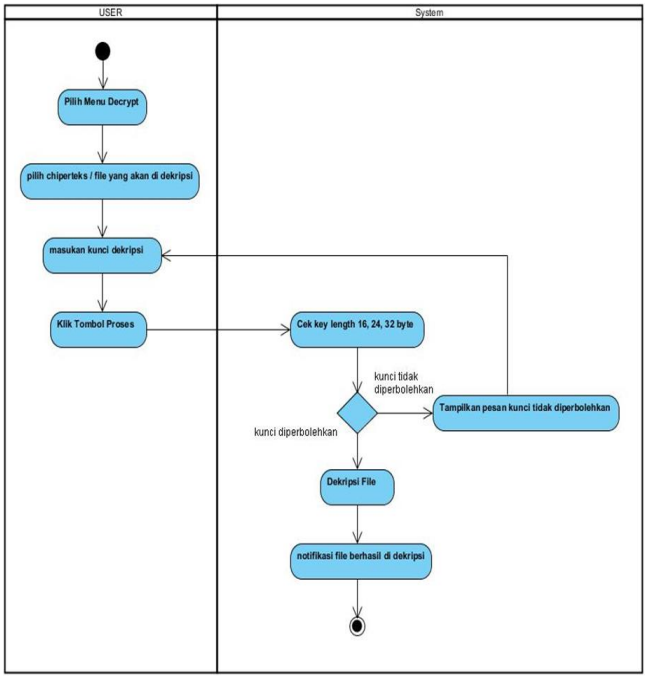
Gambar 8. *Activity Diagram* Enkripsi

Pada gambar 8. *Activity Diagram* diatas didapatkan :

a. 1 (satu) *Initial Node*, objek yang diawali.
b. 11 (sebelas) *Action State*, berawal dari user melakukan inputan file yang dienkripsi dan kunci enkripsi sampai melakukan pengiriman pada hasil enkripsi.
c. 1 (satu) *Activity Final Node*, objek yang diakhiri

3. *Activity Diagram Dekripsi*

Perancangan selanjutnya adalah *activity diagram* dari proses dekripsi. Dalam diagram *activity* dekripsi terdapat dua partition yaitu user dan system. User memilih menu *decrypt* dan memasukan *ciphertext* atau file yang akan di dekrip. Kemudian user memasukan kunci yang sama ketika enkrip file dan memilih tombol proses, maka system akan melakukan verifikasi terhadap panjang kunci dan keaslian kunci. Jika berhasil maka system akan mengeluarkan notifikasi "file berhasil di *decrypt*". Seperti ditunjukan pada gambar dibawah ini.



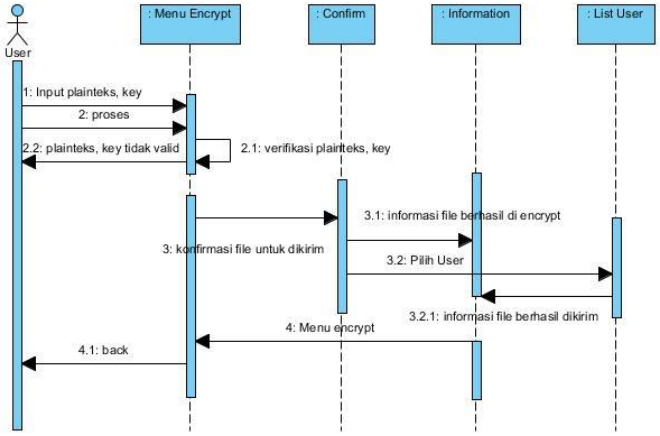
Gambar 9. *Activity Diagram* Dekripsi

Pada gambar 9. *Activity diagram* dekripsi didapatkan:

a. 1 (satu) *Initial Node*, objek yang diawali.
b. 8 (delapan) *Action State*, berawal dari user melakukan inputan *ciphertext* yang di dekripsi dan kunci dekripsi sampai melakukan pengiriman pada hasil dekripsi.
c. 1 (satu) *Activity Final Node*, objek yang diakhiri.

4. *Sequence Diagram* Enkripsi

Perancangan *sequence diagram* enkripsi dibuat untuk menjelaskan yang terjadi didalam sistem ketika proses enkripsi seperti gambar dibawah ini.



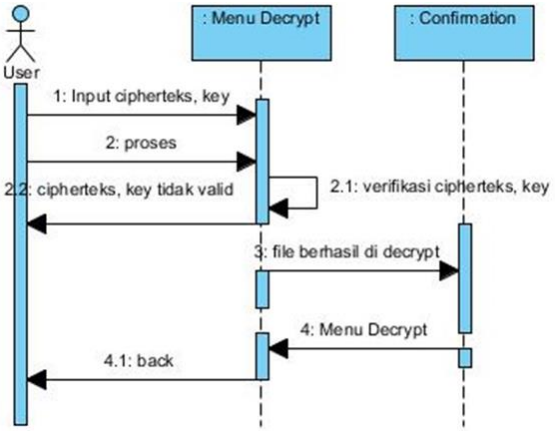
Gambar 10. *Sequence Diagram* Enkripsi

Pada gambar 10. *Seqence Diagram* diatas didapatkan :

a. 1 (satu) *actor* melakukan kegiatan yaitu sebagai user.
b. 4 (empat) *Lifeline* yaitu Menu *Encrypt*, *Confirm*, information, *List user*.
c. 10 (sepuluh) "Message" antara lain Input *plaintext key*, proses, verifikasi *plaintext key*, *plaintext key* tidak valid, informasi file berhasil di *encrypt*, konfirmasi file untuk dikirim, pilih user, informasi file untuk dikirim, menu *encypt*, *back.*

5. *Sequence Diagram Dekripsi*

Perancangan *sequence diagram* dekripsi dibuat untuk menjelaskan yang terjadi didalam sistem ketika proses dekripsi seperti gambar dibawah ini.



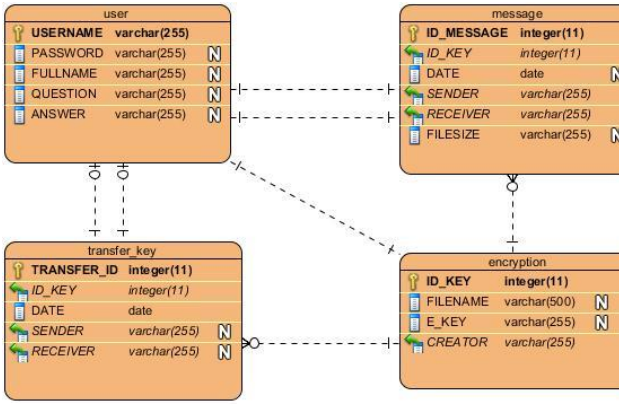
Gambar 11. *Sequence Diagram* Dekripsi

Pada gambar 11. *Activity diagram* dekripsi diatas didapatkan:

a. 1 (satu) aktor melakukan kegiatan yaitu sebagai user
b. 2 (dua) *Lifeline* yaitu Menu *Decrypt*, *Confirmation*
c. 7 (tujuh) "*Message*" antara lain Input *ciphertext*, *key*, proses, verifikasi *ciphertext key*, *ciphertext key* tidak valid, file berhasil di *decrypt*, Menu *Decrypt*,

back.

6. *Class Diagram* Database



Gambar 12. *Class Diagram* Database

Pada gambar 12. Class diagram Database menggunakan MySQL 5.6.20 dengan nama database "db_global_crypto". Ada beberapa *class* diantaranya *user*, *message*, *transfer_key*, *encryption* yang saling berelasi.

B. Interface / Tampilan

Tampilan pada Aplikasi dibuat dengan menggunakan bahasa pemrograman Java. Tampilan dibuat dengan menambahkan beberapa fitur form pada aplikasi agar terdapat penambahan fitur selain proses enkripsi dan dekripsi dan terdapat sembilan formpada menu utama yaitu *Encrypt*, *Decrypt*, *Inbox*, *Outbox*, *Profile*, *My Key*, *About*, *Help*, *Logout*. Berikut adalah tampilan menu utamanya.

Gambar 13. Tampilan Form Utama Aplikasi

a. Pengujian Proses Enkripsi dan Dekripsi

1. Pengujian Enkripsi

Pada fungsi enkripsi akan diuji coba file yang berjenis xls dengan ukuran file 15 KB dan sebuah inputan kunci sebear 16 *byte* dengan kata kuncinya "kurikulum lama 1" setelah itu file akan langsung di enkrip tanpa dikirim ke user lain. Seperti gambar berikut ini:

- Dilakukan inputan file/*plaintext* beserta kuncinya.

Gambar 14. Tampilan menu input enkripsi

- Hasil file setelah di enckripsi.

Gambar 15. Tampilan isi file hasil enkripsi

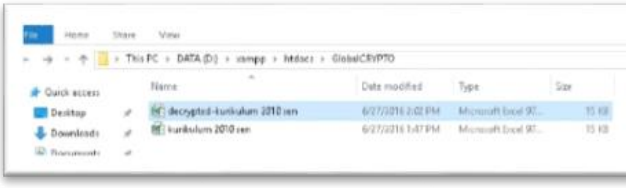
2. Pengujian Dekripsi

Pada proses dekripsi merupakan kebalikan dari proses enkripsi, file berjenis xls yang telah di enkrip akan dilakukan dekrip sehingga file kembali menjadi normal dan dapat dibuka. Kunci yang digunakan sama dengan kunci yang dipakai ketika enkrip sebesar 16 byte yaitu "kurikulum lama 1" dengan ukuran file 15 KB. Jika file berhasil di dekripsi maka terdapat penambahan nama file menjadi "*decrypted*" pada bagian depan untuk membedakan file yang sudah didekrip dan yang belum.

- Dilakukan inputan file atau *ciphertext* beserta kuncinya.

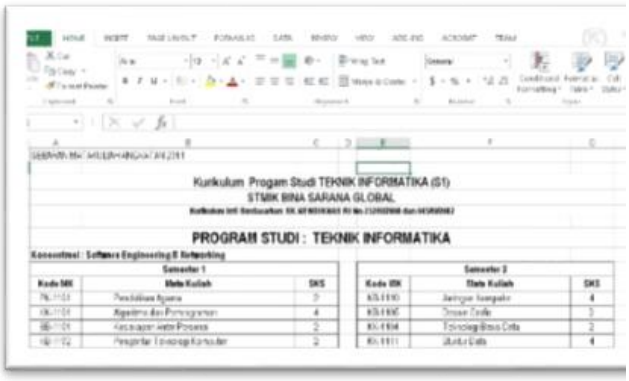
Gambar 16. Tampilan menu input decrypt

- Nama file berbeda setelah dilakukan dekrip



Gambar 17. Nama file setelah *decrypt*

- Hasil file setelah di dekrip



Gambar 18. Tampilan isi file hasil dekripsi

IX. KESIMPULAN DAN SARAN

A. Kesimpulan

1. Tehnik dalam mengamankan sebuah file dapat dilakukan dengan menggunakan sebuah metode algoritma kriptografi.
2. Untuk melakukan penerapan tehnik enkripsi dan dekripsi algoritma AES (*Advanced Encryption Standard*) diperlukan beberapa transformasi atau proses yang terjadi didalam algoritma itu sendiri yaitu *addroundkey*, *subbytes*, *shiftrows* dan *mixcolumns*.
3. Implementasi kriptografi dalam memberikan keamanan data tergantung dari pada penggunaan algoritma kriptografi itu sendiri semakin sulit proses yang terjadi didalam algoritma, maka tingkat keamanan pada algoritma akan sulit pula dipecahkan dan biasanya algoritma yang dipakai adalah bentuk algoritma simetris dan asimetris digabung untuk mendapatkan tingkat keamanan yang lebih baik terhadap data.
4. Perancangannya kedalam program aplikasi dapat dilakukan dengan program aplikasi yang mendukung terhadap algoritma itu sendiri seperti bahasa pemrograman Java.

B. Saran

Berdasarkan kesimpulan penelitian, maka penulis merekomendasikan berupa saran-saran sebagai berikut:

1. Untuk dapat lebih meningkatkan lagi dalam penggunaan aplikasi ini user harus memasukan kunci privat yang lebih panjang lagi dari pilihan kunci private yang ada yaitu 16 *byte*, 24 *byte* dan 32 *byte*.
2. Tingkat kebutuhan akademik dalam merealisasikan aplikasi ini tergantung dari keinginan dalam menjaga file itu sendiri, apabila file perlu di enkripsi maka aplikasi ini pilihan yang tepat untuk digunakan.
3. Tingkat keamanan algoritma menggunakan kunci private artinya kunci untuk enkripsi dan dekripsi sama. Jadi kunci tidak boleh sembarang orang mengetahui.

DAFTAR PUSTAKA

[1] R. Cipta, *Dasar Algoritma & Struktur Data Dengan Bahasa Java*, Yogyakarta : Penerbit Andi, 2015.

[2] Rosa A.S, dan M. Shalahuddin, *Rekayasa Perangkat Lunak Terstruktur dan Berorientasi Objek*, Bandung : Penerbit Informatika, 2014.

[3] S.Emi, *Kriptografi & Implementasinya Menggunakan Matlab*, Yoyakarta : Penerbit Andi, 2015.

[4] S. Fricles Ariwisanto, *Perancangan Aplikasi Pengaman Data Dengan Kriptografi Advanced Encryption Standard (AES)*, Jurnal Pendidikan Ilmiah, Vol. IV, No. 1, 2015.