VOL. 17. NO. 2 FEBRUARI 2022
P-ISSN: 0216-6933 | E-ISSN: 2685-807X
Diterbitkan Oleh: LPPM Nusa Mandiri

INTI NUSA MANDIRI
DOI: https://doi.org/10.33480/inti.v17i2.3900

ANALISIS KECEPATAN ENKRIPSI DEKRIPSI DAN ALOKASI MEMORI MENGGUNAKAN ALGORITMA DES, 3DES DAN ELGAMAL

Hermawan Setiawan [1*]; Mutiara Intan Kamila[2] ; Yulandi[3]

Rekayasa Kriptografi [1,2,3]
Politeknik Siber dan Sandi Negara [1,2,3]
https://poltekssn.ac.id/ [1,2,3]
hermawan.setiawan@poltekssn.ac.id[1*]; mutiara.intan@student.poltekssn.ac.id[2]; yulandi@poltekssn.ac.id[3]

Abstract— *Technological developments have brought rapid progress in the field of Science and Technology (IPTEK). These advances provide access to the availability of literature and ease of accessing information through various media. However, due to the large number of misuses and vulnerabilities, information security is needed. The science of cryptography as a way of securing information in the form of encoding data. An example of its use is with cryptographic algorithms. The DES algorithm is a symmetric cryptographic algorithm that can work fast. The 3DES algorithm, which is an extension of DES, uses a key length three times the size of the DES key and three times the iteration of the DES scheme. Whereas ElGamal is an asymmetric cryptographic algorithm that has the characteristic of having two keys, namely a public key and a private key. ElGamal has a better level of security than the previous two algorithms due to the difficulty of calculating discrete logarithms. Of course, the three algorithms have different performance and advantages. Especially if a document is used as input and output. The focus of the research discusses the comparison of running time and speed of data encryption and decryption as well as memory allocation of the DES, 3DES and ElGamal algorithms on txt text data implemented in the C programming language. . Based on the test results, the ElGamal algorithm can process encryption and decryption times faster than the DES and 3DES algorithms if the input file is small with a maximum file size of 0.01KB. Meanwhile, when a larger input file is used, the ElGamal algorithm takes much longer than the DES and 3DES algorithms. In terms of pattern, the encryption speed is different from the decryption for the three algorithms. Whereas ElGamal uses far less memory than the other two algorithms.*

Keywords*: DES, 3DES, ElGamal, speed, memory*

Abstrak—Perkembangan teknologi membawa kemajuan pesat dalam bidang Ilmu Pengetahuan dan Teknologi (IPTEK). Kemajuan ini memberikan akses ke dalam ketersediaan literatur dan kemudahan dalam mengakses informasi melalui berbagai media. Namun karena banyaknya penyalahgunaan dan kerawaan maka keamanan atas informasi sangat diperlukan. Ilmu kriptografi sebagai salah satu cara mengamankan informasi dalam bentuk menyandikan data. Contoh penggunaannya ialah dengan algoritma kriptografi. Algoritma DES merupakan algoritma kriptografi simetris yang dapat bekerja dengan cepat. Algoritma 3DES yang merupakan pengembangan dari DES memakai panjang kunci tiga kali ukuran kunci DES dan tiga kali perulangan skema DES. Sedangkan ElGamal yang merupakan algoritma kriptografi asimetris yang memiliki ciri khas adanya dua kunci yakni kunci publik dan kunci privat. ElGamal memiliki tingkat keamanan yang lebih baik dari dua algoritma sebelumnya karena sulitnya menghitung logaritma diskrit. Tentunya ketiga algoritma memiliki performansi dan keunggulan yang berbeda. Terutama jika digunakan sebuah dokumen sebagai input dan output. Fokus penelitian membahas perbandingan running time dan kecepatan enkripsi dekripsi data serta alokasi memori algoritma DES, 3DES dan ElGamal pada data teks txt yang diimplementasikan dalam bahasa pemograman C. Berdasarkan hasil pengujian bahwa algoritma ElGamal dapat memproses waktu enkripsi dan dekripsi lebih cepat dibanding algoritma DES dan 3DES jika file input berukuran kecil dengan maksimal ukuran file 0.01KB. Sedangkan ketika digunakan file input yang berukuran lebih besar maka algoritma ElGamal memakan waktu yang jauh lebih lama dibandingkan algoritma DES dan 3DES. Dari sisi pola kecepatan enkripsi berbeda dengan dekripsi untuk ketiga algoritma. Sedangkan ElGamal menggunakan memori yang jauh lebih sedikit dari kedua algoritma yang lain.

Kata kunci: *DES, 3DES, ElGamal, kecepatan, memori*

VOL. 17. NO. 2 FEBRUARI 2023
P-ISSN: 0216-6933 | E-ISSN: 2685-807X
Diterbitkan Oleh: LPPM Nusa Mandiri

PENDAHULUAN

Pada era modern, kecanggihan teknologi dan inovasi sangat membantu manusia dalam berbagai bidang. Salah satunya bidang Ilmu Pengetahuan dan Teknologi (IPTEK). Ketersediaan literatur dan kemudahan mengakses membuat informasi dan data dapat ditemukan dengan mudah melalui berbagai media. Hal ini merupakan poin penting yang membantu perkembangan pola pikir masyarakat dan penelitian berkelanjutan. Namun, tidak semua informasi berhak diketahui oleh orang lain. Oleh karena itu diperlukan suatu cara untuk mengamankan data dan informasi.

Dampak postif perkembangan teknologi bagi masyarakat juga mengakibatkan dampak negatif salah satunya adalah adanya pencurian data yang ada di komputer anda atau adanya penipuan–penipuan yang berbasis computer. Harus ada peningkatan keamanan komputer agar data yang ada dikomputer kita tidak dapat dicuri atau dirusak(Thahara & Siregar, 2021). keamanan atas informasi dan data diperlukan sebagai bentuk kerahasiaan, menjaga integritas data dan otentikasi. Oleh karena itu diperlukan ilmu kriptografi yang dapat menyandikan data. Salah satu contoh penggunaannya ialah dengan algoritma kriptografi.

Ilmu kriptografi memiliki peranan utama untuk mengubah data tersebut ke dalam bentuk data yang lain dengan cara penyandian. Terdapat dua jenis algoritma kriptografi dilihat dari kunci yang digunakan untuk enkripsi dan dekripsi yakni, algoritma simetris dan algoritma asimetris(Panhwar et al., 2019).

Waktu komputasi teknik kriptografi diklasifikasikan sebagai waktu enkripsi/dekripsi, pembuatan kunci, dan waktu pertukaran kunci. Waktu enkripsi/dekripsi dihitung dengan mengubah teks biasa (pesan) menjadi ciphertext dan sebaliknya. Ada banyak algoritma kriptografi yang digunakan untuk mengamankan informasi seperti DES, 3DES, Blowfish, AES, RSA, dan ElGamal. Diperlukan cara untuk menemukan algoritma keamanan terbaik yang memberikan keamanan tinggi dan juga membutuhkan waktu lebih sedikit untuk pembuatan kunci, enkripsi, dan dekripsi informasi (Maqsood et al., 2017).

Algoritma simetris dan asimetris memiliki performansi yang berbeda baik dalam kecepatan dan alokasi memori. Terutama jika digunakan sebuah dokumen sebagai input dan output. Oleh karena itu pada penelitian ini akan dibandingkan kedua jenis algoritma terhadap kecepatan dan alokasi memori pada data teks .txt (Hidayat & Setiana, 2018). Algoritma yang akan dibandingkan ialah DES, 3DES dan ElGamal.

DES merupakan algoritma yang dikembangkan oleh IBM pada tahun 1972 ini merupakan algoritma kriptografi simetris golongan block cipher yang paling umum digunakan saat ini. DES beroperasi pada ukuran blok 64 bit. DES mengenkripsi 64 bit plaintext menjadi 64 bit ciphertext dengan menggunakan 56 bit kunci internal (internal key). Kunci internal pada algoritma DES dibangkitkan dari kunci eksternal (external key) yang panjangnya 64 bit (Kaur & Sodhi, 2016) .

3DES (Triple Data Encryption Standard) merupakan salah satu algoritma simetris pengembangan dari algoritma DES (Data Encryption Standard) yang digunakan untuk mengamankan data dengan cara menyandikan data. Perbedaan DES dengan 3DES terletak pada panjangnya kunci yang digunakan.

Pada DES menggunakan satu kunci yang panjangnya 56 bit, sedangkan pada 3DES menggunakan 3 kunci yang panjangnya 168 bit atau terdapat 3 kunci dengan masing-masing panjangnya 56 bit(Guru et al., 2020). Pada 3DES, 3 kunci yang digunakan bisa bersifat saling bebas (K1 ≠ K2 ≠ K3) atau hanya dua buah kunci yang saling bebas dan satu kunci lainnya sama dengan kunci pertama (K1 ≠ K2 dan K3 = K1). Karena tingkat kerahasiaan algoritma 3DES terletak pada panjangnya kunci yang digunakan, maka penggunaan algoritma 3DES dianggap lebih aman dibandingkan dengan algoritma DES (Sivakumar et al., 2018) .

Skema yang dilakukan pada 3DES menggunakan tiga kunci. Plaintext yang diinputkan dioperasikan dengan kunci eksternal pertama (K1) dan melakukan proses enkripsi dengan menggunakan algoritma DES. Selanjutnya menghasilkan pra-teks sandi pertama. Lalu, pra-teks sandi pertama yang dihasilkan pada tahap pertama dioperasikan dengan kunci eksternal kedua (K2). Tahap berikutnya melakukan proses enkripsi atau proses dekripsi (tergantung cara pengenkripsian yang digunakan) dengan menggunakan algoritma DES, sehingga menghasilkan pra-teks sandi kedua. Tahap terakhir, pra-teks sandi kedua yang dihasilkan pada tahap kedua, dioperasikan dengan kunci eksternal ketiga (K3) dan melakukan proses enkripsi dengan menggunakan algoritma DES, sehingga menghasilkan teks sandi

Algoritma ElGamal merupakan algoritma kunci publik yang ditemukan oleh Taher Elgamal pada tahun 1985. Algoritma ElGamal terdiri dari 3 proses utama, yaitu pembentukan kunci, proses enkripsi, dan proses dekripsi (Asri et al., 2019). Sebelum melakukan proses enkripsi, plaintext akan dibagi menjadi blok-blok kecil. Keamanan algoritma

VOL. 17. NO. 2 FEBRUARI 2022
P-ISSN: 0216-6933 | E-ISSN: 2685-807X
Diterbitkan Oleh: LPPM Nusa Mandiri

INTI NUSA MANDIRI
DOI: https://doi.org/10.33480/inti.v17i2.3900

ini terletak pada sulitnya menghitung logaritma diskrit.

Penelitian bertujuan untuk membandingan kecepatan algoritma DES, 3DES, dan ElGamal pada data teks .txt. Selain kecepatan dibandingkan juga alokasi memori ciphertext pada algoritma DES, 3DES, dan ElGamal pada data teks .txt.
Adapun pada penelitian ini, hasil yang didapat ditemukan kesamaan pada algoritma antara DES dengan 3DES yang ditunjukkan dalam (Ratnadewi et al., 2018) dengan Bahasa pemrograman C++, (Hidayat & Setiana, 2018) yang menggunakan aplikasi Matlab, (Latif, 2020) dengan aplikasi Labview, (Iftikhar et al., 2021; Patil et al., 2016; Srinivasa Rao, 2015) dengan bahasa pemrograman Java; Thirupalu et al., 2019; dengan aplikasi Crypto++, (Tankasali & Shirahatti, 2020) dengan aplikasi simulasi Xillinx 14.7 dan ISIM simulator serta hasil simulasi

BAHAN DAN METODE

Metode Penelitian

Waktu komputasi kriptografi asimetris lebih besar daripada kriptografi simetris yang membuat enkripsi/dekripsi lebih kompleks untuk sejumlah besar data. Karena ukuran kunci yang lebih besar dan waktu komputasi kriptografi asimetris yang lebih besar, kriptografi kunci publik digunakan sekali untuk pertukaran kunci saja dan enkripsi/ dekripsi lebih lanjut dilakukan oleh kriptografi kunci simetris algoritma DES, 3DES, dan ElGamal(Maqsood et al., 2017). Metode lain yang digunakan adalah metode pengembangan perangkat lunak, yaitu melakukan software design yang dibangun dengan bahasa pemograman C dan kemudian dilakukan implementation and unit testing untuk membentuk program dan memastikannya dapat berjalan dengan sesuai perencanaan.

Alat penunjang berupa perangkat keras (hardware) dan (software). Adapun spesifikasi hardware yang digunakan pada penelitian ini ialah:

a. Operating system : Windows 10 Pro 64-bit (10.0, Build 18363)
b. BIOS : InsydeH2O Version 05.11.25F.21
c. Processor : AMD E2-7110 APU with AMD Radeon R2 Graphics
d. Memory : 4096MB RAM

Sedangkan software yang digunakan meliputi sebagai berikut :

a. DEV C++ Version 5.11
b. Sublime Text Versi 3.2.2 Build 3211
c. Notepad Version 1909.

Bahan sampling

Bahan sampling yang dibutuhkan untuk uji coba ialah kunci dan plaintext. Kunci pada algoritma DES digunakan sepanjang 64 bit dan algoritma 3DES sepanjang 192 bit. File kunci disimpan dalam key.txt. Sedangkan untuk parameter kunci algoritma ElGamal dimasukkan langsung dalam algoritma. File plaintext DES dan 3DES berisikan sebuah teks panjang dengan ukuran 0.008KB, 0.01KB, 0.5KB, 2KB, dan 4KB. Ukuran yang sama berlaku pada plaintext ElGamal hanya saja dalam bentuk binary. Berikut Gambar 1 kunci yang digunakan pada uji coba pada ketiga algoritma tersebut.

DES	3DES	ElGamal
0001001100 110100	0001001100110100010101110111 1001100110111011110011	P = 107 g = 2 k = 67
0101011101 111001	01111111110001000000010010001 101000101011001111000	
1001101110 111100	10011010101111001101111011110 0010011001101000010101	
1101111111 110001	11011110011001101110111100110 1111111110001	

Gambar 1. Kunci untuk Uji Coba

Contoh dari plaintext yang digunakan akan ditampilkan pada Gambar 2 di bawah ini. Namun plaintext akan disesuaikan dengan ukuran file yang di uji coba.

<table>
<tr><th>DES</th><th>3DES</th><th>ElGamal</th></tr>
<tr><td colspan="2">Lorem ipsum dolor sit amet, consectetur adipiscing elit. Vivamus condimentum sagittis lacus, laoreet luctus ligula laoreet ut. Vestibulum ullamcorper accumsan velit vel vehicula. Proin tempor lacus arcu</td><td>1110011110101010100 101010101011100 1111010101010010101 010100001010100 1010101010010101110 011110101010100 1010101010000101010 010101010100101</td></tr>
</table>

Gambar 2. Plaintext Sampling

Parameter Kerja

Dalam penelitian ini, untuk mengevaluasi hasil kerja algoritma DES, 3DES dan ElGamal maka digunakan paramater kerja sebagai berikut (Latif, 2020) :

a. Running Time
   Waktu yang dibutuhkan oleh sebuah algoritma untuk menyelesaikan proses enkripsi maupun dekripsi. Running time dimulai dari algoritma dijalankan hingga berhenti. Running time memiliki satuan detik (s) dan pada tabel hasil penelitian dinamakan sebagai waktu proses.
b. Ukuran File
   Ukuran file ini dapat mempengaruhi kinerja program dalam menjalankan algoritma yang ada di dalamnya. File yang dijadikan file input

VOL. 17. NO. 2 FEBRUARI 2023
P-ISSN: 0216-6933 | E-ISSN: 2685-807X
Diterbitkan Oleh: LPPM Nusa Mandiri

dengan file output dapat berbeda ukuran tergantung algoritma dan besaran input.

c. Kecepatan

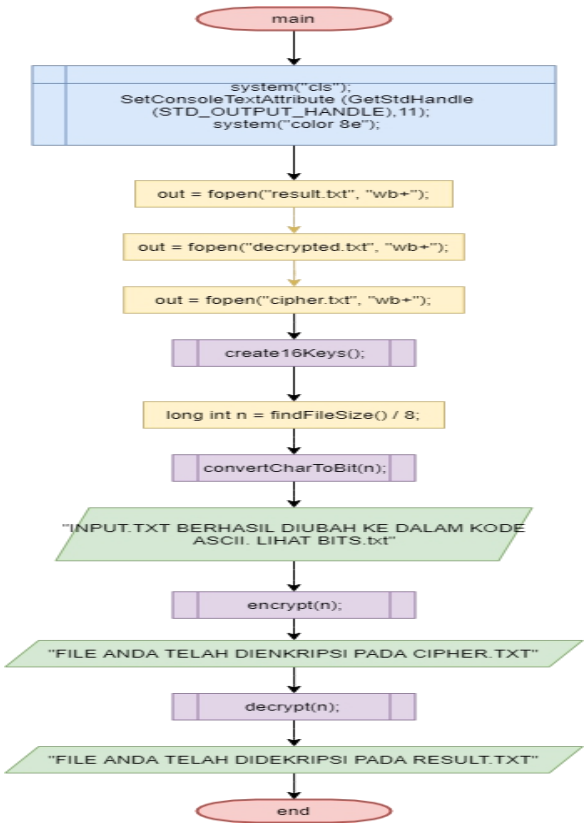
Besaran yang menunjukkan seberapa cepat suatu algoritma menyelesaikan programnya. Variabel yang digunakan untuk mengukur kecepatan ialah file input yang berasal dari data teks.txt dan running time. Sehingga untuk kecepatan memiliki satuan KB/s.

Design Program

a. Program Algoritma Data Encryption

Pada main program algoritma DES tidak terdapat pengecekan apakah plaintext ditemukan atau tidak. Karena pengecekan ini sudah dilakukan pada fungsi findFileSize. Dimana pada fungsi utama ini terdapat long int n = findFileSize() / 8. Ketika ukuran file 0 atau tidak ada, maka akan muncul pesan “failed” pada layer.

Selanjutnya akan dilakukan proses pembangkitan kunci. Pada fungsi utama, plaintext yang disimpan dalam plain.txt akan di konversi ke dalam kode ASCII dimana ini ada di dalam fungsi convertCharToBit. Setelah dikonversi, file tersebut akan tersimpan dalam bits.txt dan program akan display pesan "input.txt berhasil diubah ke dalam kode ascii. lihat bits.txt”.



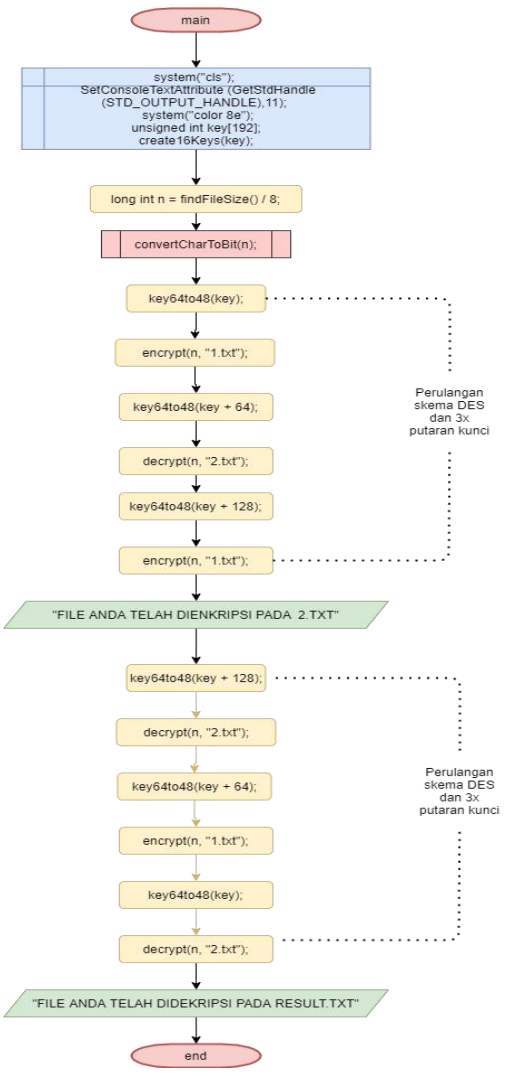
(Sumber: Peneliti, 2023)

Gambar 3. Flowchart Main Program DES

Berkaitan dengan Gambar 3 Proses selanjutnya adalah proses enkripsi dimana main akan memanggil fungsi encrypt. Setelah selesai file akan tersimpan pada cipher.txt dan terdapat pesan "file anda telah dienkripsi pada cipher.txt” yang muncul pada layar. Untuk proses dekripsi, fungsi decrypt akan dipanggil dan hasil dekripsi disimpan dalam result.txt. Terdapat pesan yang menandakan proses telah selesai yaitu "file anda telah didekripsi pada result.txt” sesuai gambar 1 diatas.

Pada program ini tidak memiliki input suatu data atau perintah karena itu akan mengakibatkan pengukuran waktu menjadi tidak efektif. Lamanya pemasukan data dan pengetikan perintah akan terhitung ke dalam running time. Untuk kunci yang digunakan disimpan dalam key.txt sehingga jika ingin mengganti kunci dapat dilakukan perubahan pada isi key.txt

b. Program Algoritma Triple Data Encryption



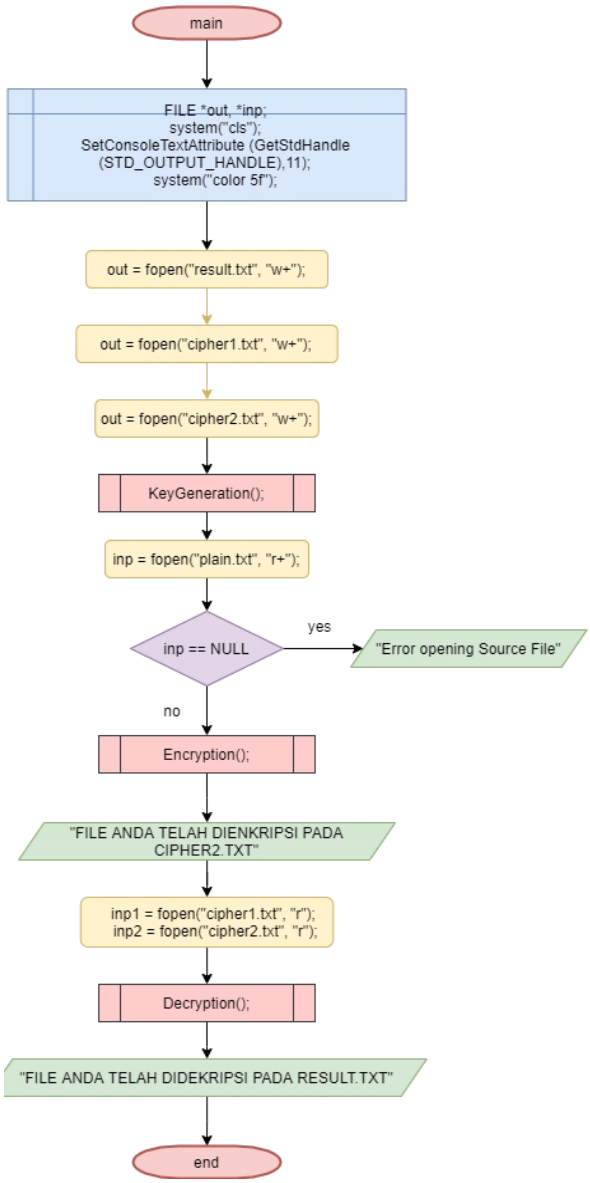
(Sumber: Peneliti, 2023)

Gambar 4. Flowchart Main Program Tripple DES

VOL. 17. NO. 2 FEBRUARI 2022
P-ISSN: 0216-6933 | E-ISSN: 2685-807X
Diterbitkan Oleh: LPPM Nusa Mandiri
INTI NUSA MANDIRI
DOI: https://doi.org/10.33480/inti.v17i2.3900

Main program algoritma 3DES tidak jauh berbeda dengan DES sesuai pada Gambar 4 diatas. Perbedaan terdapat perulangan skema DES sebanyak 3 kali. Penggunaan kunci sepanjang 192 bit akan dibagi menjadi tiga bagian masing-masing berukuran 64 bit dan dimasukkan pada 1 putaran skema DES. Pada program ini pun terdapat konversi input menjadi kode ASCII yang disimpan dalam 1.txt. Plain.txt yang berisi plaintext dapat berupa teks ataupun binary. Perubahan kunci dapat dilakukan pada key.txt. Hal ini menyebabkan program ini tidak meminta input data atau perintah dari user. Karena hal itu akan mempengaruhi pengukuran waktu yang menjadi fokus pembahasan pada penelitian ini.

c. Program Algoritma ElGamal



(Sumber: Peneliti, 2023)

Gambar 5. Flowchart Main Program ElGamal

Main program aplikasi ElGamal akan dilakukan pembangkitan kunci terlebih dahulu. Untuk parameter kunci ini sudah dimasukkan langsung ke dalam program jadi tidak membuka file kunci yang berasal dari txt. Selanjutnya akan membuka plaintext yang disimpan dalam txt dalam nama plain.txt. Terdapat pengecekan jika file tidak ada maka akan tercetak pesan “Error opening Source File” yang akan muncul pada layar program namun jika file ditemukan file akan dimasukin ke fungsi encryption dan hasil enkripsi disimpan dalam cipher2.txt. Program pun akan menampilkan pesan “"file anda telah dienkripsi pada cipher2.txt” yang menandakan file sudah terenkripsi dan disimpan.

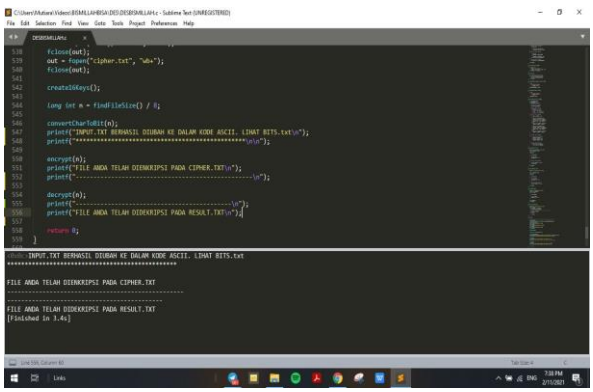
Selanjutnya file cipher1.txt dan cipher2.txt akan dibuka dengan mode “r”. Hal ini bertujuan untuk melakukan dekripsi. Setelah file dibuka maka akan dimasukkan ke dalam fungsi decryption dan akan muncul pesan "file anda telah didekripsi pada result.txt” yang menandakan dekripsi selesai dan tersimpan pada file result.txt.

Program ini tidak memiliki input suatu data atau perintah sehingga mnnakan mengakibatkan pengukuran waktu menjadi tidak efektif. Lamanya pemasukan data dan pengetikan perintah akan terhitung ke dalam running time. Oleh karena itu semua data yang diperlukan untuk enkripsi dan dekripsi sudah dimasukan ke dalam program. Jika ingin mengganti kunci maka dapat dilakukan di dalam fungsi key generation pada program. Plaintext yang disimpan dalam plain.txt pun dapat diubah sesuai kebutuhan dengan syarat harus dalam bentuk binary.

HASIL DAN PEMBAHASAN

Pengujian Program

Hasil pengujian program yang dibangun bisa berjalan sesuai perencanaan. Proses running program menggunakan aplikasi sublime text seperti ditunjukkan pada gambar 4 dibawah.



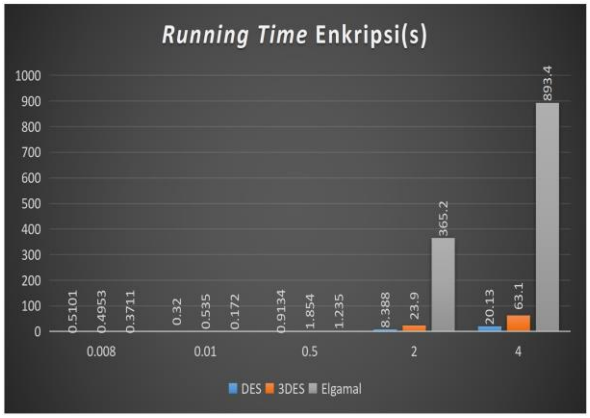
(Sumber: Peneliti, 2023)

Gambar 6. Running Program DES dengan Menggunakan Aplikasi Sublime Text

VOL. 17. NO. 2 FEBRUARI 2023
P-ISSN: 0216-6933 | E-ISSN: 2685-807X
Diterbitkan Oleh: LPPM Nusa Mandiri

Hasil Running Time

a. Running Time Proses Enkripsi

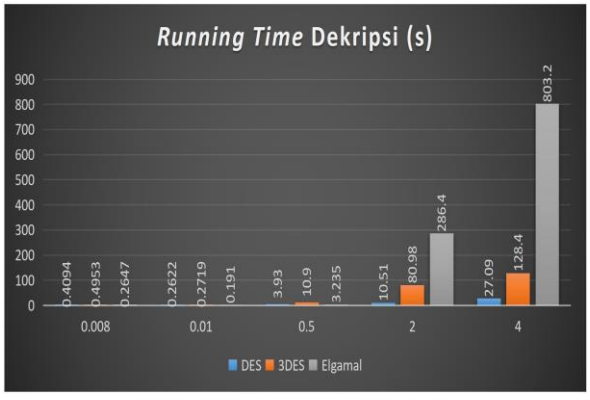


(Sumber: Peneliti, 2023)

Gambar 7. Hasil Running Time Proses Enkripsi

Gambar 7 menunjukkan perbandingan *running time* (waktu proses) saat melakukan proses enkripsi pada algoritma DES, 3DES, dan ElGamal. Terlihat ketika file input.txt yang digunakan berukuran kecil, algoritma Elgamal menjadi algoritma tercepat. Namun ketika file input semakin besar maka terjadi peningkatan yang cukup drastis. Jika ketiga algoritma ini dibandingkan maka algoritma DES merupakan algoritma tercepat dengan rata-rata running time sebesar 6.05 detik. Hasil yang sama perbandingan DES dengan 3DES ditunjukkan dalam (Ratnadewi et al., 2018) dengan Bahasa pemrograman C++, (Hidayat & Setiana, 2018) yang menggunakan aplikasi Matlab, (Latif, 2020) dengan aplikasi Labview, (Iftikhar et al., 2021; Patil et al., 2016; Srinivasa Rao, 2015) dengan bahasa pemrograman Java, dengan aplikasi Crypto++, (Tankasali & Shirahatti, 2020) dengan aplikasi simulasi Xillinx 14.7 dan ISIM simulator, dan hasil simulasi.

b. Running Time Proses Deskripsi



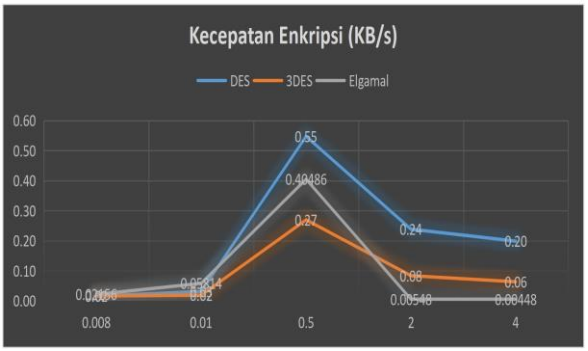
(Sumber: Peneliti, 2023)

Gambar 8. Hasil Running Time Proses Deskripsi

Gambar 8 menunjukkan perbandingan running time saat melakukan proses dekripsi. Sama seperti perbandingan running time untuk enkripsi, pada dekripsi pun algoritma ElGamal memiliki perbandingan yang sangat jauh. Rata-rata waktu yang diperlukan oleh algoritma ElGamal sebesar 218.66 detik. Nilai tersebut sangatlah besar jika dibandingkan dengan rata-rata running time DES sebesar 8.44 detik dan 3DES sebesar 44.21 detik. Demikian juga dengan penelitian lain menghasilkan perbandingan yang sama.

Perbandingan Kecepatan

a. Perbandingan Kecepatan Proses Enkripsi

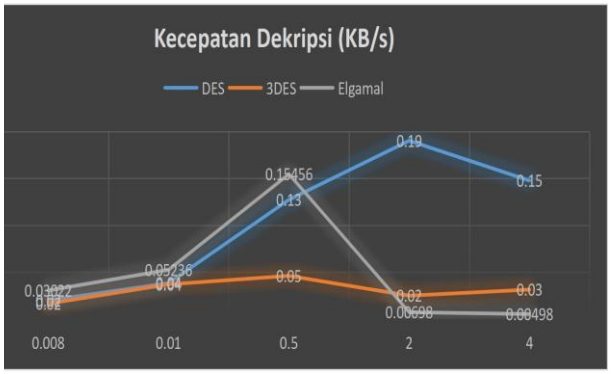


(Sumber: Peneliti, 2023)

Gambar 9. Perbandingan Kecepatan Proses Enkripsi

Pada gambar 9 menunjukkan kecepatan algoritma dalam melakukan enkripsi. Terdapat persamaan yang terjadi dimana ketiga algoritma mencapai kecepatan maksimum ketika file input sebesar 0.5KB. Namun terjadi penurunan kecepatan saat file input yang digunakan semakin besar. Hasil yang sama perbandingan DES dengan 3DES ditunjukkan dalam (Hidayat & Setiana, 2018) yang menggunakan aplikasi Matlab, (Latif, 2020) dengan aplikasi Labview dalam bentuk perhitungan Throughput(MByte/sec), dan Thirupalu et al., 2019); dengan aplikasi Crypto++.

b. Perbandingan Kecepatan Proses Deskripsi



(Sumber: Peneliti, 2023)

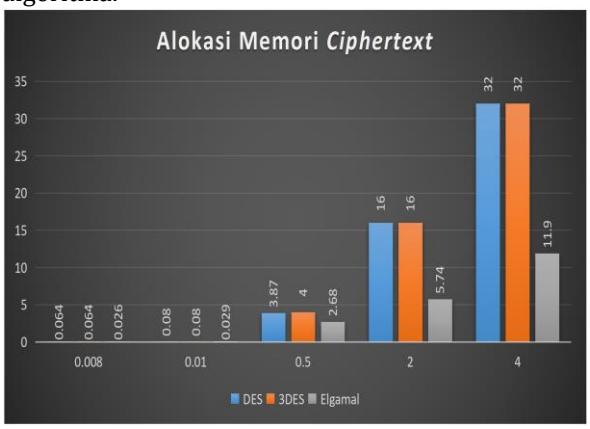
Gambar 10. Perbandingan Kecepatan Proses Deskripsi

Gambar 10 menunjukkan perbandingan kecepatan saat melakukan dekripsi. Pada proses ini

grafik dari algoritma DES berhasil menempati kecepatn maksimum saat file input.txt sebesar 2KB. Perbedaan kecepatan setiap ukuran data memiliki lonjakan yang cukup besar terutama jika dibandingkan dengan 3DES yang memiliki grafik konstan.

Perbandingan Alokasi Memori Ciphertext

Terlihat bahwa DES dan 3DES memiliki ukuran teks sandi yang sama. Sedangkan ElGamal menggunakan memori yang lebih sedikit. Hal ini dapat disebabkan oleh konversi dari input.txt menjadi kode ASCII 8 bit pada algoritma DES dan 3DES sesuai dengan gambar 11 yang menunjukkan alokasi memori dari ciphertext masing-masing algoritma.



(Sumber: Peneliti, 2023)

Gambar 11. Perbandingan Alokasi Memori Ciphertext

Ukuran(KB)	Waktu Proses(Second)			Selisih Waktu	Kecepatan (KB/Second)			Selisih Kecepatan
	DES	3DES	Elgamal		DES	3DES	Elgamal	
0.008	0.5101	0.4953	0.3711	-0.3563	0.02	0.02	0.02156	-0.02203
0.01	0.32	0.535	0.172	-0.387	0.03	0.02	0.05814	-0.04558
0.5	0.9134	1.854	1.235	-2.1756	0.55	0.27	0.40486	-0.12714
2	8.388	23.9	365.2	-380.712	0.24	0.08	0.00548	0.14928
4	20.13	63.1	893.4	-936.37	0.20	0.06	0.00448	0.13084
LAI RATA-ATA	6.05	17.98	252.08		0.21	0.09	0.10	

Gambar 12 Uji Coba Proses Enkripsi

Gambar 12 menunjukkan hasil waktu tercepat enkripsi dari ketiga algoritma yaitu algoritma DES memiliki rata-rata waktu 6.05 detik dengan kecepatan rata-rata 0.21KB/s. Namun didapat anomali pada ukuran file kecil yaitu 0,08 Kb dan 0,01 Kb yang tercepat adalah algortima ElGamal.

Ukuran(KB)	Waktu Proses(Second)			Selisih Waktu	Kecepatan (KB/Second)			Selisih Kecepatan
	DES	3DES	Elgamal		DES	3DES	Elgamal	
0.008	0.4094	0.4953	0.2647	-0.3506	0.02	0.02	0.03022	-0.02683
0.01	0.2622	0.2719	0.191	-0.2007	0.04	0.04	0.05236	-0.05100
0.5	3.93	10.9	3.235	-10.205	0.13	0.05	0.15456	-0.07320
2	10.51	80.98	286.4	-356.87	0.19	0.02	0.00698	0.15861
4	27.09	128.4	803.2	-904.51	0.15	0.03	0.00498	0.11152
LAI RATA-ATA	8.44	44.21	218.66		0.10	0.03	0.05	

Gambar 13. Uji Coba Proses Dekripsi

Gambar 13 menunjukkan hasil waktu tercepat dekripsi dari ketiga algortima yaitu algortima DES memiliki rata-rata waktu 8.44 detik dengan kecepatan rata-rata 0.1KB/s. Namun didapat anomali pada ukuran file kecil yaitu 0,08 Kb dan 0,01 Kb yang tercepat adalah algortima ElGamal.

Tabel 1. Alokasi Memori Ciphertext

Input (KB)	Output (KB)		
	DES	3DES	Elgamal
0.008	0.064	0.064	0.026
0.01	0.08	0.08	0.029
0.5	3.87	4	2.68
2	16	16	5.74
4	32	32	11.9

Alokasi memori terendah dari ketiga algortima adalah algortima ElGamal seperti ditunjukkna pada Tabel 5.

KESIMPULAN

Berdasarkan hasil pengujian dapat disimpulkan bahwa algoritma ElGamal dapat memproses waktu enkripsi dan dekripsi lebih cepat dibanding algoritma DES dan 3DES jika file input berukuran kecil dengan maksimal ukuran file 0.01KB. Sedangkan ketika digunakan file input yang berukuran lebih besar maka algoritma ElGamal memakan waktu yang jauh lebih lama dibandingkan algoritma DES dan 3DES.

Menurut rata-rata waktu yang digunakan untuk enkripsi dan dekripsi, algoritma DES merupakan algoritma tercepat. Hal ini disebabkan karena pada algoritma DES proses yang terjadi hanya pengacakan bit plaintext sehingga proses yang dijalankan tidak terlalu berat. Sedangkan pada ElGamal terdapat perulangan yang membuatnya menjadi lebih lama.

Hal lain yang dapat mempengaruhi waktu proses enkripsi dan dekripsi adalah ukuran file, spesifikasi pada perangkat keras, dan proses lain yang sedang dilakukan oleh perangkat keras.

VOL. 17. NO. 2 FEBRUARI 2023
P-ISSN: 0216-6933 | E-ISSN: 2685-807X
Diterbitkan Oleh: LPPM Nusa Mandiri

Dalam aspek alokasi memori ciphertext, memori yang digunakan oleh algoritma ElGamal untuk menyimpan ciphertext lebih sedikit dibandingkan algoritma DES dan 3DES. Ketika file input berukuran 4KB, alokasi memori ciphertext pada ElGamal hanya berukuran 11.9KB sedangkan untuk DES dan 3DES alokasi mencapai 32KB.

REFERENSI

Asri, R., Nasution, M. K. M., & Suherman, S. (2019). Modification of chipertext Elgamal algorithm using split merge. *Journal of Physics: Conference Series*, *1235*(1). https://doi.org/10.1088/1742-6596/1235/1/012054

Guru, J., Srivatsava, M., & Sheeja, M. R. (2020). Implementation of Triple DES ALGORITHM in Data Hiding and Image Encryption Techniques. *International Journal of Advanced Science and Technology*, *29*(3). https://www.researchgate.net/publication/345133617

Hidayat, A., & Setiana, D. (2018). PERBANDINGAN WAKTU DAN KECEPATAN PROSES ENKRIPSI DAN DEKRIPSI DATA TEKS.TXT MENGGUNAKAN ALGORITMA DES DAN 3DES. *Jurnal Siliwangi*, *4*(2).

Iftikhar, U., Waqas, M., Kashif Asrar, P., & Abbas Ali, S. (2021). Evaluating the Performance Parameters of Cryptographic Algorithms for IOT-based Devices. In *Technology & Applied Science Research* (Vol. 11, Issue 6). www.etasr.com

Kaur, N., & Sodhi, S. (2016). Data Encryption Standard Algorithm (DES) for Secure Data Transmission. *International Journal of Computer Applications*, 975–8887.

Latif, I. H. (2020). Time Evaluation of Different Cryptography Algorithms Using Labview. *IOP Conference Series: Materials Science and Engineering*, *745*(1). https://doi.org/10.1088/1757-899X/745/1/012039

Maqsood, F., Ahmed, M., Mumtaz Ali, M., & Ali Shah, M. (2017). Cryptography: A Comparative Analysis for Modern Techniques. In *IJACSA) International Journal of Advanced Computer Science and Applications* (Vol. 8, Issue 6). www.ijacsa.thesai.org

Panhwar, M. A., Ali Khuhro, S., Panhwar, G., & Memon, K. A. (2019). SACA: A Study of Symmetric and Asymmetric Cryptographic Algorithms. In *IJCSNS International Journal of Computer Science and Network Security* (Vol. 19, Issue 1).

Patil, P., Narayankar, P., Narayan, D. G., & Meena, S. M. (2016). A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish. *Procedia Computer Science*, *78*, 617–624. https://doi.org/10.1016/j.procs.2016.02.108

Ratnadewi, Adhie, R. P., Hutama, Y., Saleh Ahmar, A., & Setiawan, M. I. (2018). Implementation Cryptography Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES) Method in Communication System Based Near Field Communication (NFC). *Journal of Physics: Conference Series*, *954*(1). https://doi.org/10.1088/1742-6596/954/1/012009

Sivakumar, R., Balakumar, B., & Pandeeswaran, V. A. (2018). A Study of Encryption Algorithms (DES, 3DES and AES) for Information Security. *International Research Journal of Engineering and Technology*. www.irjet.net

Srinivasa Rao, O. (2015). Performance Analysis of DES and Triple DES. In *International Journal of Computer Applications* (Vol. 130, Issue 14).

Tankasali, S. P., & Shirahatti, S. (2020). Performance Analysis of DES and Triple DES Algorithm. *International Research Journal of Engineering and Technology*. www.irjet.net

Thahara, A., & Siregar, I. T. (2021). Implementasi Kriptografi untuk Keamanan Data dan Jaringan menggunakan Algoritma DES. *JURTI*, *5*(1).

Thirupalu, U., Scholar, R., & Reddy, E. K. (2019). Performance Analysis of Cryptographic Algorithms in the Information Security; Performance Analysis of Cryptographic Algorithms in the Information Security. *International Journal of Engineering Research & Technology (IJERT)*, *8*(2). www.ijert.org