

LAPORAN PRAKTIKUM SISTEM KEAMANAN DATA



Disusun Oleh:

Algeori Wira Wahyu Hidayat	(V3920006)
Ardianita Fauziah	(V3920009)
Elya Kumala Fauziah	(V3920020)
Hemalia Aisyah Putri	(V3920025)
Linda Ramawati	(V3920033)

**UNIVERSITAS SEBELAS MARET D3 TEKNIK
INFORMATIKA MADIUN**

TAHUN 2021

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

A. Judul dan Latar Belakang Masalah :

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 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.

B. Tujuan Penelitian :

Tujuan dari penelitian ini yaitu menyampaikan pesan yang terjamin akan kerahasiaan/privasinya, tetapi masih menyungung unsur keaslian dari data tersebut.

C. Algoritma yang dipakai beserta alur penelitiannya:

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 menggunakan 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

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.

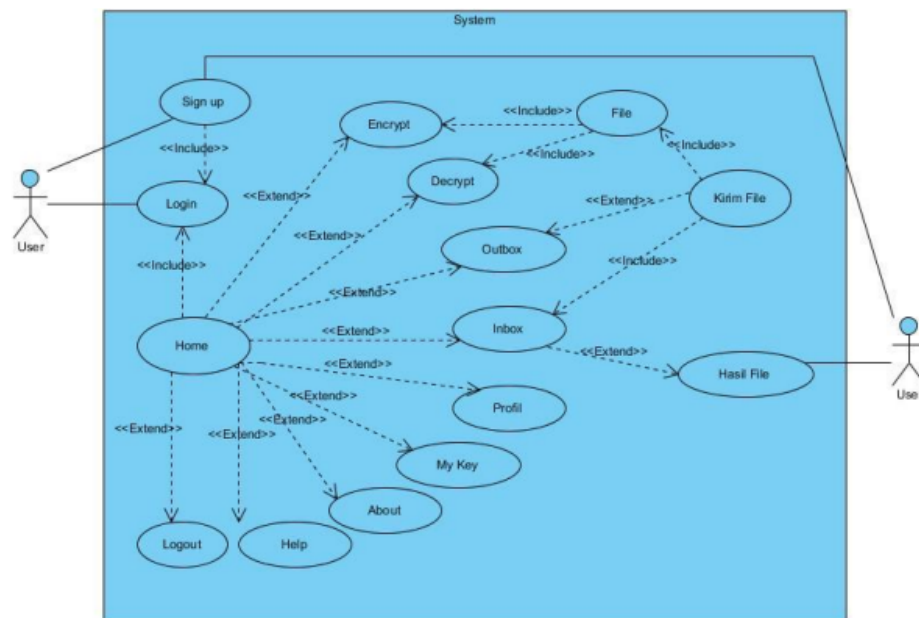
Metode AES termasuk dalam jenis algoritma kriptografi yang sifatnya simetri dan cipher block. Dengan demikian algoritma ini mempergunakan kunci yang sama saat enkripsi dan dekripsi serta masukan dan keluarannya berupa block dengan jumlah bit tertentu. Contoh Penerapan : Implementasi dilakukan dengan 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 48 49 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.
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
3. **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.
4. **MixColumns** adalah mengalikan tiap elemen dari block chiper dengan matriks yang ditunjukkan pada proses sebelumnya. Tabel sudah ditentukan dan siap pakai. Pengalihan dilakukan seperti perkalian matriks biasa yaitu menggunakan dot product lalu perkalian keduanya dimasukkan ke dalam sebuah block chiper baru.

D. Ceritakan hasil penelitian pada jurnal tersebut dan kesimpulannya

- 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 use case diagram seperti gambar dibawah ini:



Gambar 7. Use Case Diagram Aplikasi Global_Crypto

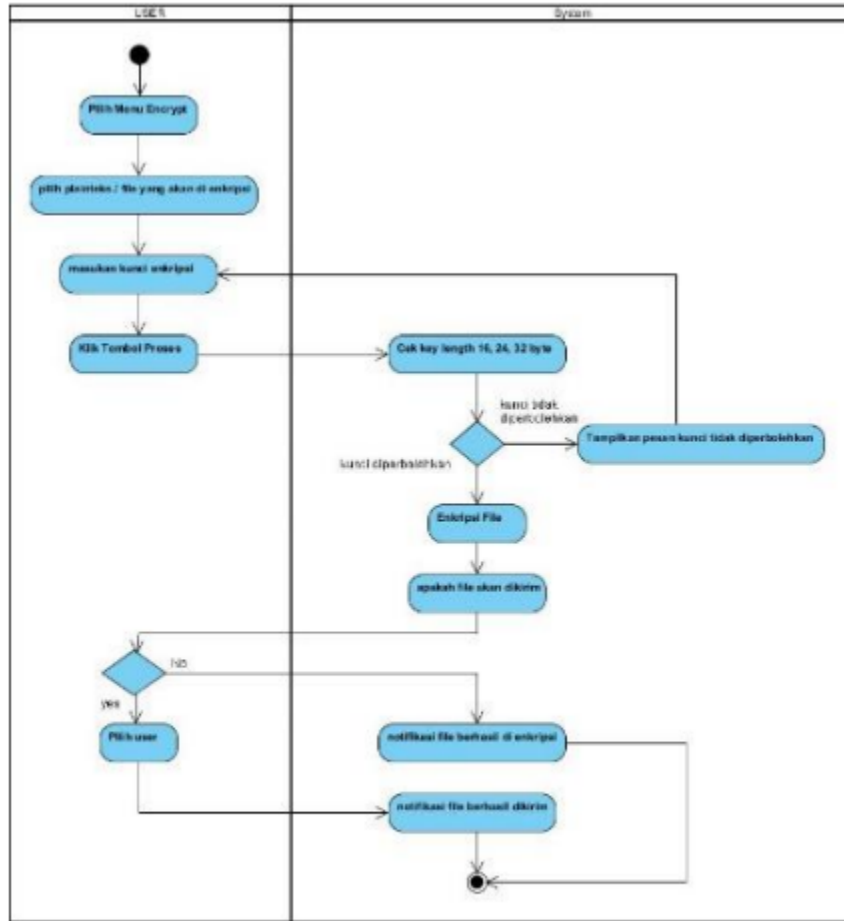
Pada gambar 7. diatas terdapat beberapa objek diantaranya:

- 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 (duabelas) 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 use case tersebut berasal dari sumber secara eksplisit dari use case 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.



Gambar 8. Activity Diagram Enkripsi

Pada gambar 8. Activity Diagram diatas didapatkan :

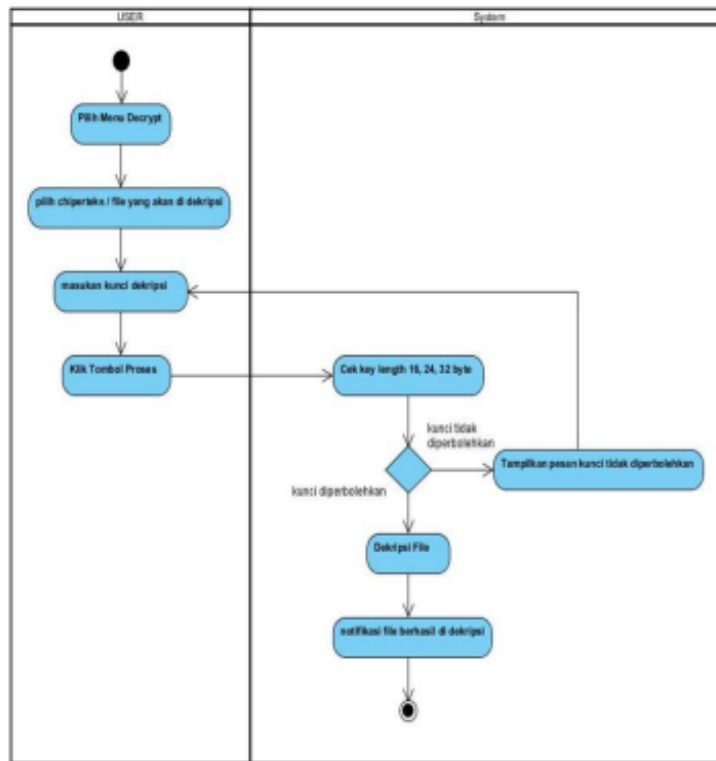
- 1 (satu) Initial Node, objek yang diawali.
- 11 (sebelas) Action State, berawal dari user melakukan inputan file yang dienkripsi dan kunci enkripsi sampai melakukan pengiriman pada hasil enkripsi.
- 1 (satu) Activity Final Node, objek yang diakhiri

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 enkripsi file dan memilih tombol proses, maka system akan melakukan verifikasi terhadap panjang kunci

dan keaslian kunci.

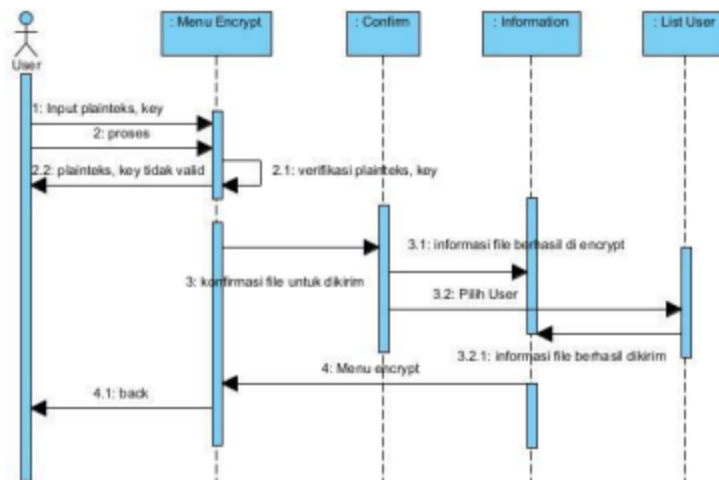


Gambar 9. Activity Diagram Dekripsi

Pada gambar 9. Activity diagram dekripsi didapatkan:

- 1 (satu) Initial Node, objek yang diawali.
- 8 (delapan) Action State, berawal dari user melakukan inputan ciphertext yang di dekripsi dan kunci dekripsi sampai melakukan pengiriman pada hasil dekripsi.
- 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.



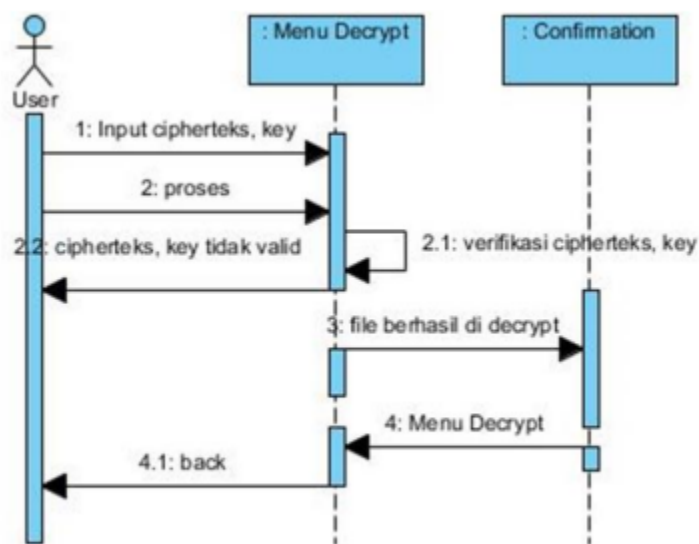
Gambar 10. Sequence Diagram Enkripsi

Pada gambar 10.

Sequence 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 encrypt, back.

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



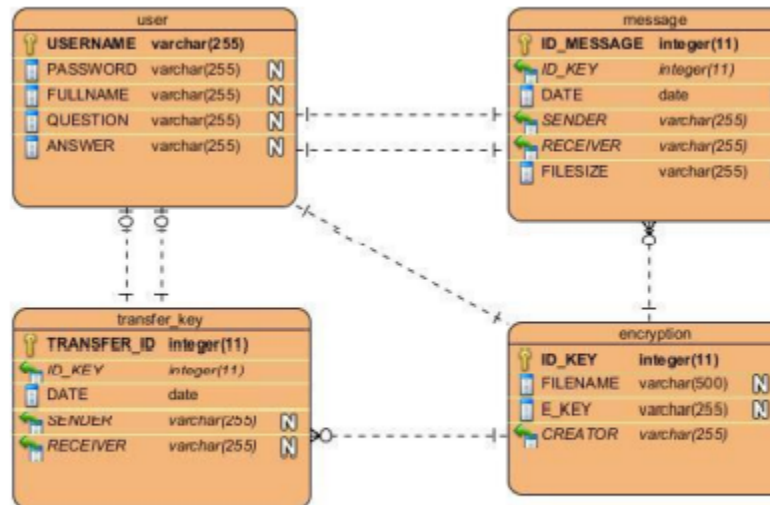
Gambar 11. Sequence Diagram Dekripsi

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 form pada 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 sebesar 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 enkripsi



Gambar 15. Tampilan isi file hasil enkripsi

2. Pengujian Dekripsi

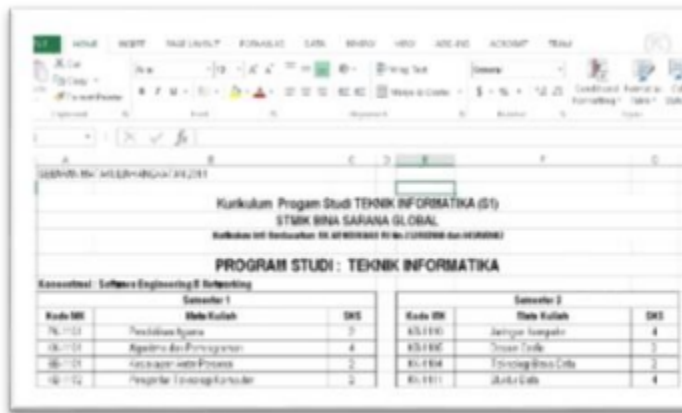
Pada proses dekripsi merupakan kebalikan dari proses enkripsi, file berjenis xls yang telah di enkrip akan dilakukan dekrip sehingga file kembali menjadi normal dan dapat dibuka. Kunci yang digunakan sama dengan kunci yang dipakai ketika enkrip sebesar 16 byte yaitu “kurikulum lama 1” dengan ukuran file 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 dekripsi



Semester 1			Semester 2		
Kode SKS	Nama Kuliah	SKS	Kode SKS	Nama Kuliah	SKS
IN-101	Pengantar Sistem	3	IN-201	Kejuruan Jaringan	4
IN-102	Algoritma dan Pemrograman	4	IN-202	Kejuruan Sistem	3
IN-103	Kejuruan Sistem	3	IN-203	Kejuruan Sistem	3
IN-104	Pengantar Teknologi Informasi	3	IN-204	Kejuruan Sistem	4

Gambar 18. Tampilan isi file hasil dekripsi

algoritma simetris dan asimetris digabung untuk mendapatkan tingkat keamanan yang lebih baik terhadap data.

3. Perancangannya kedalam program aplikasi dapat dilakukan dengan program aplikasi yang mendukung terhadap algoritma itu sendiri seperti bahasa pemrograman Java.

E. Kelebihan dan kekurangan masing-masing jurnal tersebut

Kelebihan

1. Dalam abstract sudah dipaparkan dengan jelas bahwa tujuan dari penelitian tersebut adalah agar dapat diimplementasikan dengan sebuah bahasa pemrograman Java serta membantu dalam proses pengamanan data pada bagian akademik di Perguruan Tinggi STMIK Bina Sarana Global.
2. Dalam jurnal terdapat gambaran umum dari program yang akan dibuat sehingga pembaca dapat langsung mengetahui gambaran umum dari program.
3. Terdapat banyak gambar yang dapat menunjang penjelasan program sehingga akan membantu memudahkan pembaca saat memahami.

Kekurangan

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).

Implementasi Algoritma Kriptografi AES untuk Enkripsi dan Deskripsi Email

A. Latar Belakang Masalah

Perkembangan dunia informatika yang sangat pesat saat ini membawa pertumbuhan dunia ke dalam masa teknologi informasi. Karena itulah nilai informasi saat ini sangat penting. Salah satu contohnya adalah menggunakan email. Algoritma kriptografi AES digunakan untuk proses penyandian email. Aplikasi ini menggunakan bahasa pemrograman Java dan Netbeans 7.0 sebagai perangkat lunak. Server mail yang digunakan adalah Google mail dan menggunakan port 465. Kunci yang digunakan menggunakan kunci 128-bit, sehingga hanya ada 10 putaran kunci. Langkah – langkah penelitian yang dilakukan adalah pertama, mengunduh email dari Google server kemudian mengenkripsi pesan tersebut. Kedua, pesan yang telah dienkripsi selanjutnya akan didekripsi untuk membuktikan pesan tersebut masih sama dengan pesan asli sebelum dienkripsi dengan menggunakan kunci yang sama. Hasil penelitian ini adalah suatu aplikasi enkripsi dan dekripsi email dengan menggunakan algoritma kriptografi AES (Rijndael). Dengan perangkat lunak ini, keamanan dalam mengirim dan menerima email dapat terjamin. Walaupun pesan email bisa diambil orang lain tetapi mereka tetap tidak akan bisa membacanya karena teks tertampil dalam bentuk karakter heksadesimal dan jika dijadikan string maka akan tampil sebagai simbol-simbol yang tidak jelas.

B. Tujuan Penelitian

Tujuan dari pembuatan penelitian ini adalah untuk merancang dan membuat aplikasi mail client yang dirasakan aman dari para hacker yang sering melakukan pengendusan data email yang sedang lalu lalang melalui jaringan Internet dan menerapkan algoritma kriptografi AES untuk enkripsi dan dekripsi pada email. Nilai informasi saat ini sangat penting. Salah satu contohnya adalah menggunakan email. Algoritma kriptografi AES digunakan untuk proses penyandian email. Aplikasi ini menggunakan bahasa pemrograman Java dan Netbeans 7.0 sebagai perangkat lunak. Server mail yang digunakan adalah Google mail dan menggunakan port 465. Kunci yang digunakan menggunakan kunci 128-bit, sehingga hanya ada 10 putaran kunci

C. Algoritma yang dipakai beserta alur penelitiannya:

1. Metode Enkripsi

Untuk langkah dari metode ini seperti berikut :

a. Transformasi SubBytes()

Pada langkah ini dengan cara memetakan setiap byte dari array state dengan menggunakan tabel substitusi S-box.

hex	y															
	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

S-BOX

b. Transformasi ShiftRows()

Dengan cara melakukan pergeseran secara wrapping (siklik) pada 3 baris terakhir dari array state. Jumlah pergeseran bergantung pada nilai baris (r). Baris r = 1 digeser sejauh 1 byte, baris r = 2 digeser sejauh 2 byte, dan baris r = 3 digeser sejauh 3 byte. Baris r = 0 tidak digeser
Geser baris ke-1 :

d4	e0	b8	1e
27	bf	b4	41
11	98	5d	52
ae	f1	e5	30

← rotate over 1 byte

Hasil pergeseran baris ke 1 dan geser baris ke 2 :

d4	e0	b8	1e
bf	b4	41	27
11	98	5d	52
ae	f1	e5	30

← rotate over 2 bytes

Hasil pergeseran baris ke 2 dan geser baris ke 3 :

d4	e0	b8	1e
bf	b4	41	27
5d	52	11	98
ae	f1	e5	30

← rotate over 3 bytes

Hasil pergeseran baris ke 3 :

d4	e0	b8	1e
bf	b4	41	27
5d	52	11	98
30	ae	f1	e5

← rotate over 3 bytes

c. Transformasi MixColumns()

mengalikan setiap kolom dari array state dengan polinom $a(x) \bmod (x^4 + 1)$. Setiap

kolom diperlakukan sebagai polinom 4-suku pada GF(28).

$a(x)$ yang ditetapkan adalah $a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$.

$$s'(x) = a(x) \otimes s(x)$$

$$s'(x) = a(x) \otimes s(x)$$

$$\begin{bmatrix} s'_{0x} \\ s'_{1x} \\ s'_{2x} \\ s'_{3x} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0x} \\ s_{1x} \\ s_{2x} \\ s_{3x} \end{bmatrix}$$

$$s'_{0x} = (\{02\} \bullet s_{0x}) \oplus (\{03\} \bullet s_{1x}) \oplus s_{2x} \oplus s_{3x}$$

$$s'_{1x} = s_{0x} \oplus (\{02\} \bullet s_{1x}) \oplus (\{03\} \bullet s_{2x}) \oplus s_{3x}$$

$$s'_{2x} = s_{0x} \oplus s_{1x} \oplus (\{02\} \bullet s_{1x}) \oplus (\{03\} \bullet s_{2x})$$

$$s'_{3x} = (\{03\} \bullet s_{0x}) \oplus s_{0x} \oplus s_{1x} \oplus (\{02\} \bullet s_{1x})$$

d. Transformasi AddRoundKey()

Pada transformasi ini menggunakan operasi XOR terhadap round key dengan array state, dapat hasilnya dapat disimpan di array state. Contoh bisa dilihat di bawah ini :

04	e0	48	28			a0	88	23	2a
66	cb	f8	06			fa	54	a3	6c
81	19	d3	26			fe	2c	39	76
e5	9a	7a	4c			17	b1	39	05
				Round key					

XOR-kan kolom pertama state dengan kolom pertama round key

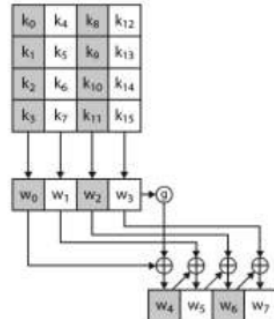
04		a0	=	a4
66	\oplus	fa	=	9c
81		fe	=	7f
e5		17	=	f2

Hasil :

a4	68	6b	02
9c	9f	5b	6a
7f	35	ea	50
f2	2b	43	49

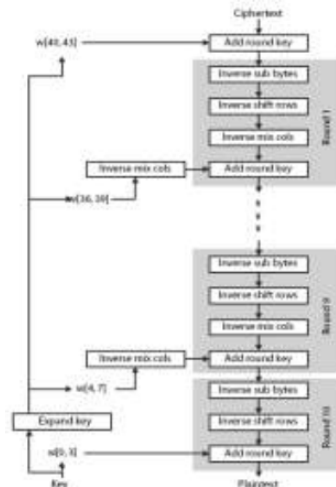
e. Ekspansi Kunci (Key Expansion)

Key Expansion pada AES 128-bit atau 16-byte menggunakan 4 words atau 16 byte untuk inputan dan menghasilkan perluasan kunci menjadi 44 words atau 176 byte.



2. Metode Deskripsi

Untuk alur dari metode ini yaitu :



D. Ceritakan hasil penelitian pada jurnal tersebut dan kesimpulannya

Dalam jurnal ini dijelaskan mengenai metode AES yang digunakan untuk Enkripsi dan Deskripsi Email. Langkah kerja metode enkripsi yaitu Transformasi SubBytes, Transformasi ShiftRows, Transformasi MixColumns, Transformasi AddRoundKey, dan Ekspansi Kunci (Key Expansion). Pada pengujian programnya juga sudah berhasil, pada saat mengenkripsi pesan cukup tekan Button 'Yes' pada program kemudian akan muncul pewaktu konfirmasi yang menunjukkan waktu untuk proses enkripsi pesan tersebut. Jika ingin pesan asli yang ditampilkan, maka cukup tekan 'No' pada program. Setelah mengenkripsi pesan dan kita ingin mengecek apakah isi pesan tersebut sama dengan yang asli, tombol Decrypt diklik, sehingga pesan asli akan tampil.

Berdasarkan hasil penelitian, dapat diambil beberapa kesimpulan yaitu dengan perangkat lunak ini, keamanan dalam mengirim dan menerima email sekiranya dapat terjamin. Walaupun pesan email bisa diambil orang lain tetapi mereka tetap tidak akan bisa

membacanya karena teks tertampil dalam bentuk karakter heksadesimal dan jika di jadikan string maka berupa simbol-simbol tidak jelas. Perangkat lunak ini hanya mengamankan isi text email bukan mengamankan jalur transfer email.

E. Kelebihan dan kekurangan masing-masing jurnal tersebut

Kelebihan

1. Judul jurnal harus memiliki judul yang jelas. Pada jurnal ini memiliki judul yang jelas sehingga pembaca mengetahui inti dari jurnal yaitu tentang Implementasi Algoritma Kriptografi Aes untuk Enkripsi dan Dekripsi Email
2. Pada abstract sudah dituliskan untuk menjadi penjelas tanpa mengacu jurnal. Bagian abstrak harus menyajikan isi yang merangkum tujuan yaitu menggunakan Algoritma kriptografi AES digunakan untuk proses penyandian email dengan metode, hasil dan kesimpulan yang sudah tertuang dalam abstrak. Abstrak ini pun sudah dilengkapi oleh Bahasa Indonesia dan Bahasa Inggris dengan masing-masing memiliki kata kunci dengan tidak lebih dari 5 kata.
3. Pada pendahuluan sudah jelas terdapat berisi latar belakang mengapa penelitian dilakukan, uraian permasalahan yang akan diteliti, dikaitkan dengan teori, dan diakhiri dengan tujuan dilaksanakan penelitian tersebut
4. Untuk Hasil dan Analisa disajikan tampilan website nya dengan enkripsi dan dekripsi sudah berfungsi dengan baik

Kekurangan

1. Pada Metode sudah dijelaskan bagaimana Langkah langkahnya tetapi menurut kami untuk setiap langkahnya belum dijelaskan secara detail sehingga pembaca harus mencari berbagai referensi lagi
2. Pada metode terdapat gambar yang tidak jelas sehingga pembaca kesulitan membaca diagram tersebut