ANALISIS PERFORMANSI KRIPTOGRAFI MENGGUNAKAN ALGORITMA AFFINE CIPHER, VIGENERE CIPHER DAN BASE64

Indra Yatini B. [1], Femi Dwi Astuti [2]

[1), 2)] Jurusan Teknik informatika, STMIK AKAKOM Yogyakarta
Jalan Raya Janti 143 Karang Jambe Yogyakarta 55198
Email: indrayatini@akakom.ac.id, femi@akakom.ac.id

ABSTRACT

Security become the most important factor in Information aspect to keep the data unreadable for unauthenticated person. Data security aspect can be improved by usingcryptography for securing the data. This Research will discuss about cryptography algorithm such as : Affine Cipher, Base 64 and Vigenere Chiper in handling the encryption and decryption. This Research used Java programming language. Some examinaton were carried out to know about the perfomance level each algorithm in handling the encryption and decryption process, including the comparison of each perfomance algorithm. The performance comparison of each algorithm based on speed , file size and the analysis of influence of time processing to the running application in text data.

The Conclusion from the speed of the process is the faster algorithm in dealing with the process is the better algorithm. In Affine Chiper algorithm, time required for encryption and decryption is faster than the others.

Keyword: *Kriptografi, komparasi, Affine Cipher, Base64, Vigenere Cipher.*

PENDAHULUAN

Kriptografi merupakan bidang pengetahuan yang menggunakan persamaan matematis untuk melakukan proses enkripsi maupun dekripsi. Teknik ini digunakan untuk mengkonversi data kedalam bentuk kode-kode tertentu sehingga menjadi susunan huruf acak yang terurut dan tidak dapat dibaca. Dalam kriptografi sendiri ada beberapa algoritma atau metode-metode diantaranya *Affine Cipher, Base 64* dan *Vigenere Cipher* yang akan digunakan dalam penelitian ini. Dari ketiga algoritma tersebut mungkin didapati *efisiensi* yang berbeda-beda, dimana *efisien* tidaknya algoritma kriptografi mengarah pada kecepatan dalam proses mengenkripsi atau mendekripsi data, besaran ukuran *file* yang dihasilkan dan pengaruh proses enkripsi-dekripsi terhadap aplikasi yang sedang berjalan.

Setiap algoritma kriptografi pasti mempunyai kelemahan dan kelebihan dalam hal penanganan proses enkripsi maupun dekripsi maka diperlukan analisis untuk mengukur unjuk kerja program melalui uji validitas waktu dan besaran ukuran file yang dihasilkan dari tiap proses eksekusi enkripsi dan dekripsi, dimana algoritma yang efisien ialah algoritma yang meminimumkan kebutuhan ruang dan waktu. Kebutuhan ruang dan waktu suatu algoritma bergantung pada ukuran masukan (input) yang menyatakan jumlah data yang diproses beserta waktu prosesnya.

Tujuan dari penelitian ini adalah membangun suatu aplikasi untuk menganalisis performansi data dari algoritma kriptografi *Affine Cipher, Base-64,* dan *Vigenere Cipher* dengan jenis *file* (berkas) bertipe text (*.txt*) ataupun dokumen (*.doc*) dan dituntut untuk mengembangkan

 ISSN 2088 - 3676

model alat bantu uji yang efisiensi dari program dengan cara mengoptimalkan program dari aspek struktur program maupun struktur data yang digunakan sehingga didapati program yang efisien.

METODE PENELITIAN

Analisis Algoritma

Analisis algoritma dilakukan untuk menduga besarnya sumber daya yang dibutuhkan untuk sembarang ukuran input *n* (Cormer et al.1990) dan T(n) didefinisikan sebagai waktu yang dibutuhkan suatu algoritma untuk menyelesaikan proses dengan *input* berukuran *n*.

Berdasarkan waktu eksekusi program *T(n)*, dapat ditentukan laju pertumbuhan terhadap variasi ukuran file sehingga kompleksitas komputasi dari suatu algoritma memberikan gambaran umum bagaimana perubahan *T(n)* terhadap *n*. Kemungkinan waktu eksekusi ini dapat dipengaruhi oleh faktor-faktor nonteknis implementasi seperti platform atau bahasa pemrograman yang digunakan dan sarana perangkat lunak tertentu.

Tahapan Penelitian

Tahap-tahap yang dilakukan dalam penelitian ini:

1. Tahap pembuatan program enkripsi dan dekripsi pada file teks menggunakan algoritma *Affine Cipher, Base64* dan *Vigenere Cipher* dengan bahasa pemrograman java dimana JAVA *Swing* digunakan untuk membuat tampilan berbasis *Graphical User Interface* (GUI) dan windows7 sebagai sitem operasi.
2. Tahap pengujian program terhadap *file* teks (*.txt*). Pada tahap ini, uji coba dilakukan dengan dengan cara menghitung waktu eksekusi enkripsi-dekripsi data serta mengetahui besaran ukuran *file* yang dihasilkan pada saat proses enkripsi-dekripsi yang ditangani oleh kode program serta mengetahui pengaruh aplikasi yang sedang berjalan secara bersamaan terhadap waktu proses enkripsi-dekripsi.

Spesifikasi Uji Implementasi

Uji implementasi dilakukan dengan menggunakan 10 ukuran *file* teks yang berbeda, dengan ukuran *file* minimum 10 *Byte* dan maksimal *n Byte*, pengujian ini dilakukan penghitungan waktu eksekusi dan besaran ukuran yang dihasilkan dari setiap perlakuan serta menguji pengaruh aplikasi yang sedang berjalan dengan cara menjalankan aplikasi secara bersamaan dengan proses enkripsi-dekripsi dimana aplikasi yang digunakan untuk pengujian ini adalah browser *mozillaFirefox*, *googleCrome*, dan *media player AIMP3*.

Lingkungan Penelitian

Perangkat yang digunakan dalam penelitian ini adalah sebagai berikut :

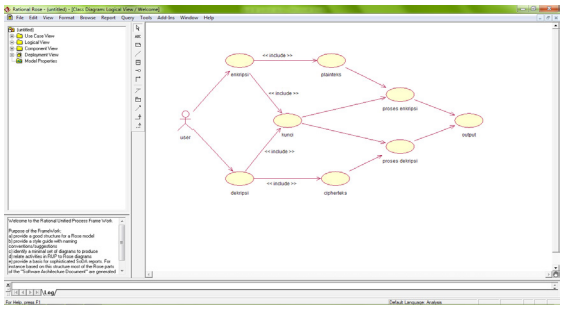
1. Perangkat lunak : sistem operasi windows 7, Netbeans IDE 7.3, JDK (Java Development Kit)
2. Perangkat keras : Intel(R) core(TM) i3-2330M CPU @ 2.20 GHz, RAM 2.00 GB, hardisk 500 GB.

PERANCANGAN SISTEM

Dalam pemodelan sistem, pada pembuatan aplikasi ini menggunakan metode *object oriented* dengan UML (*Unified Modelling Language*). Perancangan yang dibuat pada penelitian ini adalah dengan mengguanakan *use case* diagram

Use case Diagram

Use case diagram diperlukan untuk menggambarkan fungsionalitas yang diharapkan dari perspektif pengguna. Yang ditekankan adalah ”apa” yang dilakukan sistem yang merepresentasikan sebuah interaksi antara aktor dengan sistem. Ditunjukkan dalam gambar relasi-relasi yang terjadi antar *use case*



Gambar 1. *Use Case* Diagram

Pada gambar diatas menunjukkan bahwa user dapat mengakses beberapa fasilitas, yaitu user dapat memasukkan teks atau dokumen yang akan dienkripsi maupun yang akan didekripsi. User juga yang bertugas memasukkan kunci untuk enkripsi maupun dekripsi, user dapat mengakses teks / dokumen hasil dari enkripsi dan dekripsi tersebut.

HASIL DAN PEMBAHASAN

Konsep Program

Program yang dibuat adalah aplikasi enkripsi dan dekripsi pada algoritma *Affine Cipher, Base64,* dan *Vigenere Cipher*. Program ini digunakan untuk mengenkripsi dan mendekripsi sebuah *file* bertipe *file* teks (*.txt*) ataupun dokumen (*.doc*).

Uji Coba

Untuk mengetahui penghitungan kinerja algoritma kriptografi *Affine Cipher, Base64,* dan *Vigenere Cipher* dalam hal waktu eksekusi satuan yang digunakan adalah *millisecond* (*mscd*) dan besaran ukuran yang dihasilkan dalam satuan *Byte* pada pengujian yang dilakukan terhadap file teks (*.txt*). untuk penghitungan besaran ukuran file yang dihasilkan akan ditangani oleh kode program.

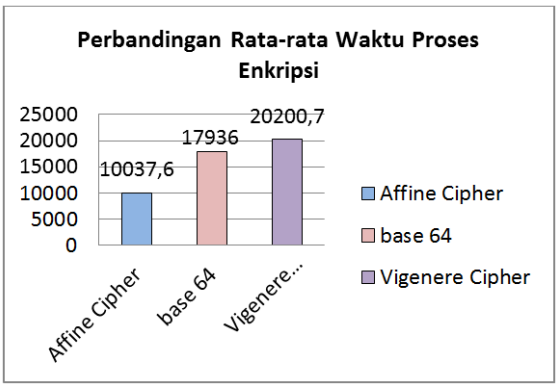
Hasil Implementasi

Implementasi algoritma kriptografi pada penelitian ini menggunakan bahasa pemrograman JAVA. Hal ini didasarkan atas pertimbangan bahasa pemrograman Java mampu membangkitkan bilangan besar dan platform java yang digunakan adalah NETBEANS IDE 7.3.

Uji implementasi dilakukan dengan menggunakan 10 ukuran file teks (*.txt*) yang berbedadengan ukuran minimum 10 *byte* dan maksimal *n byte*, pada pengujian ini diakukan penghitungan waktu eksekusi dari tiap penanganan dan besaran ukuran *file* yang dihasilkan.

Tabel 1. Analisis waktu enkripsi terhadap ukuran file *.txt* pada algoritma kriptografi

ukuran File (*byte*)	Algoritma yang ditangani (enkripsi)		
	Affine Cipher (mscd)	Base 64 (mscd)	Vigenere Cipher (mscd)
10675	445.0	1490.0	1007.0
20896	1287.0	3129.0	2843.0
33094	2953.0	5905.0	5550.0
41691	4235.0	8105.0	8579.0
52380	6708.0	12141.0	13692.0
63072	9566.0	17622.0	19858.0
73898	13145.0	23257.0	25684.0
82864	16073.0	28286.0	32051.0
93172	20643.0	35495.0	40597.0
104040	25321.0	43930.0	52146.0
Rerata waktu enkripsi	**10037,6**	**17936**	**20200,7**

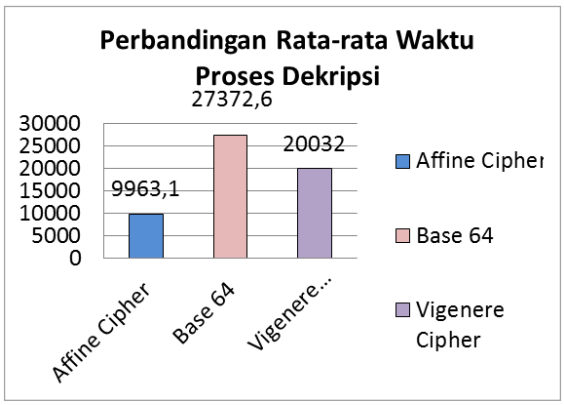


Gambar 2. Grafik perbandingan waktu pada proses enkripsI

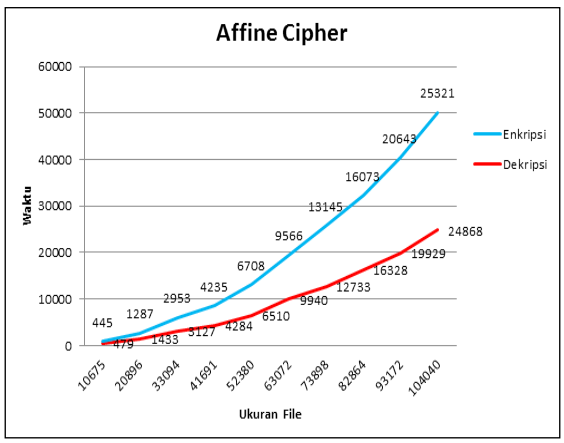
ISSN 2088 - 3676

Tabel 2. Analisis waktu dekripsi terhadap ukuran file *.txt* pada algoritma kriptografi

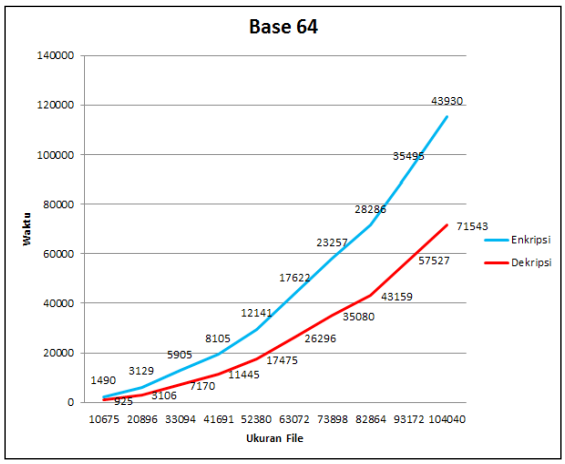
ukuran File	Algoritma yang ditangani (dekripsi)		
	Affine Cipher (mscd)	Base 64 (mscd)	Vigenere Cipher (mscd)
10675	479.0	925.0	785.0
20896	1433.0	3106.0	2715.0
33094	3127.0	7170.0	5604.0
41691	4284.0	11445.0	9089.0
52380	6510.0	17475.0	13427.0
63072	9940.0	26296.0	19808.0
73898	12733.0	35080.0	25699.0
82864	16328.0	43159.0	32666.0
93172	19929.0	57527.0	41276.0
104040	24868.0	71543.0	49251.0
Rerata waktu dekripsi	**9963,1**	**27372,6**	**20032**



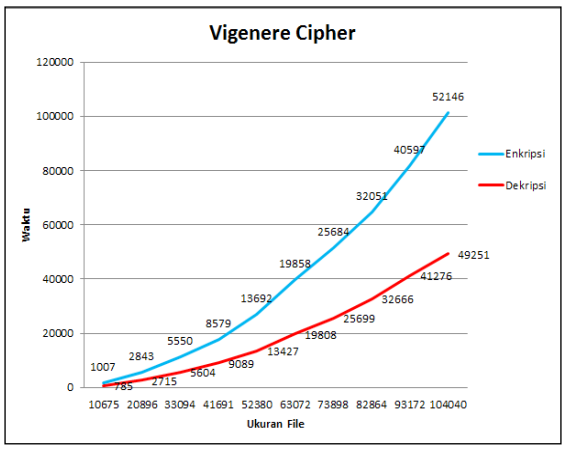
Gambar 3. Grafik perbandingan waktu proses dekripsi



Gambar 4. Grafik korelasi besaran file dengan waktu pada proses *Affine Cipher*.



Gambar 5. Grafik korelasi besaran file dengan waktu pada proses *Base 64*.

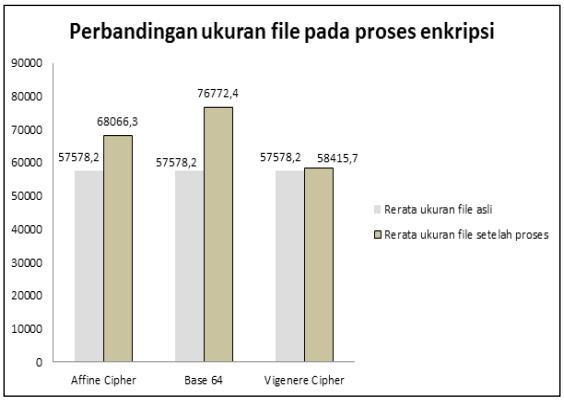


Gambar 6. Grafik korelasi besaran file dengan waktu pada proses *Vigenere Cipher*.

Pada algoritma kriptografi *Vigenere Cipher* kunci yang digunakan adalah AKAKOM. Pada uji coba proses enkripsi dan dekripsi menggunakan ekstensi file *.txt* dengan ukuran yang berbeda–beda dapat disimpulkan bahwa semakin besar ukuran file maka waktu proses enkripsi dan dekripsi file semakin lama. Hal ini disebabkan oleh efek cache dan efek penanganan file (file handling) oleh sistem operasi, begitu sebaliknya untuk proses dekripsi.

Tabel 3. Analisis besaran ukuran file *.txt* pada proses enkripsi

Ukuran File (*byte*)	Ukuran file enkripsi/cipherteks		
	Affine Cipher (*byte*)	Base 64 (*byte*)	Vigenere Cipher (*byte*)
10675	12622	14236	10802
20896	24715	27864	21180
33094	39097	44128	33563
41691	49253	55588	42291
52380	61905	69840	53167
63072	74560	84096	64021
73898	87323	98532	74933
82864	97957	110488	84070
93172	110169	124232	94528
104040	123062	138720	105602
Rerata Ukuran file	**68066,3**	**76772,4**	**58415,7**



Gambar 7. Grafik perbandingan ukuran file yang dihasilkan pada proses enkripsi

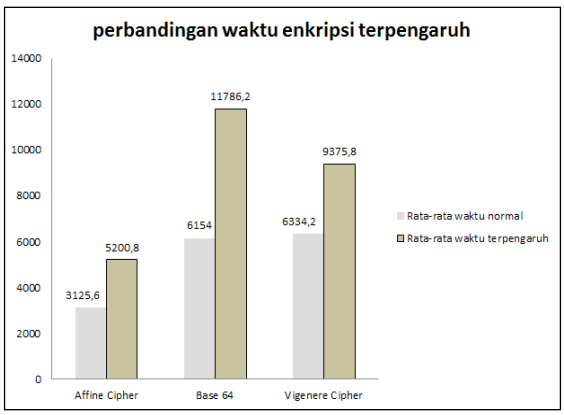
Dari tabel 3. dapat dilihat bahwa ukuran file sebelum proses enkripsi dengan ukuran file setelah proses enkripsi pada algoritma Affine Cipher dan Vigenere Cipher tidak mengalami perubahan yang mencolok. Perubahan yang terjadi sangat kecil, hal ini terjadi karena adanya proses padding. Sedangkan pada Base 64 terjadi perubahan ukuran yang signifikan dikarenakan dalam proses enkripsi terjadi penambahan karakter setiap kelipatan 4. Dan dari grafik di atas dapat dilihat bahwa proses penanganan enkripsi sangat mempengaruhi besaran ukuran file.

Tabel 4. Waktu proses enkripsi secara normal

Ukuran File	Algoritma yang ditangani (enkripsi)		
	Affine Cipher (*mscd*)	Base 64 (*mscd*)	Vigenere Cipher (*mscd*)
10675	445.0	1490.0	1007.0
20896	1287.0	3129.0	2843.0
33094	2953.0	5905.0	5550.0
41691	4235.0	8105.0	8579.0
52380	6708.0	12141.0	13692.0
Rata-rata	**3125,6**	**6154**	**6334,2**

Tabel 5. Perbandingan waktu proses enkripsi terhadap aplikasi yang sedang berjalan

Ukuran File	Proses Enkripsi		
	Affine Cipher terpe-ngaruh (*mscd*)	Base 64 terpe-ngaruh (*mscd*)	Vigenere Cipher terpe-ngaruh (*mscd*)
10675	516	3854	1315
20896	2336	9297	4518
33094	4931	11892	9447
41691	7573	14926	12944
52380	10648	18962	18655
Rerata Waktu	**5200,8**	**11786,2**	**9375,8**



Gambar 8. Grafik perbandingan pengaruh aplikasi berjalan terhadap proses enkripsi

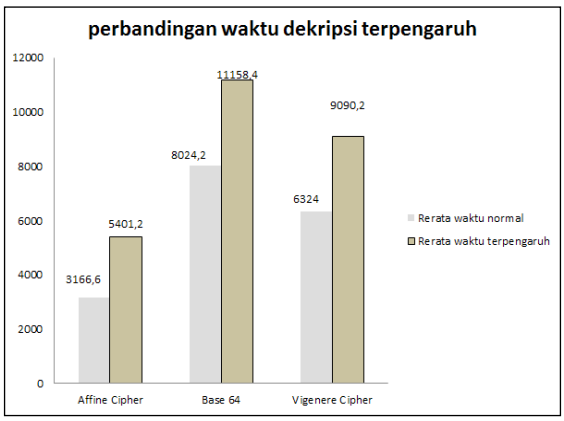
ISSN 2088 - 3676

Tabel 6. Waktu proses dekripsi secara normal

ukuran File	Algoritma yang ditangani (dekripsi)		
	Affine Cipher (*mscd*)	Base 64 (*mscd*)	Vigenere Cipher (*mscd*)
10675	479.0	925.0	785.0
20896	1433.0	3106.0	2715.0
33094	3127.0	7170.0	5604.0
41691	4284.0	11445.0	9089.0
52380	6510.0	17475.0	13427.0
Rata-rata	**3166,6**	**8024,2**	**6324**

Tabel 7. Perbandingan waktu proses dekripsi terhadap aplikasi yang sedang berjalan

Ukuran File	Proses Dekripsi		
	Affine Cipher terpengaruh (*mscd*)	Base 64 terpengaruh (*mscd*)	Vigenere Cipher terpengaruh (*mscd*)
10675	1235	1822	1434
20896	2720	4681	4564
33094	5623	10565	8820
41691	6689	16520	13001
52380	10739	22204	17632
Rerata waktu	**5401,2**	**11158,4**	**9090,2**



Gambar 9. Grafik perbandingan pengaruh aplikasi berjalan terhadap proses enkripsi

Pada Tabel 5 dan tabel 7 digambarkan lebih lanjut pengaruh adanya aplikasi yang berjalan pada waktu yang dibutuhkan pada saat proses enkripsi dan dekripsi. Dari grafik di atas juga, dapat terlihat jelas bahwa banyaknya aplikasi yang berjalan sangat mempengaruhi kecepatan dari proses enkripsi maupun dekripsi. Hal ini disebabkan adanya fungsi scedulling pada sistem operasi yang mengatur processor untuk membagi waktu proses tiap aplikasi yang sedang berjalan. Jadi semakin banyak aplikasi yang berjalan pada sebuah komputer, maka kecepatan proses dari enkripsi dan dekripsi akan semakin berkurang.

KESIMPULAN

Setelah melalui tahap perancangan sistem dan implementasi, serta berdasarkan uraian dan pembahasan pada bab-bab sebelumnya maka dapat diambil kesimpulkan, yaitu:

1. Perangkat lunak yang dibangun dapat menangani proses enkripsi dan dekripsi metode Affine Cipher, Base 64, dan Vigenere Cipher sehingga mampu memberikan hasil dari performansi algoritma kriptografi tersebut.
2. Pada uji coba proses enkripsi dengan menggunakan ekstensi file .doc dengan ukuran yang berbeda–beda dapat disimpulkan bahwa semakin besar ukuran file maka waktu proses enkripsi/ dekripsi file semakin lama.
3. Dalam hal penanganan proses enkripsi, waktu yang dibutuhkan oleh algoritma Affine Cipher lebih cepat dibanding Base 64 dan Vigenere Cipher.
4. besaran ukuran file, pada algoritma Vigenere Cipher ukuran file yang dihasilkan lebih kecil dibanding Affine Cipher dan Base 64 yang menghasilkan ukuran Cipher sangat besar.
5. Terhadap pengaruh aplikasi yang sedang berjalan, dapat disimpulkan bahwa banyaknya aplikasi yang berjalan sangat mempengaruhi kecepatan dari proses enkripsi maupun deskripsi. Hal ini disebabkan adanya fungsi scedulling pada sistem operasi yang mengatur processor untuk membagi waktu proses

tiap aplikasi yang sedang berjalan. Jadi semakin banyak aplikasi yang berjalan pada sebuah komputer, maka kecepatan proses dari enkripsi akan semakin berkurang.

SARAN

Berbagai macam perangkat lunak aplikasi tidak menutup kemungkinan untuk terus dikembangkan dan disempurnakan, begitu pula dengan aplikasi ini. Berikut adalah beberapa saran yang dipandang perlu dalam proses pengembangan berikutnya:

1. Perlu diadakan penelitian yang lebih mendalam tentang sistem kriptografi pada algoritma Affine Cipher, Base 64, dan Vigenere Cipher yang diimplementasikan pada perangkat keras yang berbeda.
2. Dilakukan pengujian algoritma kriptografi Affine Cipher, Base 64 dan Vigenere Cipher untuk menangani proses enkripsi dan dekripsi pada karakter atau simbol-simbol tertentu.
3. Mengembangkan penelitian pada algoritma kriptografi yang lain, selain algoritma kriptografi Affine Cipher , Base 64 dan Vigenere Cipher.

DAFTAR PUSTAKA

Fauzi Nurrikza, 2012, *Enkripsi dan Dekripsi Teks Menggunakan Metode Vigenere Cipher dan Cipher Block Chaining, STMIK AKAKOM, Yogyakarta*

I.Y.B Aditya Eka Prabawa W, 2007, *Analisis Perbandingan dan Pengujian Algoritma Kunci Publik RSA dan Pailler,* ITB, Bandung.

Rinaldi Munir, 2006, *Kriptografi,* Penerbit Informatika, Bandung.

Rifki Sadikin, 2012, *Kriptografi untuk Keamanan Jaringan,* Penerbit Andi.

Dony Ariyus, 2006, *Kriptografi Keamanan Data dan Komunikasi, Graha Ilmu,* Yogyakarta.

Adi Nugroho, 2005, *Rational Rose untuk Pemodelan Berorientasi Objek.*

Scheier, Bruce. 1996. Applied Cryptography, second edition, John Wiley & Son : New York.

Stalling W. “Network and Internetwork Security”. Englewood Cliffs, New Jersey : Prentice Hall, 1995.

 ISSN 2088 - 3676