Jurnal Siliwangi Vol.4. No.2, 2018 **P-ISSN 2477-3891**
Seri Sains dan Teknologi **E-ISSN 2615-4765**

PERBANDINGAN WAKTU DAN KECEPATAN PROSES ENKRIPSI DAN DEKRIPSI DATA TEKS.TXT MENGGUNAKAN ALGORITMA DES DAN 3DES

Akik Hidayat[1)], Deni Setiana[2)]

[1,2]Program Studi Teknik Informatika Departemen Ilmu Komputer
Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Padjadjaran
e-mail: akik@unpad.ac.id [1], deni@unpad.ac.id[2]

Abstrak

3DES (*Triple Data Encryption Standard*) adalah salah satu sistem enkripsi berlapis tiga dari sistem yang sebelumnya sudah ada, yaitu DES (*Data Encryption Standard*). Triple DES lebih aman dari DES, karena mengalami enkripsi tiga kali.Pada awalnya, ukuran kunci sandi DES yaitu 56 bit sudah mencukupi pada saat algoritme ini dibuat. Namun, dengan meningkatnya kemampuan komputasi, serangan brutal telah mungkin terjadi. Triple DES menyediakan metode yang sederhana dengan menambah ukuran kunci DES untuk mencegah serangan tersebut, tanpa memerlukan perancangan sandi blok (*block cipher*) yang sama sekali baru. Pada DES menggunakan satu kunci yang panjangnya 56-bit, sedangkan pada 3DES menggunakan 3 kunci yang panjangnya 168-bit (masing-masing panjangnya 56-bit). Pada 3DES, 3 kunci yang digunakan bisa bersifat saling bebas ($K_1 \neq K_2 \neq K_3$) atau hanya dua buah kunci yang saling bebas dan satu kunci lainnya sama dengan kunci pertama ($K_1 \neq K_2$ dan $K_3 = K_1$). Karena tingkat kerahasiaan algoritma 3DES terletak pada panjangnya kunci yang digunakan, maka penggunaan algoritma 3DES dianggap lebih aman dibandingkan dengan algoritma DES. Untuk memudahkan penggunaan algoritma 3DES, diperlukan software untuk dapat mengenkripsi dan mendekripsi file yang berekstensi .txt. serta mengetahui kecepatan dan kekuatan terhadap brute force menggunakan algoritma 3DES.

Kata kunci : 3DES (*Triple Data Encryption Standard*), DES (*Data Encryption Standard*), kriptografi, enkripsi, dekripsi, kunci. Brute force.

Abstract

3DES (Triple Data Encryption Standard) is one of the three layered encryption systems from the existing system, namely DES (Data Encryption Standard). Triple DES is safer than DES, because it was encrypted three times. Initially, the DES password lock size of 56 bits was sufficient when this algorithm was created. However, with increasing computing capabilities, brutal attacks have been possible. Triple DES provides a simple method by increasing the size of the DES key to prevent such attacks, without requiring a completely new block cipher. In DES it uses a key that is 56-bit long, whereas in 3DES it uses 3 keys that are 168-bits in length (each 56-bit in length). In 3DES, the 3 keys used can be mutually independent (K1 ≠ K2 ≠ K3) or only two keys are mutually independent and one other key is the same as the first key (K1 ≠ K2 and K3 = K1). Because the level of secrecy of the 3DES algorithm lies in the length of the key used, the use of the 3DES algorithm is considered safer than the DES algorithm. To facilitate the use of the 3DES algorithm, software is needed to be able to encrypt and decrypt files with the extension .txt. and know the speed and strength of brute force using the 3DES algorithm.

Keywords: *3DES (Triple Data Encryption Standard), DES (Data Encryption Standard), cryptography, encryption, decryption, keys. Brute force.*

I. PENDAHULUAN

Kriptografi adalah ilmu mengenai teknik enkripsi dimana "naskah asli" (plaintext) diacak menggunakan suatu kunci enkripsi menjadi "naskah acak yang sulit dibaca" (ciphertext) oleh seseorang yang tidak memiliki kunci dekripsi [1]. Sesuai dengan perkembangan zaman diperlukan suatu cara untuk mengamankan data dan informasi. Salah satu cara untuk mengamankan data adalah dengan cara merubah data tersebut ke dalam bentuk data yang lain yang tidak dapat dimengerti oleh pihak lain, yaitu dengan cara penyandian. Dalam kriptografi terdapat beberapa algoritma yang dapat menyandikan data. Algoritma yang paling terkenal adalah algoritma DES. DES ditetapkan sebagai standard untuk melindungi data dan informasi. Tetapi, DES dianggap sudah tidak aman lagi, karena dengan perangkat keras khususnya kuncinya dapat ditemukan dalam waktu beberapa hari. Kemudian

IBM yang membuat algotima DES mengembangkan DES menjadi 3DES. 3DES juga banyak digunakan dan penggunaannya lebih aman dibandingkan DES. Dalam paper ini dibahas tentang enkripsi dan dekripsi data dengan algoritma 3DES, dengan lama waktu yang diperlukan dan kecepatannya, serta kekuatan 3DES terhadap serangan *brute force*.

II. METODE PENELITIAN

Metode yang digunakan untuk mengembangkan aplikasi ini menggunakan Algoritma 3DES.

2.1. Operator Logika

Operator biner identik dengan bit pada komputer, yang melibatkan angka 0 dan angka 1. Operator yang digunakan pada algoritma 3DES adalah XOR. Operator XOR digunakan untuk dua inputan. Jika kedua inputan nilainya sama maka nilai outputnya 0, dan jika kedua inputan nilainya berbeda maka nilai outputnya 1 [2].

Tabel 1. Operator XOR

A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

2.2. Relasi Fungsi

Definisi 2.1 Suatu relasi *f* dari A ke B dikatakan suatu fungsi apabila setiap $x \in A$ dipasangkan atau dipetakan pada tepat satu unsur di B [3].

Definisi 2.2 $f : A \to B$ disebut fungsi *injektif* atau satu-satu apabila

$$x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$$

atau apabila

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2$$

Proses enkripsi dan proses dekripsi dapat dinyatakan dalam notasi matematika sebagai berikut:

$E_K(P) = C$ dan (1)

$D_K(C) = P$ (2)

dan keseluruhan dapat dinyatakan sebagai:

$D_K(E_K(P)) =$ (3)

Relasi antara himpunan P (plainteks) dengan himpunan C (cipherteks) harus merupakan fungsi korespondensi satu-satu (*one to one relation*). Maksudnya, dalam proses dekripsi hanya ada satu elemen C yang menyatakan satu elemen P.

2.3. Proses *Padding*

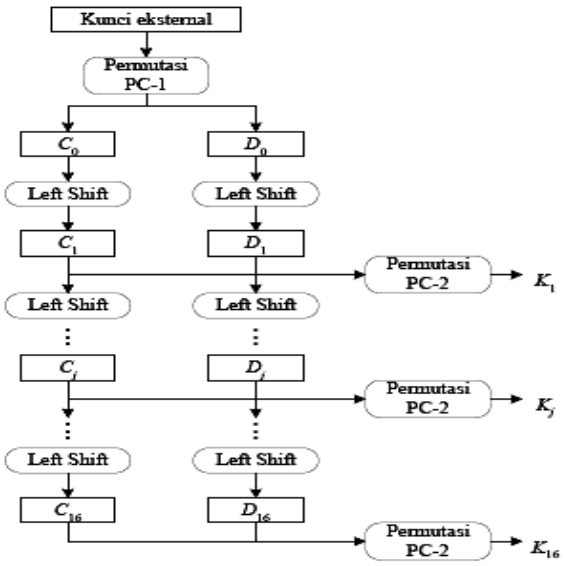
Proses *padding* adalah suatu proses penambahan byte-byte *dummy* pada byte-byte sisa yang masih kosong pada blok plainteks, disimpan pada posisi paling terakhir [4].

2.4. Data Encryption Standard

DES beroperasi pada ukuran blok 64-bit. DES mengenkripsikan 64-bit plainteks menjadi 64-bit cipherteks dengan menggunakan 56-bit kunci internal yang dibangkitkan dari kunci eksternal yang panjangnya 64-bit.

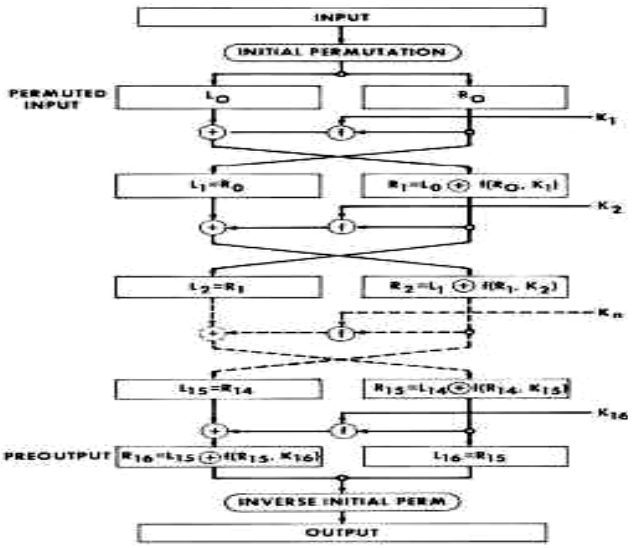
2.4.1. Proses Kunci

Kunci eksternal yang diinputkan akan diproses untuk mendapatkan 16 kunci internal. Pertama, Kunci eksternal yang panjangnya 64-bit disubstitusikan pada matriks permutasi kompresi PC-1. Dalam permutasi ini, setiap bit kedelapan (*parity bit*) dari delapan byte diabaikan. Hasil permutasi panjangnya menjadi 56-bit, yang kemudian dibagi menjadi dua bagian, yaitu kiri (C_0) dan kanan (D_0) masing-masing panjangnya 28-bit. Kemudian, bagian kiri dan kanan melakukan pergeseran bit pada setiap putaran sebanyak satu atau dua bit tergantung pada tiap putaran. Pada proses enkripsi, bit bergeser kesebelah kiri (*left shift*). Sedangkan untuk proses dekripsi, bit bergeser kesebelah kanan (*right shift*). Setelah mengalami pegeseran bit, C_i dan D_i digabungkan dan disubstitusikan pada matriks permutasi kompresi dengan menggunakan matriks PC-2, sehingga panjangnya menjadi 48-bit. Proses tersebut dilakukan sebanyak 16 kali secara berulang-ulang.



Gambar 1. Proses Pembangkitan Kunci-kunci Internal DES [5].

2.4.2. Proses Enkripsi



Gambar 2. Proses Enkripsi DES [6].

Plainteks yang diinputkan pertama akan disubatitusikan pada matriks permutasi awal (*initial permutation*) atau IP panjangnya 64-bit. Kemudian dibagi menjadi dua bagian, yaitu kiri (*L*) dan kanan (*R*) masing-masing panjangnya menjadi 32-bit. Kedua bagian ini masuk ke dalam 16 putaran DES. Satu putaran DES merupakan model jaringan Feistel, secara matematis jaringan Feistel dinyatakan sebagai berikut:

$$L_i = R_{i-1} \quad ; 1 \le i \le 16 \qquad (4)$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, k_i) \qquad (5)$$

Bagian *R* disubstituaikan pada fungsi ekspansi panjangnya menjadi 48-bit kemudian di-XOR-kan dengan kunci internal yang sudah diproses sebelumnya pada proses pembangkitan kunci (pada putaran pertama menggunakan kunci internal pertama, dan seterusnya). Hasil XOR kemudian disubstitusikan pada *S-box* yang dikelompokkan menjadi 8 kelompok, masing-masing 6-bit hasilnya menjadi 4-bit. Kelompok 6-bit pertama menggunakan S_1, kelompok 6-bit kedua menggunakan S_2, dan seterusnya. Setelah proses *S-box* tersebut panjangnya menjadi 32-bit. Kemudian disubstitusikan lagi pada matriks permutasi *P-box*, kemudian di-XOR-kan dengan bagian *L*. Hasil dari XOR tersebut disimpan untuk bagian *R* selanjutnya. Sedangkan untuk bagian *L* diperoleh dari bagian *R* yang sebelumnya. Proses tersebut dilakukan 16 kali.

Setelah 16 putaran selesai, bagian *L* dan *R* digabungkan dan disubstitusikan pada matriks permutasi awal balikan (*invers initial permutation*) atau IP^{-1} [7], hasilnya merupakan cipherteks 64-bit.

2.4.3. Proses Dekripsi

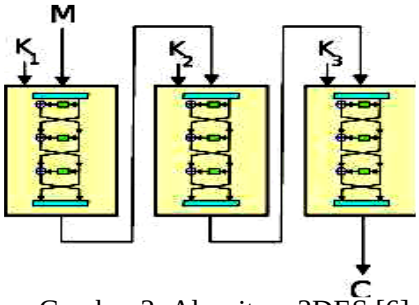
Proses dekripsi terhadap cipherteks merupakan kebalikan dari proses enkripsi. DES menggunakan algoritma yang sama untuk proses enkripsi dan dekripsi. Jika pada proses enkripsi urutan kunci internal yang digunakan adalah $k_1, k_2, ..., k_{16}$ maka pada proses dekripsi urutan kunci internal yang digunakan adalah $k_{16}, k_{15}, ..., k_1$.

2.5. Triple Data Encryption Standard

3DES (*Triple Data Encryption Standard*) merupakan suatu algoritma pengembangan dari algoritma DES (*Data Encryption Standard*). Pada dasarnya algoritma yang digunakan sama, hanya pada 3DES dikembangkan dengan melakukan enkripsi dengan implementasi algoritma DES sebanyak tiga kali. 3DES memiliki tiga buah kunci yang berukuran 168-bit (tiga kali kunci 56-bit dari DES). Pada algoritma 3DES dibagi menjadi tiga tahap, setiap tahapnya merupakan implementasi dari algoritma DES.

Tahap pertama, plainteks yang diinputkan dioperasikan dengan kunci eksternal pertama (K_1) dan melakukan proses enkripsi dengan menggunakan algoritma DES. Sehingga menghasilkan pra-cipherteks pertama. Tahap kedua, pra-cipherteks pertama yang dihasilkan pada tahap pertama, kemudian dioperasikan dengan kunci eksternal kedua (K_2) dan melakukan proses enkripsi atau proses dekripsi (tergantung cara pengenkripsian yang digunakan) dengan menggunakan algoritma

DES. Sehingga menghasilkan prs-cipherteks kedua. Tahap terakhir, pra-cipherteks kedua yang dihasilkan pada tahap kedua, dioperasikan dengan kunci eksternal ketiga (K_3) dan melakukan proses enkripsi dengan menggunakan algoritma DES, sehingga menghasilkan cipherteks (C).



Gambar 3. Algoritma 3DES [6].

2.5.1. Pemilihan Kunci

Ada dua pilihan untuk pemilihan kunci eksternal algoritma 3DES [6], yaitu:

a. K_1, K_2, dan K_3 adalah kunci-kunci yang saling bebas

$K_1 \neq K_2 \neq K_3 \neq K_1$

b. K_1 dan K_2 adalah kunci-kunci yang saling bebas, dan K_3 sama dengan K_1

$K_1 \neq K_2$ dan **$K_3 = K_1$**

2.5.2. Proses Enkripsi dan Dekripsi

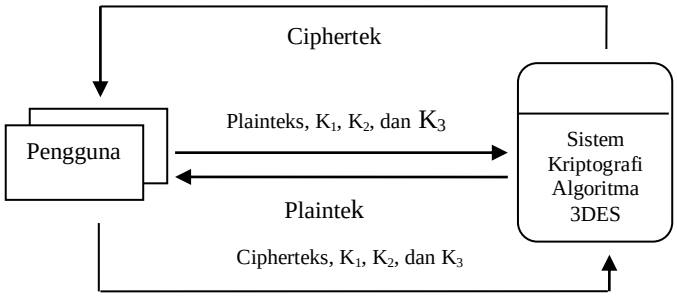
Proses enkripsi dan dekripsi algoritma 3DES dapat dicapai dengan beberapa cara [8], yaitu:

Tabel 2. Cara pengenkripsian dan pendekripsian

Cara	Enkripsi	Dekripsi
1	DES – EDE2 ▪ $K_1 \neq K_2$, $K_3 = K_1$ ▪ C = E [D {E (P, K_1), K_2}, K_3]	DES – DED2 ▪ $K_1 \neq K_2$, $K_3 = K_1$ ▪ P = D [E {D (C, K_3), K_2}, K_1]
2	DES – EEE2 ▪ $K_1 \neq K_2$, $K_3 = K_1$ ▪ C = E [E {E (P, K_1), K_2}, K_3]	DES – DDD2 ▪ $K_1 \neq K_2$, $K_3 = K_1$ ▪ P = D [D {D (C, K_3), K_2}, K_1]
3	DES – EDE3 ▪ $K_1 \neq K_2 \neq K_3 \neq K_1$ ▪ C = E [D {E (P, K_1), K_2}, K_3]	DES – DED3 ▪ $K_1 \neq K_2 \neq K_3 \neq K_1$ ▪ P = D [E {D (C, K_3), K_2}, K_1]
4	DES – EEE3 ▪ $K_1 \neq K_2 \neq K_3 \neq K_1$ ▪ C = E [E {E (P, K_1), K_2}, K_3]	DES – DDD3 ▪ $K_1 \neq K_2 \neq K_3 \neq K_1$ ▪ P = D [D {D (C, K_3), K_2}, K_1]

2.6. Perancangan Sistem

Perancangan dimulai dengan pembuatan diagram konteks, berupa gambaran sistem penerapan algoritma 3DES secara garis besar.



Gambar 4. Diagram Konteks

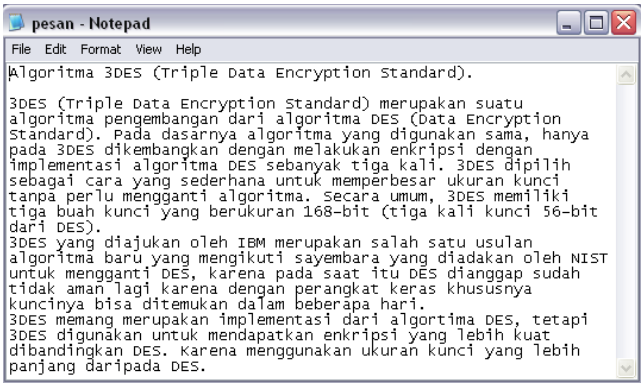
III. HASIL DAN PEMBAHASAN

Contoh file yang akan dienkripsi dan didekripsi berikut ini diambil dari file yang berekstensi .txt yang berukuran 1 KB (Kilo Byte) dan kunci yang digunakan adalah saling bebas ($K_1 \neq K_2 \neq K_3 \neq K_1$) yaitu:

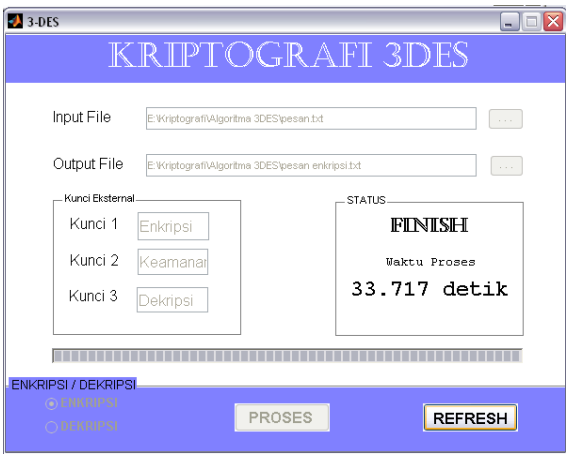
- Kunci 1 : Enkripsi
- Kunci 2 : Keamanan
- Kunci 3 : Dekripsi

Cara pengenkripsian yang dipilih adalah DES – EDE3 dan cara pendekripsian yang dipilih adalah DES – DED3 :

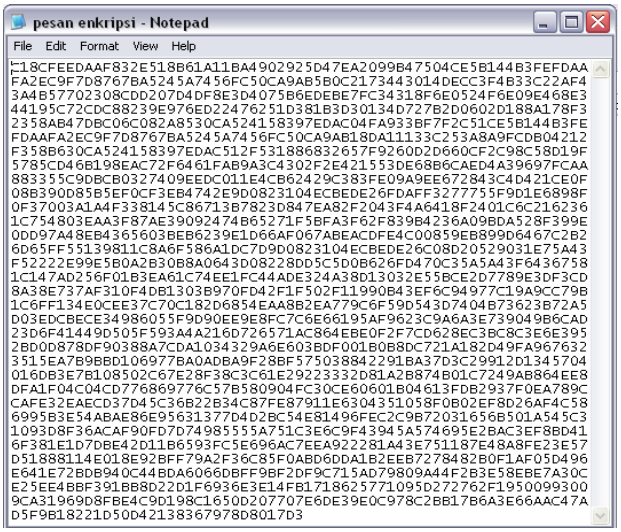
Contoh file plainteks:



Gambar 5. Contoh file plainteks



Gambar 6. Tampilan Aplikasi



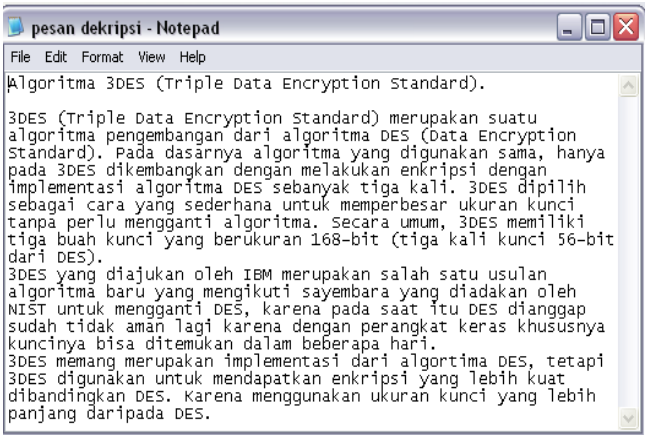
Gambar 7. Contoh file cipherteks

Cipherteks diatas akan didekripsikan kembali dengan menggunakan tiga buah kunci yang sama pada proses enkripsi.

Aplikasi yang akan ditampilkan adalah sebagai berikut:

Gambar 8. Proses dekripsi

Maka hasilnya akan sama dengan plainteks semula, yaitu:



Gambar 9. Hasil dekripsi

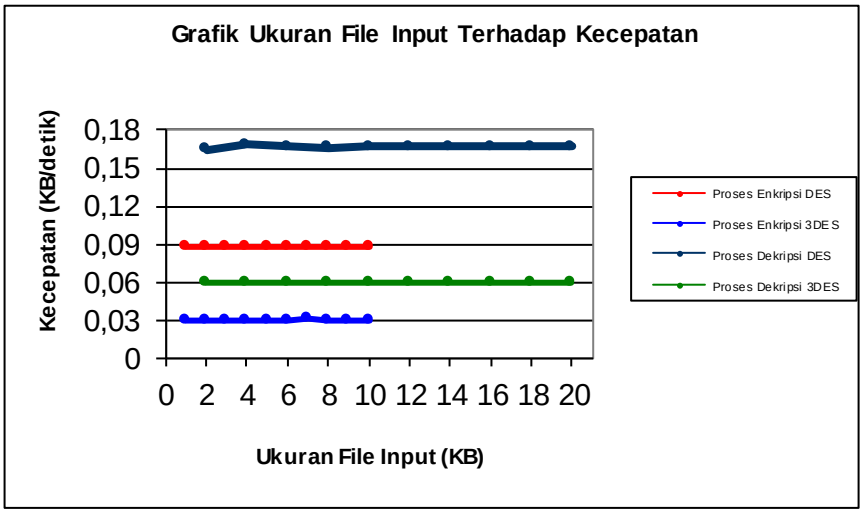
Berikut akan ditampilkan proses file untuk algoritma DES dan algoritma 3DES, dengan kunci yang digunakan sebagai berikut:

- Kunci 1 : Software
- Kunci 2 : Komputer
- Kunci 3 : Hardware

Tabel 3. Waktu Proses dan Kecepatannya untuk Proses Enkripsi dengan Algoritma DES dan Algoritma 3DES

No	Nama File			Ukuran File (KB)		Waktu Proses (detik)		Kecepatan (KB/detik)	
	Input	Output							
		DES	3DES	Input	Output	DES	3DES	DES	3DES
1	P1.txt	EP1 DES.txt	EP1 3DES.txt	1	2	11.34	33.093	0.08818	0.03022
2	P2.txt	EP2 DES.txt	EP2 3DES.txt	2	4	22.658	66.197	0.08827	0.03021
3	P3.txt	EP3 DES.txt	EP3 3DES.txt	3	6	33.98	99.302	0.08829	0.03021
4	P4.txt	EP4 DES.txt	EP4 3DES.txt	4	8	45.26	132.324	0.08838	0.03023
5	P5.txt	EP5 DES.txt	EP5 3DES.txt	5	10	56.586	165.29	0.08836	0.03025
6	P6.txt	EP6 DES.txt	EP6 3DES.txt	6	12	67.924	198.463	0.08833	0.03023
7	P7.txt	EP7 DES.txt	EP7 3DES.txt	7	14	79.262	231.15	0.08831	0.03028
8	P8.txt	EP8 DES.txt	EP8 3DES.txt	8	16	90.733	264.882	0.08817	0.03020
9	P9.txt	EP9 DES.txt	EP9 3DES.txt	9	18	101.909	297.451	0.08831	0.03026
10	P10.txt	EP10 DES.txt	EP10 3DES.txt	10	20	113.342	330.389	0.08823	0.03027
Kecepatan Rata-rata								**0.08828**	**0.03024**

Dimana P adalah pesan, EM adalah enkripsi pesan, dan DP adalah dekripsi pesan.



Gambar 10. Grafik Ukuran File Input Terhadap Kecepatan

3.1. Tingkat Kerahasiaan Kunci

Semakin panjang kunci yang digunakan, semakin kuat tingkat kerahasiaannya. Algoritma 3DES menggunakan kunci yang panjangnya 168 bit, maka jumlah seluruh kombinasi kemungkinan kunci yang harus dicoba untuk memecahkan cipherteks [9] adalah $2^{168} = 3,741\times10^{50}$ kali. Karena, ada 168 posisi pengisian bit yang masing-masing mempunyai dua nilai kemungkinan, yaitu 0 dan 1.

3.2. Kekuatan Terhadap Serangan *Brute Force*

Brute force adalah teknik mencoba satu persatu kemungkinan kunci untuk memperoleh plainteks. Waktu yang diperlukan untuk mencoba seluruh kemungkinan kunci oleh serangan *brute force* adalah [10].

$$\frac{2^{168}}{3600\times24\times366}=\frac{3.741\times10^{50}}{31.622.400}=1.183\times10^{43}$$

IV. KESIMPULAN

Proses enkripsi dan dekripsi suatu data dengan algoritma 3DES dilakukan dengan cara mengimplementasikan algoritma DES sebanyak tiga kali, sesuai dengan pemilihan kuncinya dan urutan proses yang dipilih. Sedangkan Waktu yang diperlukan untuk proses enkripsi dan dekripsi dipengaruhi oleh ukuran file, spesifikasi pada perangkat keras, dan proses lain yang sedang dilakukan oleh perangkat keras. Plainteks yang diproses dengan kunci 1, kunci 2, dan kunci 3 menghasilkan cipherteks dengan jumlah karakter yang lebih besar, karena adanya proses padding dan disimpan dalam bentuk heksadesimal. Jika salah satu kunci atau ketiga kunci dirubah, maka cipherteks juga akan berubah. Kecepatan untuk proses enkripsi dan dekripsi pada setiap pertambahan ukuran file input sebesar 1 KB, kecepatannya adalah sama. Untuk algoritma 3DES, pada proses enkripsi kecepatan rata-ratanya adalah 0.03024 KB/detik dan pada proses dekripsi kecepatan rata-ratanya adalah 0.05908 KB/detik. Sedangkan untuk algoritma DES, pada proses enkripsi kecepatan rata-ratanya adalah 0.08828 KB/detik dan pada proses dekripsi kecepatan rata-ratanya adalah 0.16667 KB/detik. Sedangkan rata rata waktu proses enkripsi 3DES adalah 62.2 dtk dan Dekripsinya 181,9 dtk, sedangkan rata rata waktu proses enkripsi DES adalah 65,98 dtk dan Dekripsinya 186,9 dtk. Sehingga waktu proses Enkripsi dan dekripsi DES lebih cepat dari pada 3DES sedangkan Untuk Kecepatannya 3DES lebih cepat daripada DES. Untuk mendapatkan plainteks tanpa mengetahui kuncinya, jumlah kombinasi kemungkinan kunci yang harus dicoba adalah sebanyak $3,741\times10^{50}$ kali sedangkan Waktu yang diperlukan untuk mencoba seluruh kemungkinan kunci oleh serangan *brute force* adalah $1,183\times10^{43}$ tahun.

V. DAFTAR PUSTAKA

[1] Felix, Fidens. 2006. *Dasar Kriptografi*, (online), http://www.ilmukomputer.com, (diakses September 2007).

[2] Purcell, Edwin J. 2001. *Kalkulus Edisi ke-7 Jilid 1*. Terjemahan oleh I Nyoman Susila. 2001. Bandung: Interaksara.
[3] Bartle, Robert G.1994. *Introduction to Real Analysis Second Edition*. Singapore: John Wiley.
[4] Menezes, Alfred J. 1996. *Handbook of Applied Cryptography*. CRC Press.
[5] Stinson, Douglas. 1995. *Cryptography: Theory and Practice, (online)*, http://www.easywebtech.com, (diakses 22 Januari 2018).
[6] NIST. 2004. *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, (online), http://www.csrc.nist.gov, (diakses 22 Januari 2018).
[7] Achmad, Ikhwanudin. 2007. *An Application of Generalized Inverse Matrices on the Hill Cipher*, (online), http://www.ikhwan.web.ugm.ac.id, (diakses 22 Januari 2018).
[8] Hasan, Rusydi. 2003. *Mengenal Algoritma DES*, (online), http://www.ilmukomputer.com, (diakses September 2017).
[9] Away, Gunaidi A. 2006. *The Shortcut of Matlab Programming.* Bandung: Informatika.
[10] Risanto. 2006. *Keamanan Data dengan Kriptografi Kunci Simetris Algoritma DES*. Skripsi tidak diterbitkan. Bandung: Program Pascasarjana UNPAD.