ANALISA KOMPUTASI ALGORITMA DES DENGAN RC4 UNTUK KEAMANAN DATA

Busran[1)], Jeri Widodo Putra[2)]
Prodi Teknik Informatika S1
Fakultas Teknik
Institut Teknologi Padang
busran.nofit@gmail.com, jeriwidodo@gmail.com

Abstract

Data security and confidentiality is one of the most important aspects in the field of communication, especially communication using computer media. One of the fields of science that is used to secure data is cryptography, the speed of the cryptographic process in its implementation is often an important thing to pay attention to. This study aims to determine the speed of time required to encrypt and decrypt data between two algorithms, namely the RC4 algorithm and the DES algorithm. From research conducted using data in pdf, jpg, mp3 format where the data size from the smallest is 1000kb to the largest data size of 20mb which is each tested five times and the resulting data is the smallest size of the RC4 algorithm resulting in a time of 0 , 23288 / s and the largest data yield 0.2529 / s time and using the DES algorithm the smallest time is 0.23508 / s and the largest time is 0.2545 / s, from these tests it can be concluded that the RC4 algorithm is faster than the algorithm. DES in computing data.

Keywords- *Put 4-6 of your keywords here, keywords separated by commas*

Intisari

Keamanan dan kerahasiaan data merupakan salah satu aspek terpenting dalam bidang komunikasi khususnya komunikasi yang menggunakan media komputer. Salah satu bidang ilmu pengetahuan yang digunakan untuk mengamankan data adalah kriptografi, kecepatan proses kriptografi dalam implementasinya sering menjadi hal yang penting diperhatikan. Penelitian bertujuan untuk mengetahui kecepatan waktu yang diperlukan dalam melakukan proses enkripsi dan dekripsi data antara dua algoritma yaitu algoritma RC4 dengan algoritma DES. Dari penelitian yang dilakukan menggunakan data berformat pdf, jpg, mp3 dimana ukuran data dari yang terkecil yaitu 1000kb sampai ukuran data yang terbesar 20mb yang dimasing - masing dilakukan pengujian sebanyak lima kali pengujian dan dihasilkan dari data yang ukuran terkecil dari algoritma RC4 dihasilkan waktu selama 0,23288/s dan data yang terbesar menghasilkan waktu 0,2529/s dan mengunakan algoritma DES dihasilkan waktu terkecil 0,23508/s dan waktu terbesar 0,2545/s, dari pengujian tersebut dapat diambil kesimpulan bahwa algoritma RC4 lebih cepat dari pada algoritma DES dalam melakukan komputasi data.

Kata Kunci*—Keamanan Data, Kriptografi, Algoritma RC4, Algoritma DES.*

1. PENDAHULUAN

Keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatu data, pesan dan informasi [1]. Pengiriman suatu pesan dan data yang sangan penting membutuhkan tingkat keamanan yang tinggi. Dengan perkembangan teknologi informasi sekarang ini yang begitu pesat, dimana setiap orang sangat mudah mendapatkan suatu pesan, data dan informasi. Dengan berbagai cara setiap orang berusahan untuk mendapatkan informasi dan data tersebut dengan cara apapun dan berbagai cara pula seseorang melakukan cara apapun untuk melindungi data tersebut.

Ilmu yang mempelajari tentang proses pengaman data adalah kriptografi. Secara umum ada dua jenis kriptografi yaitu kriptografi klasik dan kriptografi modern. Kriptografi klasik adalah suatu algoritma yang menggunakan satu kunci untuk mengamankan data. Dua teknik yang biasa digunakan adalah substitusi dan transposisi. Sedangkan kriptografi modern adalah algoritma yang lebih kompleks dari pada algoritma kriptografi klasik. Banyak algoritma yang digunakan oleh seseorang untuk mengamankan data, diantaranya algoritma RC4[2] merupakan jenis stream chipher, artinya operasi enkripsi

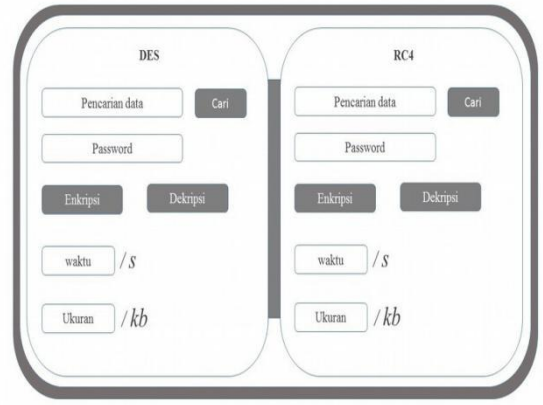
DOI : https://doi.org/10.21063/jtif.2021.V9.1.20-23

dilakukan per karakter 1 byte untuk sekali operasi dan algoritma DES[3] merupakan algoritma enkripsi yang paling banyak dipakai didunia. Secara umum standar enkripsi data terbagi tiga kelompok yaitu proses kunci, enkripsi 64bit dan dekripsi data 64 bit.

Privasi mengandung arti bahwa data yang diinginkan hanya dapat dimengerti informasinya oleh penerima yang sah atau berhak. Sedangkan keotentikan mencegah pihak ketiga untuk mengirimkan data yang salah atau mengubah data yang dikirimkan . Tujuan sistem kriptografi menurut M. Yuliandri (2009) [4] antara lain Convidentiality yaitu memberikan kerahasiaan pesan dan menyimpan data dengan menyembunyikan informasi lewat teknik-teknik enkripsi, Integrity yaitu memberikan jaminan untuk tiap bagian bahwa pesan tidak akan mengalami perubahan dari saat data dibuat atau dikirim sampai dengan saat data tersebut dibuka, Non-repudiation yaitu memberikan cara untuk membuktikan bahwa suatu dokumen datang dari seseorang apabila ia mencoba menyangkal memiliki dokumen tersebut dan Authentication yaitu memberikan dua layanan. Pertama mengidentifikasikan keaslian suatu pesan dan memberikan jaminan keotentikannya. Kedua untuk menguji identitas seseorang apabila ia akan memasuki sebuah sistem.

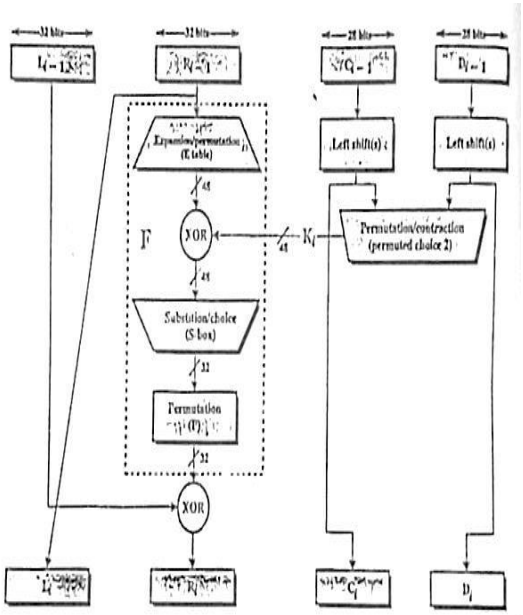
2. METODOLOGI

Penelitian ini dilakukan dengan membangun aplikasi yang digunakan sebagai mesin pembanding data yang akan dilakukan proses enkripsi dan dekripsi data, seperti gambar 1.

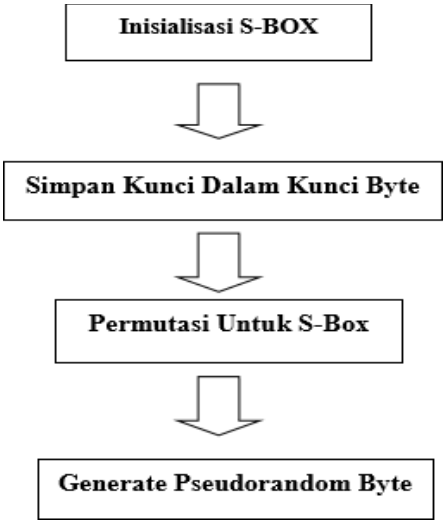


Gambar 1. Tampilan User Interface

Dengan mengimplementasikan algoritma DES dan RC4 dalam aplikasi tersebut. Algoritma DES dengan single round seperti gambar 2.



Gambar 2. Single round DES



Gambar 3. Rangkaian Proses enkripsidata (Emy Setyaningsih, 2015).

Pengujian dilakukan dengan mengukur kecepatan proses dari masing-masing algoritma dengan besaran *file* yang bervariasi pada aplikasi.

DOI : https://doi.org/10.21063/jtif.2021.V9.1.20-23

3. HASIL DAN PEMBAHASAN

3.1 Proses Enkripsi

Melalui aplikasi seperti gambar 4, diisikan data dengan variasi ukuran file yang berbeda, selanjutnya dilakukan proses enkripsi dengan memilih jenis algoritma yang ada pada pilihan chiper Algoritma.

Gambar 4. Tampilan Aplikasi Proses Enkripsi

Pada pengujian pertama dengan jenis file PDF, dimana ukuran file bervariasi pada algoritma DES dan RC4 didapatkan waktu proses seperti pada tabel 1.

Tabel 1. Hasil Pengukuran Proses Enkripsi pada jenis file PDF pada Algoritma DES dan RC4

Nama	Size (KB)	Waktu (s)	
		DES	RC4
PDF 1	*931*	*0,23508*	*0,23288*
PDF 2	*1386*	*0,2382*	*0,2372*
PDF 3	*1430*	*0,2411*	*0,2403*
PDF 4	*1602*	*0,242*	*0,2411*
PDF 5	*2269*	*0,2439*	*0,243*
PDF 6	*2460*	*0,2452*	*0,2445*
PDF 7	*2605*	*0,2469*	*0,2464*
PDF 8	*3574*	*0,2481*	*0,2475*
PDF 9	*18567*	*0,2514*	*0,2499*
PDF 10	*2021*	*0,2545*	*0,2529*

Selanjutnya pengujian dilakukan untuk jenis file gambar berjenis JPG, daiapatkan waktu proses seperti tabel 2, selisih waktu proses antara jenis file ini cukup signifikan yaitu sebesar 0,1 detik.

Tabel 2. Hasil Pengukuran Proses Enkripsi pada jenis file JPG pada Algoritma DES dan RC4

Nama	Size (kb)	Waktu (s)	
		DES	RC4
JPG 1	*1535*	*0,3442*	*0,336*
JPG 2	*2376*	*0,3449*	*0,3371*
JPG 3	*3061*	*0,3453*	*0,3373*
JPG 4	*3544*	*0,3454*	*0,3374*
JPG 5	*4943*	*0,3457*	*0,3375*
JPG 6	*5371*	*0,346*	*0,3378*
JPG 7	*6256*	*0,3463*	*0,338*
JPG 8	*8091*	*0,3468*	*0,3385*
JPG 9	*8415*	*0,3469*	*0,339*
JPG 10	*9386*	*0,3470*	*0,3396*

Untuk file jenis audio MP3 didapatkan hasil proses yg tidak terlalu signifikan dibandingkan dengan jenis file gambar terkompres jenis file JPG, seperti tabel 3.

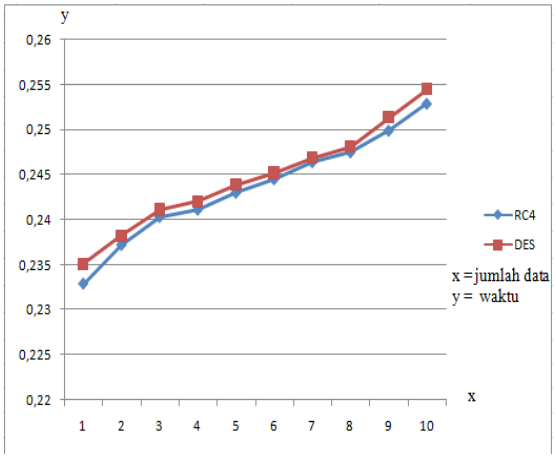
Tabel 3. Hasil Pengukuran Proses Enkripsi jenis file Audio MP3 pada Algoritma DES dan RC4

Nama	Size (kb)	Waktu (s)	
		DES	RC4
MP3 1	*2860*	*0,3595*	*0,3499*
MP3 2	*3395*	*0,3597*	*0,3501*
MP3 3	*4625*	*0,3601*	*0,3504*
MP3 4	*5568*	*0,3603*	*0,3509*
MP3 5	*6528*	*0,3604*	*0,351*
MP3 6	*7174*	*0,3606*	*0,3512*
MP3 7	*7713*	*0,3607*	*0,3515*
MP3 8	*13000*	*0,3612*	*0,3524*
MP3 9	*15390*	*0,3621*	*0,3528*
MP3 10	*17895*	*0,3631*	*0,3535*

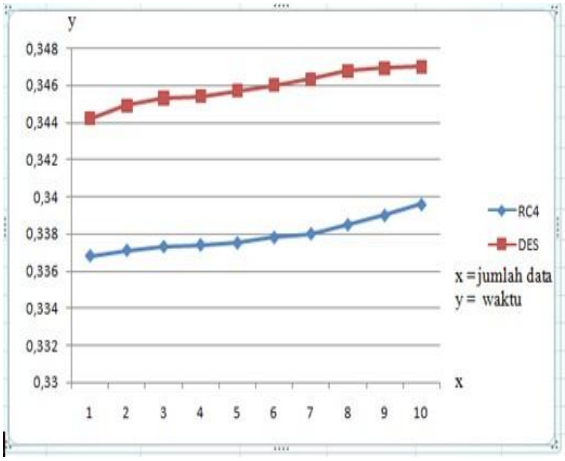
3.2 Grafik Perbandingan

Dari data yang didapatkan, untuk dapat melihat perbandingan yang relatif sederhana, maka dilakukan visualisasi data lewat grafik.

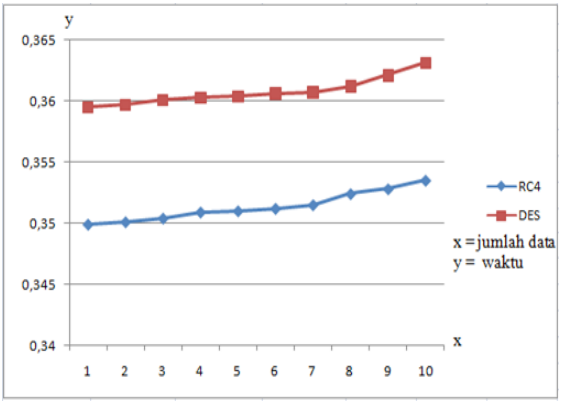
DOI : https://doi.org/10.21063/jtif.2021.V9.1.20-23



Gambar 5. Grafik perbadingan Algoritma DES dengan RC4 pada Jenis File PDF



Gambar 6. Grafik perbadingan Algoritma DES dengan RC4 pada Jenis File JPG



Gambar 6. Grafik perbadingan Algoritma DES dengan RC4 pada Jenis File MP3

4. KESIMPULAN DAN SARAN

Berdasarkan pengujian yang dilakukan untuk proses enkripsi dari algoritma DES dan RC4 dapat dijelaskan bahwa algoritma RC4 memiliki kecepatan yang lebih baik dibandingkan DES dengan selisih waktu proses enkripsi antara 0,05 sampai 0,1 detik.

DAFTAR PUSTAKA

[1] William Stallings, *Networks Security Essentials Applications anda Standards*. Prentice Hall, New Jersey, 2000, pp. 22-75.
[2] Yusuf Kurniawan, *Kriptografi Keamanan Internet dan Jaringan Komunikasi*, Informatika, Bandung, 2004, pp. 93 – 96
[3] Yusuf Kurniawan, *Kriptografi Keamanan Internet dan Jaringan Komunikasi*, Informatika, Bandung, 2004, pp. 51 – 56
[4] Yuli Andri, *Implementasi algoritma kriptografi DES,RSA dan algortima koplesi LZW pada berkas digital*,Medan, 2009

DOI : https://doi.org/10.21063/jtif.2021.V9.1.20-23