JASIEK, Vol.1, No.2, Desember 2019, pp. 143~148
ISSN: 2685-497X
DOI: 10.12928/JASIEK.v13i2.xxxx

PERBANDINGAN KRIPTOGRAFI MENGGUNAKAN ALGORITMA *DATA ENCRYPTION STANDART* (DES) DAN ALGORITMA *RIVEST SHAMIR ADLEMAN* (RSA) UNTUK KEAMANAN DATA

Achmad Hidayat, Arif Faizin
Teknik Informatika, Universitas Yudharta Pasuruan.
Sengonagung, Purwosari, Pasuruan, Jawa Timur 67162
e-mail: hachmad08@gmail.com

Abstrak

Sekarang ini pertukaran informasi sudah semakin berkembang pesat, teknologi informasi juga telah terbukti mendorong kinerja pada berbagai bidang salah satunya di bidang keamanan, Bidang keamanan sendiri digunakan untuk mengamankan suatu data. Berbagai cara dilakukan untuk mengamankan data atau pesan tersebut. Salah satu cara untuk mengamankan data atau informasi tersebut dengan Kriptografi. Dalam kriptografi ada beberapa Algoritma yang digunakan dalam pengamanan data atau informasi pun beragam jenisnya, seperti , DES ,RSA.Penelitian ini bertujuan untuk membandingkan kinerja beberapa algoritma kriptografi dalam proses enkripsi dan deskripsi data berdasarkan segi proses perhitungannya yang akan di enkripsi. Hasil dari penelitian menunjukkan adanya perbedaan proses perhitungan dari hasil enkripsi dan deskripsi data dari masing-masing algoritma. untuk Kecepatan enkripsi dan deskripsi data dengan menggunakan algoritma RSA lebih cepat di bandingkan dengan algoritma DES.Untuk masalah keamanannya DES lebih baik di bandingkan karena proses perhitungannya rumit dan sulit. DES keamanannya mengandalkan perhitungan biner sedangkan RSA keamanannya mengandalkan perhitungan pemfaktoran.

***Kata kunci** : Algoritma, Enkripsi , Deskripsi , DES dan RSA.*

1. Pendahuluan

Sekarang ini pertukaran informasi sudah semakin berkembang pesat, teknologi informasi juga telah terbukti mendorong kinerja pada berbagai bidang contoh nya di bidang keamanan, Bidang keamanan sendiri digunakan untuk mengamankan suatu data. Data merupakan bentuk jamak dari *datum* yang berarti fakta atau bagian dari peristiwa yang memiliki arti yang dihubungkan dengan, simbol, gambar, angka, huruf, yang menunjukkan berbagai ide, objek dan lain-lain.

Data memiliki berbagai kategori, ada yang sifatnya rahasia maupun tidak rahasia, data yang bersifat rahasia memiliki informasi yang didalamnya sangat dibutuhkan oleh pemilik, sehingga data tersebut perlu diamankan agar tidak disalah gunakan oleh orang yang tidak bertanggung jawab.

Berbagai cara dilakukan untuk mengamankan data atau pesan tersebut. Salah satu acara untuk mengamankan data atau informasi tersebut dengan Kriptologi. Kriptografi merupakan ilmu yang memahami tentang pengamanan (kerahasian) tulisan. Karena itu, untuk mengamankan data atau informasi dibutuh suatu cara yang mampu mengatasi masalah keamanan data. Kriptografi sendiri terdiri dari 2 bagian, yaitu kriptografi modern dan kriptografi klasik. Secara teknik algoritma kriptografi di bagi menjadi dua teknik yakni teknik substitusi dan teknik transposisi.

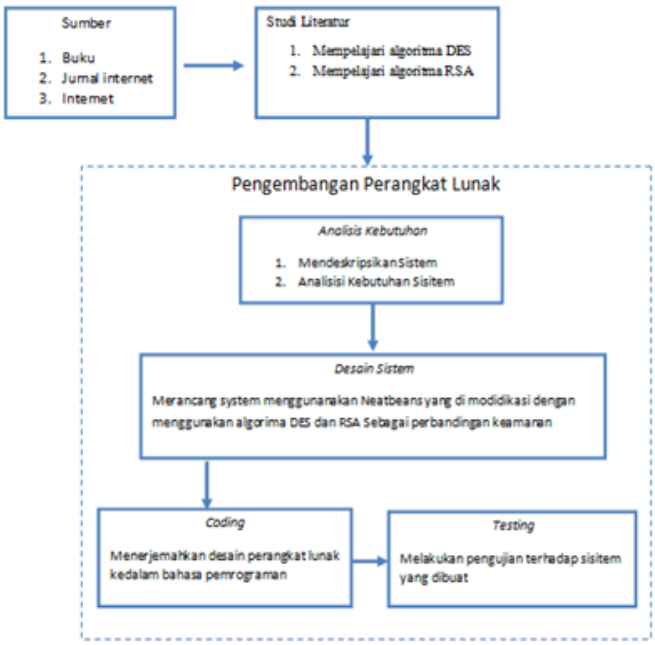
Teknik kriptografi dipercaya dapat menangani masalah keamanan data atau informasi, karena selain menggunakan bahasa pemrograman komputer, kriptografi juga menggunakan rumus-rumus matematika, mulai dari rumus yang sederhana sampai dengan rumus yang kompleks. Dalam kriptografi terdapat dua konsep, yaitu dekripsi dan enkripsi. Enkripsi merupakan proses dimana data atau informasi dirubah menjadi bentuk yang tidak dikenali atau samar sebagai informasi awalnya dengan menggunakan metode tertentu. Sedangkan dekripsi adalah mengubah kembali bentuk yang tidak dikenali menjadi data awal.

Algoritma yang digunakan dalam pengamanan data atau informasi pun beragam jenisnya, seperti *Caesar,* Abjad Majemuk, *DES, IDEA, RSA* dan lain sebagainya. Pada penelitian ini akan dilakukan perbandingan kriptografi dengan metode *RSA* dan *DES* untuk keamanan data.

Berdasarkan uraian permasalahan di atas maka penulis menggunakan bahasa pemrograman java sebagai bahasa pemrograman yang digunakan, untuk itu penulis mengusulkan perbandingan kriptografi menggunakan algoritma *data encryption standart (DES)* dan algoritma *rivest shamir adleman (RSA)* untuk keamanan data.

2. Metode Penelitian

A. Tahapan Penelitian



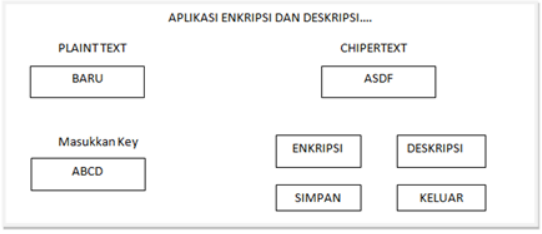
Gambar 1. Tahapan penelitian

Adapun penjelasan dari gambar tahapan penelitian diatas adalah sebagai berikut:

1. Sumber data pada penelitian ini adalah menggunakan *Library Research* yang merupakan cara mengumpulkan data dari beberapa buku, jurnal, skripsi tesis maupun literatur lainnya yang bisa dijadikan acuan pembahasan dalam masalah ini. Penelitian ini terkait pada sumber-sumber di internet ataupun hasil dari penelitian sebelumnya sebagai bahan referensi bagi peneliti selanjutnya.
2. Studi Literatur yaitu dilakukannya pengumpulan referensi informasi dari buku-buku, artikel, jurnal, situs internet yang terkait dengan topik sebagai dasar penentuan konsep penelitian yang akan dilakukan. Referensi yang akan diperlukan yaitu berupa datasheet maupun prinsip kerja dari beberapa komponen yang akan digunakan. Dari referensi yang didapat ini akan dilakukan untuk penyusunan sebuah landasan teori dari penelitian ini.
3. Pengembangan Perangkat Lunak yaitu tahap pengembangan *system* dilakukan berdasarkan metode sekuensial *linear* yang terdiri dari tahapan *analysis, design, code, testing.*

B. Perancangan Sistem

Perencanaan suatu sistem yang akan dibuat merupakan suatu tahapan proses awal merupakan tahapan yang sangat penting dalam membuat suatu program ataupun untuk melanjutkan ke langkah berikutnya, karena dengan perencanaan tersebut diharapkan mendapatkan hasil yang baik dan maksimal.



Gambar 2. Perancangan Program

3. Hasil dan Analisis

Dalam bab ini membahas mengenai implementasi dan pengujian sistem. Implementasi dan pengujian ini dilakukan untuk mengetahui apakah sistem yang telah dibuat sesuai dengan rancangan sistem.

A. *Enkripsi dan Deskripsi*

Untuk proses pertama adalah proses *enkripsi message* dan *deskripsi message*, dimana pada proses *enkripsi* dan *deskripsi* ini terdapat beberapa tahapan-tahapan dalam pemrosesan *teks*. Tahap pertama dilakukan *enkripsi teks* yaitu pengacakan *teks* dengan menggunakan aplikasi di bawah ini.

```
Masukkan plaintext 8 karakter:
CONGRATS
Nilai Biner:
0100001101001111010011100100011101010010010000010101010001010011

masukkan kunci 8 karakter :
69040004
Nilai biner:
0011011000111001001100000011010000110000001100000011000000110100

------------------------------------------------------------------------
Hasil Biner :
0100001101001111010011100100011101010010010000010101010001010011
Hasil Deskripsi: CONGRATS
BUILD SUCCESSFUL (total time: 7 minutes 22 seconds)
```

Gambar 3. *Enkripsi* dan *Deskripsi* DES

User memasukkan kata dalam *form input plain text* itu sebagai kata yang ada di *enkripsi* dan *deskripsi*.

1. *User* memasukkan *key* sesuai dengan keinginan *user* dengan *string* 8 *char*.
2. Hasil dari *enkripsi* sehingga menjadi kata yang acak.
3. Hasil dari kata yang acak akan kembali menjadi kata awal.

Gambar 4. *Enkripsi* RSA

Dalam form *enkripsi* di atas terdapat beberapa tombol dengan fungsi tombol-tombol antara lain.
User memasukkan kata dalam kolom input *plaintext* itu sebagai kata yang akan di *enkripsi*.

1. *User* memasukkan *key* berupa angka di P & Q.
2. Kita klik tombol *enkripsi*.
3. Hasil dari *enkripsi* sehingga menjadi kata yang acak.

Gambar 5. *Deskripsi* RSA

Dalam form deskripsi di atas terdapat beberapa tombol dengan fungsi tombol-tombol lain :

1. *User* memasukkan *teks key* setelah di *enkripsi* yang disebut dengan *chipertext*.
2. *User* memasukkan *teks* setelah di *enkripsi* yang disebut dengan *chipertext*.
3. Kita klik tombol deskripsi.
4. Maka akan muncul teks awal yang telah di isikan oleh *user*.

B. Perbandingan *DES dan RSA.*

Tabel 1. Perbandingan

NO	DES Kelebihan dan Kekurangan	RSA Kelebihan dan Kekurangan
1	Key dari DES bisa berupa angka dan huruf	Key dari RSA hanya berupa angka
2	Proses perhitungan manual terlalu lama dan rumit	Proses perhitungan manual agak lama
3	Keamanan lebih bagus	Keamanannya bagus
4	Kecepatan proses enkripsi jelas baik	Kecepatan proses enkripsi jelas jauh lebih baik
5	Proses deskripsi membutuhkan sangat lama	Proses deskripsi membutuhkan waktu sedikit lebih lama
6	Keamanannya mengandalkan kekuatan sulitnya pembineran	Keamanannya mengandalkan kekuatan sulitnya pemfaktoran

Berdasarkan penelitian diatas dapat di simpulkan bahwa:

a. Kecepatan *enkripsi* dan *dekripsi* data dengan menggunakan algoritma RSA lebih cepat di bandingkan dengan algoritma DES.
b. Untuk masalah keamanannya DES lebih baik di bandingkan karena proses perhitungannya rumit dan sulit.
c. DES keamanannya mengandalkan perhitungan biner sedangkan RSA keamanannya mengandalkan perhitungan pemfaktoran.

C. Pengujian Data

Pada penelitian Perbandingan kriptografi menggunakan algoritma DES dan RSA untuk keamanan data peneliti ingin mengetahui kesetujuan dari beberapa sampel yang diambil secara random mengenai program yang akan digunakan untuk membandingkan algoritma tersebut. Peneliti menggunakan kelebihan dan kekurangan sebagai alat untuk pengumpulan data. Mengolah data tersebut dengan beberapa metode. Serta diperoleh hasil sebagai berikut:

Uji Student T Test

Pada metode uji T Test, variable diperoleh dari jumlah seluruh responden tabel perbandingan. Dan diperoleh seperti pada tabel berikut:

Tabel 2. Data *T-Test*

Nomor	DES	RSA
1	10	5
2	5	10
3	10	5
4	5	10
5	5	10
6	5	10

Pada tabel diatas diperoleh hasil yang akan diuji dengan menggunakan metode uji *Student T Test*. Uji *T-Test* ini dilakukan dengan aplikasi *Ms. Excel* dengan menggunakan *Paired Two Sampel for Means*. Yang bertujuan untuk menguji perbedaan rata-rata dua *variable* dari *sample* yang sama. Dan diperoleh pada seperti pada tabel berikut:

Tabel 3. Hasil Uji *T-Test*

t-Test: Paired Two Sample for Means

	Variable 1	*Variable 2*
Mean	6,666667	8,333333
Variance	6,666667	6,666667
Observations	6	6
Pearson Correlation	-1	
Hypothesized Mean Difference	0	
Df	5	
t Stat (nilai T hitung)	-0,79057	
P(T<=t) one-tail	0,232511	
t Critical one-tail (nilai T tabel)	2,015048	
P(T<=t) two-tail	0,465023	
t Critical two-tail	2,570582	

Berdasarkan pada tabel di atas *Mean* yaitu rata-rata hasil kedua *variable*, dimana terdapat perbedaan rata-rata antara *variable* 1 dan *variable* 2. *Variable* 1 merupakan hasil DES sedangkan *variable* 2 merupakan RSA. Dapat dilihat bahwa *variable* 2 memiliki nilai rata-rata lebih banyak. Kepustusan hipotesis yang diperoleh berdasarkan tabel di atas yakni nilai T hitung adalah -0,79057 dan nilai T tabel adalah 2,015048. dapat diperoleh keputusan sebagai berikut: Jika T hitung > T tabel maka ada perbedaan antara kedua rata-rata dari kedua variabel.

4. Kesimpulan

Berdasarkan penelitian diatas dapat di simpulkan bahwa;

a. Kecepatan *enkripsi* dan *dekripsi* data dengan menggunakan algoritma RSA lebih cepat di bandingkan dengan algoritma DES.
b. Untuk masalah keamanannya DES lebih baik di bandingkan karena proses perhitungannya rumit dan sulit.
c. DES keamanannya mengandalkan perhitungan biner sedangkan RSA keamanannya mengandalkan perhitungan pemfaktoran.

5. Saran

a. Perbandingan di penelitian ini hanya dapat mengenkripsi dan mendekripsi data yang berupa *teks* atau tulisan, bukan suara maupun gambar, untuk penelitian selanjutnya dapat di kembangkan lebih lanjut untuk enkripsi dan deskripsi berupa suara maupun gambar.
b. Untuk pengembangan penelitian selanjutnya bisa di kembangkan melalui android atau desktop.

References

1. Bangun, E. A., & Setiawan, G. N. (2016). PERBANDINGAN METODE MODIFIKASI 3DES. *Departemen Teknik Informatika* , 4.
2. Gunawan, I. (2018). KOMBINASI ALGORITMA CAESAR CIPHER DAN ALGORITMA RSA UNTUK. 6.
3. Hidayat, A., & Setiana, D. (2018). PERBANDINGAN WAKTU DAN KECEPATAN PROSES ENKRIPSI DAN DEKRIPSI. *Jurnal Siliwangi* , 7.
4. Kurniawan, S. T., Dedih, & Supriyadi. (2017). Implementasi Kriptografi Algoritma Rivest. 8.
5. Meko, D. A. (2018). Perbandingan Algoritma DES, AES, IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data. *Jurnal Teknologi Terpadu* , 8.
6. Prasetiyo, B., Gernowo, R., & Noranita, B. (2014). Kombinasi Steganografi Berbasis Bit Matching dan. 16.
7. Santoso, B. W., & AlHadi, F. R. (2017). PERBANDINGAN HASIL IMPELEMENTASI. *Jurnal ICT Learning* , 17.
8. Sumarno, Gunawan, I., Tambunan, H. S., & Irawan, E. (2018). ANALISIS KINERJA KOMBINASI ALGORITMA MESSAGE-DIGEST. *JUSIKOM PRIMA* , 8.
9. Udayana, I. P., & Sastra, N. P. (2015). Perbandingan Performansi Pengamanan File Backup LPSE. *Teknologi Elektro* , 7.
10. Udayana, I. P., & Sastra, N. P. (2016). Perbandingan Performansi Pengamanan File Backup LPSE. *Teknologi Elektro* , 7.