Terbit online pada laman web jurnal : **http://jurnal.iaii.or.id**

JURNAL RESTI

(Rekayasa Sistem dan Teknologi Informasi)

Vol. 2 No. 3 (2018) 783 – 791 ISSN : 2580-0760 (media online)

Komparatif Performance Model Keamanan Menggunakan Metode Algoritma AES 256 bit dan RSA

Nizirwan Anwar[a], Munawwar[b], Muhammad Abduh[c], Nugroho Budhi Santosa[d]

[a, b, c] Program Studi Teknik Informatika, Fakultas Ilmu Komputer Universitas Esa Unggul

[d] Program Studi Teknik Industri, Fakultas Teknik Universitas Esa Unggul

Abstract

Along with the rapid development of information technology, the ability to access and provide information to users is getting quicker and more accurate, Therefore, protecting those from any unauthorized access is very important. Cryptography can be use as they're one of the fields of information technology development to secure data or messages that are personal and confidential. So, it takes a security to prevent things that are not desired. In this case, the message sending process will be encrypted (plaintext to ciphertext) and the recipient of the message will need to be decrypted (ciphertext to plaintext). The algorithm that we will be using are 256-bit American Encryption Standard (AES) symmetric encryption and RSA asymmetric encryption. Performance testing (size and time-process), integrity ("data integrity"), confidentiality, and "non-repudiation" of data or message security with the algorithm method above will refer to 4 (four) modern cryptographic objectives developed. Those algorithm will be used to encode data stored in document files and implementing it using Python 3.0 language and some support applications. And the results of the process of designing and testing data (text and images) obtained did not experience significant growth, but the encryption / decryption of the RSA algorithm method is much slower than the performance of the AES algorithm time-processing method

Keywords: Cryptography, Encryption, Decryption, AES-256, RSA

Abstrak

Seiring dengan berkembangnya teknologi informasi yang semakin pesat, kemampuan untuk mengakses dan menyediakan informasi ke pengguna semakin cepat dan akurat. Maka dari itu, melindungi informasi tersebut terhadap pihak yang tidak berwenang merupakan suatu hal yang penting. Kriptografi dapat digunakan karena kriptografi adalah salah satu bidang pengembangan teknologi informasi untuk mengamankan data atau pesan yang bersifat pribadi dan rahasia. Sehingga, dibutuhkan sebuah pengamanan untuk mencegah hal-hal yang tidak di inginkan. Dalam hal ini proses pengiriman pesan akan melakukan enkripsi (plainteks ke ciphertext) dan penerima pesan perlu dilakukan dekripsi (ciphertext ke plainteks), Algoritma yang akan digunakan adalah algoritma simetrik "American Encryption Standard" (AES) 256-bit dan asimetrik (RSA). Pengujian performa (ukuran dan time-proses), keutuhan ("data integrity"), kerahasiaan, dan "non-repudiation" keamanan data atau pesan dengan metode algoritma di atas akan merujuk pada 4 (empat) tujuan kriptografi modern dikembangkan. Algoritma tersebut digunakan untuk menyandikan data yang disimpan dalam file dokumen dan mengimplementasinya menggunakan bahasa Python 3.0 dan beberapa aplikasi yang didukung. Dan hasil proses perancangan dan pengujian data (teks maupun gambar) diperoleh tidak mengalami perubahan yang signifikan, akan tetapi enkripsi/dekripsi pada metode algoritma RSA jauh lebih lambat dibandingkan kinerja time-processing metode algoritma AES.

Kata kunci: Kriptografi, Enkripsi, Dekripsi, AES-256, RSA

© 2018 Jurnal RESTI

1. Pendahuluan

Pada perkembangan teknologi saat ini, manusia banyak tergantung pada bidang teknologi informasi. Dengan semakin majunya teknologi memungkinkan manusia untuk bertukar informasi, ataupun bertukar data. Keuntungan yang diberikan dalam teknologi juga diiringi dengan dampak negatif dan ketidaknyamanan, yaitu kejahatan dalam pencurian data. Mengingat sangat pentingnya sebuah data menyajikan data, dapat digunakan oleh pihak tertentu. Jatuhnya informasi data kepada pihak lain yang tidak diinginkan dapat merugikan bagi pihak yang tidak memegang otoritas informasi data. Dengan demikian keamanan dari penyimpanan data yang digunakan haruslah terjamin dalam batas yang dapat diterima sesuai dengan 4 (empat) prinsip dalam kriptografi [3][2][6].

Diterima Redaksi : 22-10-2018 | Selesai Revisi : 13-12-2018 | Diterbitkan Online : 20-12-2018

Berdasarkan latar belakang tersebut, kami akan menggunakan konsep kriptografi untuk mengamankan data tersebut dan kami akan membahas bagaimana implementasi performa (keutuhan data dan waktu proses enkripsi/ dekripisi) keamanan data dengan menggunakan metode algoritma AES 256 bit dan RSA.

2. Tinjauan Pustaka

Kriptografi berasal dari bahasa Yunani, yang terdiri dari dua kata yaitu kata *crypto* yang berarti rahasia dan *graphia* diartikan sebagai tulisan. Kriptografi (*cryptography*) berasal dari bahasa Yunani: "cryptos" yang artinya "secret" (rahasia) dan "graphein" yang artinya "writing" (tulisan). Jadi kriptografi berarti "secret writing" (tulisan rahasia). Kriptografi adalah ilmu dan seni untuk menjaga keamanan ketika pesan dikirim dari suatu tempat ke tempat lain **[4].**

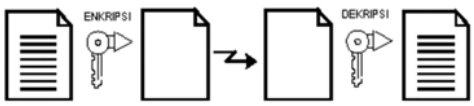
Proses kriptografi terdiri dari 2 (dua) tahapan yaitu proses enkripsi dan dekripsi. Kedua proses tersebut berfungsi untuk mentransformasikan data asli atau lebih dikenal dengan istilah plaintext dan data sandi yang dikenal dengan ciphertext. Bila direpresentasikan dalam rumus matematis diempiriskan sebagai berikut, asumsikan plaintext = P, ciphertext = C, enkripsi = E dan = D maka akan diperoleh persamaan sebagai berikut:

$$E(P) = C \text{ (proses enkripsi)} \quad (1)$$

$$D(C) = P \text{ atau } D(E(P)) = P \text{ (proses dekripsi)} \quad (2)$$

2.1 Algoritma Simetrik

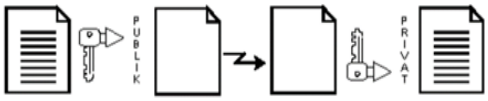
Algoritma Simetri adalah salah satu jenis kunci pada algoritma kriptografi yang menggunakan kunci enkripsi yang sama dengan kunci dekripsinya. Bila mengirim pesan dengan menggunakan algoritma ini, si penerima pesan harus diberitahu kunci dari pesan tersebut agar bisa mendekripsikan pesan yang dikirim.



Gambar 1 Proses Algoritma Simetrik [8]

2.2 Algoritma Asimetrik

Algoritma asimetrik sering juga disebut dengan algoritma kunci publik. Kunci yang digunakan untuk melakukan enkripsi dan dekripsi berbeda, atau dengan dekripsi lain merupakan algoritma yang dengan kunci yang berbeda.



Gambar 2 Proses Algoritma Asimetrik [8]

2.3 Elemen dan Tujuan Kriptografi

Komponen kriptografi [2][5][8] pada dasarnya terdiri dari beberapa elemen pokok antara lain :

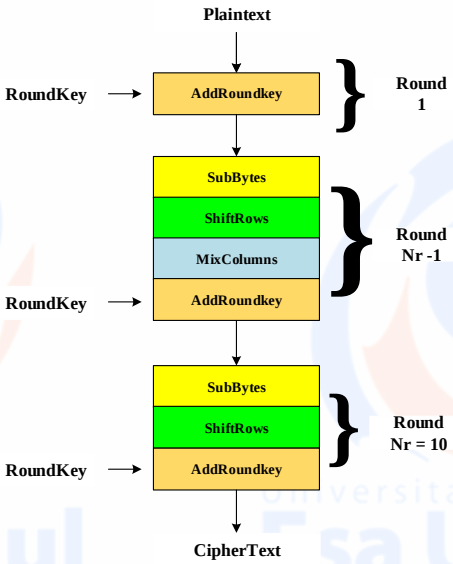
(a) Pesan (*message*)
(b) Pengirim dan Penerima (*receiving and transmitting*)
(c) Enkripsi/Dekripsi (*encryption/ decryption*)
(d) Kunci (*Key*), terdiri kunci p*ublic* dan *private*

Tujuan mendasar dari teknologi kriptografi (proses transformasi message plaintext ke ciphertext dan sebaliknya) ini merupakan untuk pengamanan data/informasi [6][1] :

(a) Kerahasiaan (*Confidentialty*), layanan yang bertujuan memberikan kerahasiaan pesan dan menyimpan data dengan menyembunyikan informasi lewat teknik-teknik enkripsi kepada siapa pun kecuali pemegang otoritas atau kata kunci untuk membuka informasi yang telah di enkripsi tersebut.
(b) Integritas data (*Data Integrity*), layanan untuk memberikan jaminan bahwa pesan tidak akan mengalami perubahan dari saat dibuat sampai dibuka.
(c) Autentikasi (*Authentication*), layanan untuk identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Layanan ini juga berfungsi untuk menguji identitas seseorang apabila ia akan memasuki sistem tersebut
(d) Non-repudiasi (*Non-Repudiation*), layanan untuk membuktikan bahwa suatu data ataupun dokumen datang dari seseorang apabila yang bersangkutan menyangkal memiliki data ataupun dokumen tersebut.

2.4 Metode Algoritma Simetrik AES (*Advanced Encryption Standard*)

Kriptografi algoritma AES merupakan standar enkripsi dengan kunci-simetris yang diadopsi oleh pemerintah Amerika Serikat, AES dipublikasikan oleh *Institut Nasional Standar dan Teknologi* (NIST) sebagai Standar Pemrosesan Informasi Federal (FIPS) publikasi 197 (FIPS197) pada tanggal 26 November 2001. Dan AES [7] muncul sebagai suatu kebutuhan akan adanya standar keamanan baru untuk menggantikan *Data Encryption Standard* (DES) yang semakin lama semakin mudah di bobol (*unsecure*), terutama sejak adanya perangkat keras khusus yang mampu memecahkan algoritma kriptografi DES. Proses enkripsi algoritma AES 256 (gambar 3) terdiri dari 4 (empat) jenis transformasi yang akan dijalankan, yaitu *SubBytes, ShiftRows, MixColumns* dan *AddRoundKey* awal proses enkripsi, input yang telah disamakan atau diduplikasi ke dalam state akan mengalami transformasi *SubBytes ,ShiftRows, Mixcolumns* dan *AddRoundKey* secara berulang sesuai banyaknya Nr=10, jumlah kunci Nk = 8 dan ukuran blok Nb=4.



Gambar 3 Proses Enkripsi AES 256 bit [13]

AddRoundKey

Pada proses transformasi enkripsi dan dekripsi AES 256-bit, sebuah round key ditambahkan pada *state* dengan operasi XOR. Setiap *round key* terdiri dari Nb word di mana tiap word tersebut akan dijumlahkan dengan word atau kolom yang bersetaraan w_i [9] dari *state* sehingga :

$$[s'o,c\ ,\ s'1,c\ ,\ s'2,c\ ,\ s'3,c\ ] * [so,c\ ,\ s1,c\ ,\ s2,c\ ,\ s3,c] \oplus [wround*Nb+c\ ] \quad (3)$$

Dengan i = round*Nb+c.

SubBytes

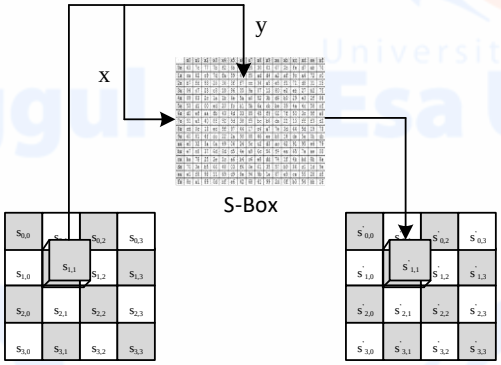
SubBytes merupakan transformasi byte dimana setiap elemen pada state akan dipetakan dengan menggunakan sebuah tabel subtitusi (S-Box). Tabel subtitusi S-Box akan dipaparkan dalam tabel 1. Untuk setiap byte pada array state, misalkan S[r,c]=xy, yang dalam hal ini xy adalah digit heksadesimal dari nilai S[r,c], maka nilai subtitusinya, dinyatakan dengan S[r,c], adalah elemen di dalam tabel subtitusi yang merupakan pengaruh pemetaan byte pada setiap byte dan state (gambar 3).

ShiftRows

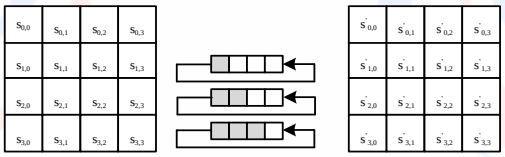
Shift Rows adalah sebuah proses yang melakukan pergeseran dalam elemen blok/tabel yang harus dilakukan per baris, baris pertama tidak harus dilakukan pergeseran 2 byte lalu setelah itu baris yang keempat dilakukan pergeseran 3 bytes, berikut pada gambar 4.

Tabel 1 S-Box [9]

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



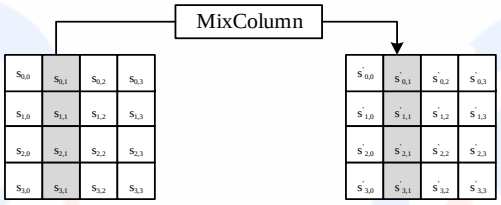
Gambar 4 Pengaruh Pemetaan pada setiap byte dalam state [9]



Gambar 4 Proses ShiftRows [9]

MixColumns

MixColumn adalah proses perkalian tiap elemen dari blokcipher dengan matriks (gambar 5 dan persamaan 4)

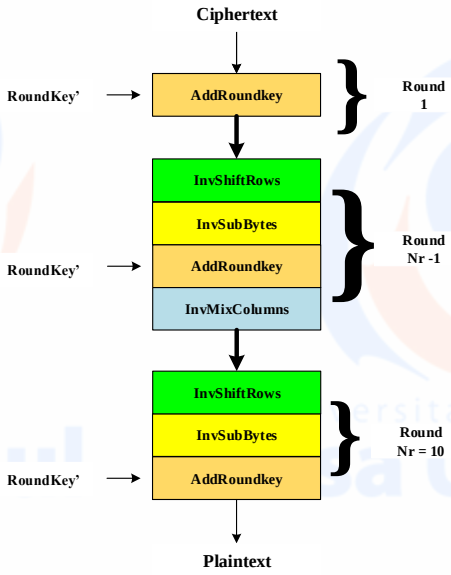


Gambar 5 MixColumn [9]

$$\begin{pmatrix} s'0,1 \\ s'1,1 \\ s'2,1 \\ s'3,1 \end{pmatrix} = \begin{pmatrix} 2\ 3\ 1\ 1 \\ 1\ 2\ 3\ 1 \\ 1\ 1\ 2\ 3 \\ 3\ 1\ 1\ 2 \end{pmatrix} \begin{pmatrix} s0,1 \\ s1,1 \\ s2,1 \\ s3,1 \end{pmatrix} \quad (4)$$

Proses Dekripsi AES-256 bit, tahapan transformasi byte digunakan proses invers cipher ke plaintext adalah InvShiftRows, InvSubBytes, InvMix-

Columns, dan AddRoundKey. Algoritma dekripsi dapat dilihat pada skema (gambar 6)



Gambar 6 Proses Dekripsi AES 256 bit [13]

a. Metode Algoritma Asimetrik RSA (Rivest, Shamir, dan Adleman)

Algoritma RSA, dipublikasikan pada tahun 1977 di MIT yang bertujuan untuk menjawab tantangan dari algoritma pertukaran kunci Diffie Helman. RSA merupakan algoritma yang paling handal untuk digital signature (enkripsi/dekripsi). Keamanan enkripsi dan dekripsi algoritma RSA terletak pada kesulitan untuk memfaktorkan modulus n yang sangat besar. Pelabelan algoritma RSA diambil dari nama penemunya, yaitu Rivest, Shamir dan Adleman [5][10]. Algoritma RSA beroperasi dengan pola skema block cipher, yaitu sebelum dilakukan enkripsi, plainteks yang ada dibagi ke dalam blok-blok yang sama panjang dimana plainteks dan cipherteksnya berupa integer antara 1 sampai n dengan n biasanya berukuran 1024 bit dan panjang bloknya berukuran tidak lebih dari log (n) + 1 dengan basis (module) 2. Fungsi enkripsi dan dekripsi algoritma RSA adalah sebagai berikut.

Fungsi enkripsi

$$C = M^e \bmod n \quad (5)$$

Fungsi dekripsi

$$M = C^d \bmod n \quad (6)$$

dimana: C = cipherteks; M = *message* (plainteks); e = kunci public dan d = kunci private.

Untuk pembangkitan pasangan kunci RSA, digunakan algoritma sebagai berikut:

(1) Memilih dua buah bilangan prima sembarang yang besar, p dan q, dengan syarat nilai p dan q wajib dirahasiakan.
(2) Menghitung n = p x q (bersifat public)
(3) Menghitung m = (p – 1)*(q – 1). (bersifat public)
(4) Dipilih sebuah bilangan bulat sebagai kunci publik, disebut namanya e, yang relatif prima terhadap m. e relatif prima terhadap m artinya faktor pembagi terbesar keduanya adalah 1, secara matematis disebu (e,m)

3. Metodologi Penelitian

Metode penelitian dalam menyelesaikan permasalahan pengujian performa implementasi kriptografi dengan algoritma AES dan RSA, dilakukan dengan pendekatan hipotesis dan eksperimental dengan menggunakan data secara random (acak).

3.1 Pengumpulan data

Metode dalam pengumpulan dilakukan dengan dengan beberapa pendekatan antara lain;

(1) Studi pustaka diperoleh dari buku, jurnal, dan prosising
(2) Hipotesis dan eksperimental dengan pengamatan secara langsung pada proses pengujian dan implementasi dari aplikasi yang dibangun.

3.2. Instrumen Penelitian

Dalam pelaksanaan penelitian dibutuhkan beberapa instrumen pendukung antara lain ;

Perangkat lunak (*Software*)

Software yang dibutuhkan dalam penelitian ini sebagai berikut ;

(1) Sistem operasi Windows 10 Pro (64bit)
(2) Web browser Google Chrome / Mozilla/ Firefox
(3) Pengolah kata Microsoft Word/Excel 2010
(4) Platform program Python 3.0
(5) Microsoft Visio

Perangkat Keras (*Hardware*)

Hardware dibutuhkan juga dalam penelitian ini sebagai berikut ;

(1) Processor Intel(R) Core (TM) i3 - i7 CPU M640 @240Hz 2.4 Ghz
(2) RAM 2.00 – 4.00 GB
(3) System type base 32 – 64 bit

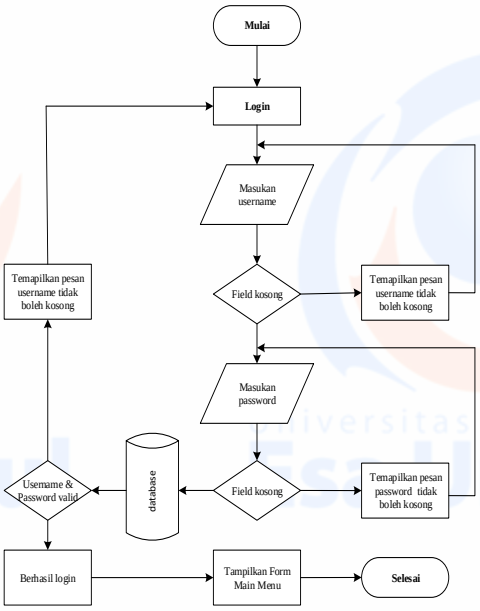
3.3 Rancangan Arsitektur dan Algoritma Kriptografi

Diagram Alir (*flowchart*)

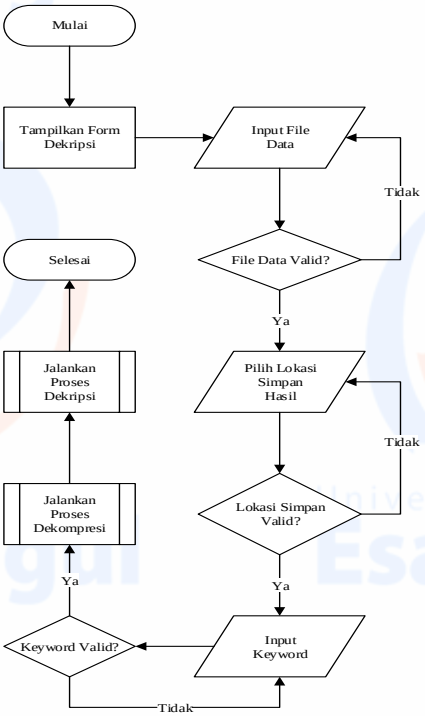
Diagram alur, simbol untuk menggambarkan dan menguraikan alur beserta tahapan proses, berikut ini adalah *flowchart* untuk masing-masing setiap proses,

(1) Proses Login ke aplikasi
(2) Proses Enkripsi

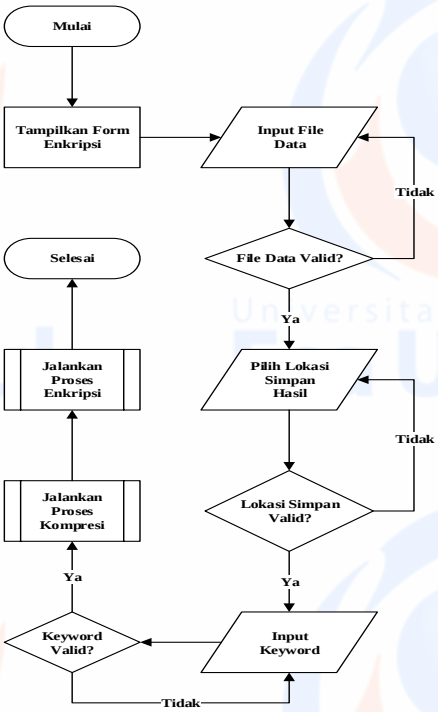
(3) Proses Dekripsi
(4) Password (mengubah)



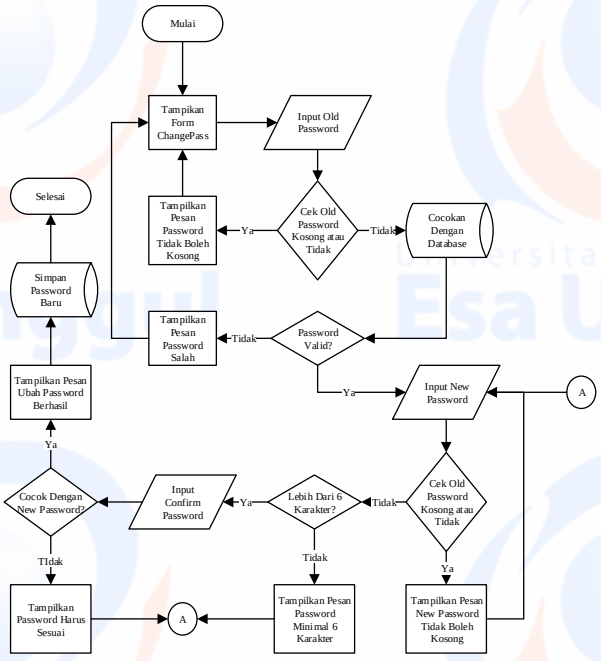
Gambar 7 Diagram Alir Proses Login



Gambar 9 Diagram Alir Proses Dekripsi



Gambar 8 Diagram Alir Proses Enkripsi



Gambar 9 Diagram Alir Proses Mengubah Password

Proses algoritma form login

Input Username dan Password
If "Login" then
Cari ketabel Login berdasarkan fieldUsername dan fieldPassword
If "Username kosong" then
Tampilkan pesan "Username Tidak Boleh Kosong"
Elseif "Password kosong" then
Tampilkan pesan "Password Tidak Boleh Kosong"

```
    End if
Else
    Cocokan Dengan Database
        If "Data Valid"
            Tampilkan Form Main Menu
        Else
            Tampilkan pesan "Username atau Password salah"
        End if
End if
```

Proses algoritma form enkripsi

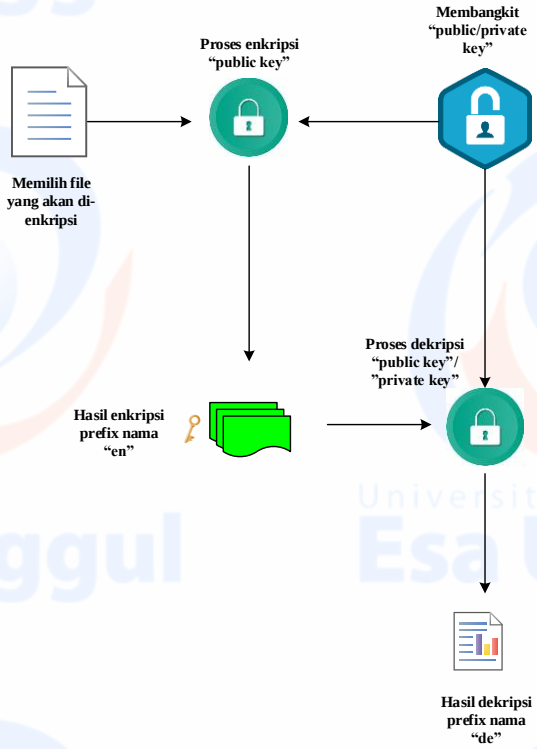
```
Input File Data
If "File Data Valid" then
    Pilih Lokasi Simpan Hasil
        If "Lokasi Simpan Valid" then
            Input Keyword
                If "Keyword Valid" then
                    Jalankan Proses Enkripsi
                    Jalankan Proses Kompresi
                Else
                    Input Keyword
                End if
        Else
            Pilih Lokasi Simpan Hasil
        End if
Else
    Input File Data
End if
```

Proses algoritma form dekripsi

```
Input File Data
If "File Data Valid" then
    Pilih Lokasi Simpan Hasil
        If "Lokasi Simpan Valid" then
            Input Keyword
                If "Keyword Valid" then
                    Jalankan Proses Dekompresi
                    Jalankan Proses Dekripsi
                Else
                    Input Keyword
                End if
        Else
            Pilih Lokasi Simpan Hasil
        End if
Else
    Input File Data
End if
```

Proses algoritma form mengubah password

```
Input Old Password
Cocokan dengan Database
If "Password Valid" then
    Input New Password
        If "Lebih dari 6 Karakter" then
            Input Confirm Password
                If "Confirm Password Valid" then
                    Tampilkan Pesan "Password Berhasil Diganti"
                    Simpan Password kedalam Database
                Else
                    Input New Password
                End if
        Else
            Tampilkan Pesan "Password Minimal 6 Karakter"
        End if
Else
    Tampilkan Pesan "Old Password Incorrect"
End if
```



Gambar 10 Arsitektur Proses Enkripsi dan Dekripsi

Rancangan Tampilan

Tampilan layar tampilan pertama saat aplikasi dibuka dimana user harus mengentry ID username dan password sebelum masuk ke dalam menu utama

Gambar 11 Tampilan Login
Arsitektur Proses dan Hasil Enkripsi/Dekripsi

Tampilan layar pada form ini merupakan alur proses untuk melakukan enkripisi file

Gambar 12 Tampilan Enkripsi

Tampilan layar pada form ini merupakan alur proses untuk melakukan dekripsi file

Gambar 13 Tampilan Dekripsi

Berikut adalah tampilan layar menu utama dimana *user* dapat memilih untuk melakukan proses mengubah password sekarang

Gambar 14 Tampilan Mengubah Password

3.4 Data Pengujian

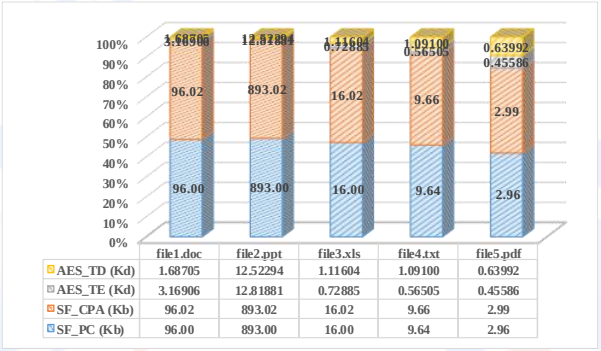
Pengujian performance pada kedua metode algoritma tersebut dengan kriteria sebagai berikut;

(1) Tipe file yang digunakan adalah dengan format teks (*.doc, , *.txt, *.xls, *.ppt, *.pdf)
(2) Tipe file dengan format compress *image* (bmp, tif, png, jpg dan gif).
(3) Ukuran file sesuai point (1) dan (2) dengan mempunyai ukuran file ≤ 10 MB.

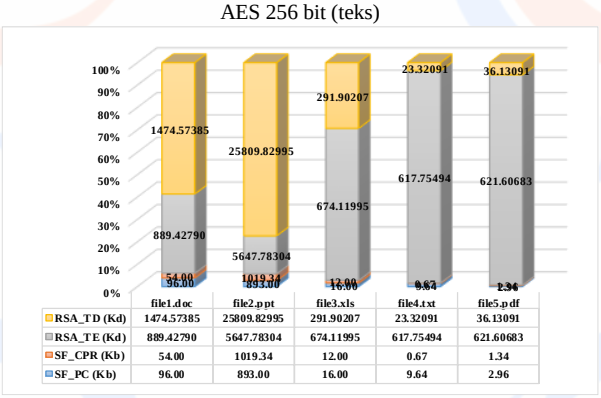
4. Hasil dan Pembahasan

4.1 Pengujian dan pembahasan waktu dan ukuran file enkripsi / dekripsi AES 256 bit dan RSA (teks)

Analisis untuk gambar 14 dan tabel 2, metode algoritma AES (enkripsi dan dekripsi) data teks tidak diperoleh perubahan yang signifikan dalam ukuran file, secara rata2 ≅ 100.33 %. Proses plaintext ke ciphertext dan ciphertext ke plaintext file tetap terjaga keutuhannya. Dan pada aspek hubungan waktu proses dan ukuran file proses enkripsi secara rata2 diperoleh ≅ 6.11 % dan proses dekripsi ≅ 5.86 % (gambar 16).



Gambar 14 Grafik Ukuran dan Waktu Enkripsi dan Dekripsi AES 256 bit (teks)

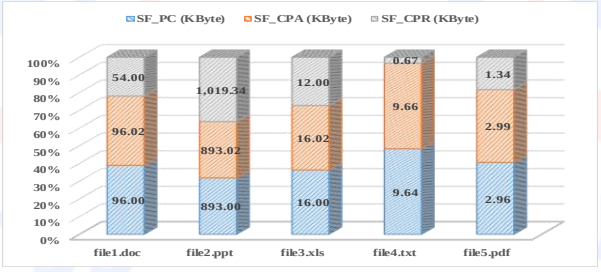


Gambar 15 Grafik Ukuran dan Waktu Enkripsi dan Dekripsi RSA (teks)

Analisis untuk gambar 15 dan tabel 2, metode algoritma RSA (enkripsi dan dekripsi) data teks mengalami pengurangan yang sangat signifikan dalam ukuran file, secara rata - rata ≅ 59.50 %. Proses plaintext ke ciphertext dan ciphertext ke plaintext file tetap terjaga keutuhannya. Dan pada aspek hubungan waktu proses dan ukuran file proses enkripsi secara rata2 diperoleh ≅ 6640.53 % dan proses dekripsi ≅ 1539.27 %, terjadi peningkatan waktu proses enkripsi/dekripsi. (gambar 16)

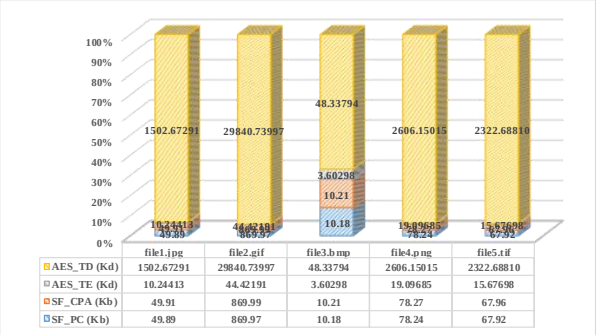
Tabel 2 Perbandingan Ukuran File (teks)

No.	NF	SF_PC (Kb)	SF_CPA (Kb)	SF_CPA (Kb)
1	file1.doc	96.00	96.02	54.00
2	file2.ppt	893.00	893.02	1,019.34
3	file3.xls	16.00	16.02	12.00
4	file4.txt	9.64	9.66	0.67
5	file5.pdf	2.96	2.99	1.34



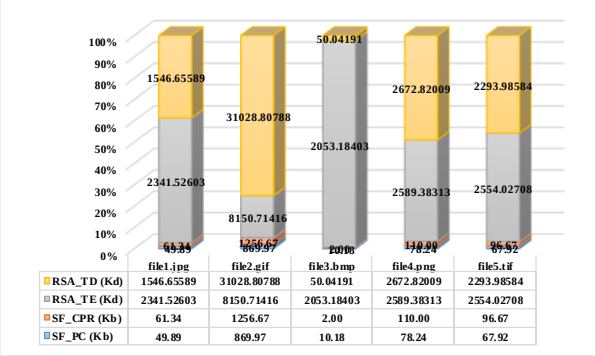
Gambar 16 Grafik Perbandingan Ukuran File (teks)

4.2 Pengujian dan pembahasan waktu dan ukuran file enkripsi / dekripsi AES 256 bit dan RSA (*image*)



Grafik 17 Grafik Ukuran dan Waktu Enkripsi dan Dekripsi AES 256 bit (*image*)

Analisis untuk tabel 3 dan gambar 17, metode algoritma AES (enkripsi dan dekripsi) data *image* tidak diperoleh perubahan yang signifikan dalam ukuran file, secara rata2 ≅ 100.10 %. Proses plaintext ke ciphertext dan ciphertext ke plaintext file tetap terjaga keutuhannya. Dan pada aspek hubungan waktu proses dan ukuran file proses enkripsi secara rata2 diperoleh ≅ 21.71 % dan proses dekripsi ≅ 2732.23 % (gambar 19)

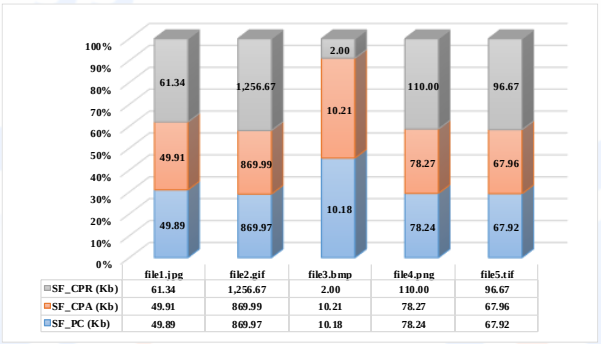


Grafik 18 Grafik Ukuran dan Waktu Enkripsi dan Dekripsi RSA (*image*)

Analisis untuk tabel 3 dan gambar 18, metode algoritma RSA (enkripsi dan dekripsi) data teks mengalami pengurangan yang sangat signifikan dalam ukuran file, secara rata2 ≅ 113.99 %. Proses plaintext ke ciphertext dan ciphertext ke plaintext file tetap terjaga keutuhannya. Dan pada aspek hubungan waktu proses dan ukuran file proses enkripsi secara rata2 diperoleh ≅ 6640.53 % dan proses dekripsi ≅ 1539.27 %, terjadi peningkatan waktu proses enkripsi/dekripsi. (gambar 19)

Tabel 3 Perbandingan Ukuran File (*image*)

No.	NF	SF_PC (Kb)	SF_CPA (Kb)	SF_CPA (Kb)
1	file1.jpg	49.89	49.91	61.34
2	file2.gif	869.97	869.99	1,256.67
3	file3.bmp	10.18	10.21	2.00
4	file4.png	78.24	78.27	110.00
5	file5.tif	67.92	67.96	96.67



Gambar 19 Grafik Perbandingan Ukuran File (*image*)

Keterangan ;

NF = nama file; SF_PC = ukuran file plaintext; SF_CPA = ukuran file ciphertext AES; SF_CPR = ukuran file ciphertext RSA; AES_TE = waktu proses enkripsi AES; AES_TD = waktu proses dekripsi AES; RSA_TE = waktu proses enkripsi RSA; RSA_TD = waktu proses dekripsi RSA; NFE = nama file luaran enkripsi; NFD = nama file luaran dekripsi

5. Kesimpulan

Bagian terdiri atas simpulan dan saran atas penelitian hasil penelitian.

5.1 Simpulan

Kesimpulan yang diperoleh diuraikan sebagai berikut :

(1) Berdasarkan data eksperimen di atas, performa algoritma AES jauh lebih cepat dibanding RSA. Dengan rata – rata ≅ 236x lebih cepat pada saat proses enkripsi dan ≅ 2.5x lebih cepat pada saat dekripsi.

(2) Dari sisi sekuritas, RSA dapat dikatakan lebih aman dibanding AES karena memiliki key yang simetris. Akan tetapi, keamanan tersebut memiliki penalti terhadap performa waktu dan pembaca diharapkan untuk mempertimbangkan apakah sekuritas itu lebih penting daripada performa waktu.

(3) Aplikasi keamanan data dengan menggunakan algoritma simetris AES 256 bit dan asimetris RSA ini telah dapat mengamankan data atau informasi, baik dalam *performance* ukuran dan kualitas data serta waktu proses (enkripsi/dekripsi file) ean terlindungi dalam aspek keamanan datanya, keutuhan data, dan kerahasiaannya dari pihak yang tidak bertanggung jawab (berwenang). Ini dicapai dengan mengimplementasikan konsep kriptografi dan algoritma tersebut ke dalam aplikasi keamanan tersebut.

(4) Terdapat pengurangan atau penambahan data saat proses enkripsi atau dekripsi terjadi, terutama pada metode algoritma RSA. Tetapi, walaupun data mengalami perubahan, integritas data pada

saat dikembalikan menjadi keadaan semula (dekripsi) data tetap sama sehingga integritas data terjaga.

(5) Semakin besar ukuran file yang di enkripsi, maka akan semakin lama waktu yang dibutuhkan dalam metode RSA (asimetris) bilang dikomparasikan dengan AES (simetris). Perbandingan waktu rata – rata enkripsi file size terbesar dengan rata – rata file size setiap algoritma sebesar ≅ 2.6x lebih lama sedangkan RSA memerlukan 4.35x lebih lama pada saat proses dekripsi dibandingkan AES yang memerlukan waktu 2.6x lebih lama — sama dengan waktu enkripsi.

5.2 Saran

Penelitian ini dapat dikembangkan kembali dengan menggunakan algoritma dengan pendekatan hybrid dengan model kasus yang lebih spesifik. Masukan dan saran kami sangat mengharapkan agar di kemudian hari naskah ini dapat bermanfaat.

Ucapan Terima Kasih

Ucapan terima kasih disampaikan kepada pihak-pihak yang membantu pelaksanaan penelitian. Peneltian ini dibiayai oleh Direktorat Riset dan Pengabdian Masyarakat, Direktorat Jendral Penguat Riset dan Pengembangan Kementerian Riset, Teknologi dan Pendidikan Tinggi Sesuai dengan Kontrak Penelitian Nomor 020/KM/PNT/2018 dengan skema penelitian dasar unggulan perguruan tinggi (PDUPT) tahun 2018, dan mengucapkan terima kasih pada pihak-pihak lain yang tidak disebutkan satu per satu atas dukungan dan bantuannya.

Daftar Rujukan

[1] Schneier, Bruce. 1996. Applied Cryptography. Second Edition, John Wiley & Sons.
[2] Stallings, William. 2013. Cryptography and Network Security : Principles and Practice Sixth Edition. Prentice Hall.
[3] Munir, Rinaldi. 2006. Kriptografi. Penerbit Informatika. Bandung
[4] Donny, Ariyus. 2007. Pengantar Ilmu Kriptografi : Teori, Analisis, dan Implementasi. Penerbit Andi Offset. Yogyakarta.
[5] Menezes, Oorchshot,& Vanstone. 1996. Handbook of Applied Cryptography. CRC Press. Florida
[6] Stinson, Douglas R. 2006. Cryptography: theory and Practice Third Edition. CRC Press. Florida.
[7] R. Shah Kruti ., Bhavika Gambhava. 2012. New Approach of Data Encryption Standard Algorithm. http://www.ijsce.org/wp-content/uploads/papers/v2i1/A0444022112.pdf. International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012
[8] Delfs, Hans & Knebl, Helmut. 2015. Introduction to cryptography principles and applications, Symmetric-key encryption. Penerbit Springer. ISBN 9783662479742
[9] Federal Information Processing Standards Publication 197. 2001. Advanced Encryption Standard (AES).
[10] Marwan Ali Albahar, Olayemi Olawumi, Keijo Haataja, Pekka Toivanen. 2018. Novel Hybrid Encryption Algorithm Based on Aes, RSA, and Twofish for Bluetooth Encryption. Journal of Information Security, 2018, 9, 168-176 https://file.scirp.org/pdf/JIS_2018040814373482.pdf. ISSN Online: 2153-1242
[12] Prabhakar Telagarapu Birendra Biswal Vijaya Santhi Guntuk. 2011. Design and Analysis of Multimedia Communication System. IEEE- Third International Conference on Advanced Computing, ICoAC 2011 MIT, Anna University, Chennai. December 14-16, 2011

Universitas Esa Unggul
LPPM

SURAT KETERANGAN

No. 021/S.Ket-Penelitian/LPPM/UEU/II/2019

Yang bertanda tangan di bawah ini :

Nama : Dr. Erry Yudhya Mulyani, M.Sc

Jabatan : Kepala LPPM

Menerangkan dengan sebenarnya bahwa :

No	Nama	NIDN	Fakultas
1	Ir. Nizirwan Anwar, MT	0018107001	Ilmu Komputer
2	Ir. Munawar MMSI., M.Com, PhD	0324047005	Ilmu Komputer
3	Mukhammad Abduh, ST, MT	0319127407	Teknik
4	Nugroho Budhi Santosa, ST, MMSI	0321066601	Ilmu Komputer

Telah melakukan penelitian dan hasilnya diterbitkan pada jurnal "JURNAL RESTI (Rekayasa Sistem dan Teknologi Informasi) Volume 2, No 3 (2018) 783-791, ISSN: 2580-0760 dengan judul yaitu "Komparatif Performance Model Keamanan Menggunakan Metode Algoritma AES 256 bit dan RSA".

Demikian surat keterangan ini dibuat untuk dipergunakan sebagaimana mestinya.

Jakarta, 20 Februari 2019
Kepala LPPM,

Universitas Esa Unggul LPPM

Dr. Erry Yudhya Mulyani, M.Sc
NIK. 209100388