ISSN 2477-0043
e-ISSN 2460-7908

Jurnal Teknologi Terpadu
Vol. 4, No. 1, Juli 2018

Perbandingan Algoritma DES, AES, IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data

Donzilio Antonio Meko
Program Studi Teknik Informatika, STIMIK Kupang
E-mail: donzi.antonio.g@gmail.com

ABSTRACT

Kemajuan teknologi informasi telah memberikan dampak yang sangat luas, salah satunya sebagai media penyampaian informasi dari suatu tempat ke tempat lainnya, sehingga memudahkan orang dalam mengakses suatu informasi. Kemudahan pengaksesan media komunikasi oleh semua orang, tentunya akan memberikan dampak bagi keamanan informasi atau pesan yang menggunakan media komunikasi tersebut. Informasi menjadi sangat rentan untuk diketahui, diambil dan dimanipulasi oleh pihak-pihak yang tidak bertanggung jawab. Oleh sebab itu dibutuhkan suatu metode atau cara yang dapat menjaga kerahasiaan informasi ini, yang salah satunya dikenal dengan sebutan kriptografi. Dalam kriptografi terdapat banyak algoritma, diantaranya algoritma DES, AES, IDEA dan Blowfish. Penelitian ini bertujuan untuk membandingkan kinerja beberapa algoritma kriptografi dalam proses enkripsi dan dekripsi data berdasarkan segi kecepatan atau lama waktu serta ukuran file hasil enkripsi. Hasil penelitian ini menunjukkan adanya perbedaan waktu proses serta ukuran file dari hasil enkripsi dan dekripsi data dari masing-masing algoritma.

Kata Kunci *: Algoritma, Deskripsi, Enskripsi, DES, AES, IDEA, Blowfish*

1. PENDAHULUAN

Kemajuan teknologi informasi yang sangat pesat turut memajukan media komunikasi sebagai media penyampaian informasi dari suatu tempat ke tempat lainnya, sehingga memudahkan orang dalam mengakses media komunikasi. Kemudahan pengaksesan media komunikasi oleh semua orang, tentunya akan memberikan dampak bagi keamanan informasi atau pesan yang menggunakan media komunikasi tersebut. Informasi menjadi sangat rentan untuk diketahui, diambil dan dimanipulasi oleh pihak-pihak yang tidak bertanggung jawab. Oleh sebab itu dibutuhkan suatu metode atau cara yang dapat menjaga kerahasiaan informasi ini, yang salah satunya dikenal dengan sebutan kriptografi.

Algoritma kriptografi dapat dibagi ke dalam kelompok algoritma simetris dan algoritma asimetris. Algoritma simetris merupakan algoritma kriptografi yang menggunakan kunci yang sama baik untuk proses enkripsi maupun dekripsi. Algoritma simetris dapat dikelompokkan menjadi dua kategori, yaitu *cipher* aliran dan *cipher* blok. *Cipher* aliran merupakan algoritma kriptografi yang beroperasi dalam bentuk bit tunggal. Sedangkan algoritma kriptografi kategori *cipher* blok beroperasi dalam bentuk blok bit. Saat ini sudah banyak berkembang algoritma kriptografi simetris baik untuk kategori *cipher* aliran maupun *cipher* blok.

Beberapa algoritma kriptografi yang dikategorikan ke dalam algoritma simetris adalah DES, AES, Blowfish, IDEA, Saphent, Skipjack, Twofish dan lain-lain. Setiap algoritma simetris ini memiliki kelebihan dan kekurangan masing-masing dalam proses enkripsi dan dekripsi data dilihat dari segi kecepatan maupun keamanan data *ciphertext* yang dihasilkan.

Dilihat dari perbedaan-perbedaan ini maka penulis tertarik untuk mengimplementasikan dan membandingkan kinerja algoritma DES, AES, IDEA dan Blowfish dalam suatu program aplikasi enkripsi dan dekripsi data digital yang dinilai dari kecepatan proses data atau lama waktu yang dibutuhkan untuk mengenkripsi atau mendekripsi file serta ukuran file hasil enkripsi

2. LANDASAN TEORI

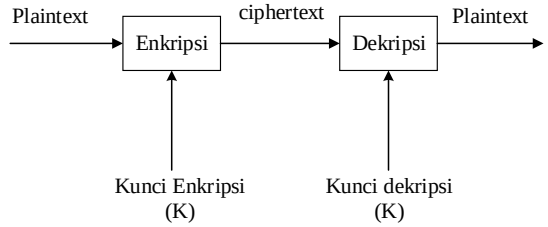
a. Pengertian Kriptografi

Kata kriptografi berasal dari bahasa Yunani, "*kryptós*" yang berarti tersembunyi dan "*gráphein*" yang berarti tulisan. Kriptografi merupakan ilmu yang mempelajari Teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan

data, antektikasi, integritas dan keabsahan data. Kriptografi juga dapat diartikan sebagai ilmu untuk menjaga kerahasiaan pesan [1]

b. **Pengertian Kriptografi Simetris**

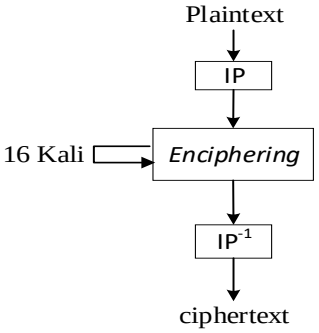
Algoritma ini disebut simetris karena memiliki *key* atau kunci yang sama dalam proses enkripsi dan dekripsi sehingga algoritma ini juga sering disebut algoritma kunci tunggal atau satu kunci. *Key* dalam algoritma ini besifat rahasia atau *private key* sehingga algoritma ini juga disebut dengan algoritma kunci rahasia [2].



Gambar 1. Kriptografi Simetris

c. **Data Encryption Standard (DES)**

DES, atau juga dikenal sebagai *Data Encryption Algorithm* (DEA) oleh ANSI dan DEA-1 oleh ISO, merupakan algoritma kriptografi simetris yang paling umum digunakan saat ini. Secara umum, DES termasuk ke dalam sistem kriptografi simetri dan tergolong jenis *cipher* blok. DES beroperasi pada ukuran blok 64 bit. DES mengenkripsikan 64 bit *plainteks* menjadi 64 bit *cipherteks* dengan menggunakan 56 bit kunci internal (*internal key*) atau lupa-kunci (*subkey*). Kunci internal dibangkitkan dari kunci eksternal *(external key)* yang panjangnya 64 bit [3]



Gambar 2. Skema global dari algoritma DES

d. **Pengertian Advanced Encryption Standard (AES)**

AES adalah lanjutan dari algoritma enkripsi standar DES. AES merupakan algoritma *cryptographic* yang dapat digunakan untuk mengamankan data. Algoritma AES adalah blok*chipertext* simetrik yang dapat mengenkripsi (*encipher*) dan dekripsi (*decipher*) informasi. Enkripsi merubah data yang tidak dapat lagi dibaca disebut *ciphertext*, sebaliknya dekripsi adalah merubah *ciphertext* data menjadi bentuk semula yang kita kenal sebagai *plaintext*. Algoritma AES menggunakan kunci kriptografi 28, 192, dan 256 bit untuk mengenkrip dan dekripsi data pada blok 128 bits [3]

e. **International Data Encryption Algorithm (IDEA)**

IDEA adalah algoritma enkripsi blok kunci yang aman dan rahasia yang dikembangkan oleh James Massey dan Xuejia Lai. Algoritma ini berkembang pada 1992 dari algoritma semula yang disebut dengan *Proposed Encryption Standard and The Inproved Proposed Encryption Standard*. IDEA merupakan algoritma simetris yang beroperasi pada sebuah blok pesan terbuka dengan lebar 64 bit dan panjang kunci berukuran 128 bit. Algoritma IDEA menggunakan algoritma yang sama untuk proses enkripsi dan dekripsi. Dan pesan rahasia yang dihasilkan oleh algoritma ini berupa blok pesan rahasia dengan lebar atau ukuran 64 bit. [4]

Algoritma IDEA menggunakan operasi campuran dari tiga operasi aljabar yang berbeda, yaitu :

a. Operasi XOR, operasi ini disimbolkan dengan tanda $\oplus$
b. Operasi penjumlahan modulo 2^{16} .
c. Operasi perkalian modulo ($2^{16} + 1$).

f. **Algoritma Blowfish**

Blowfish alias "*OpenPGP.Cipher.4*" merupakan enkripsi yang termasuk dalam golongan *Symmetric Cryptosystem*, metoda enkripsinya mirip dengan DES (*DES-like Cipher*) diciptakan oleh seorang *Cryptanalyst* bernama Bruce Schneier Presiden perusahaan *Counterpane Internet Security, Inc* (Perusahaan konsultan tentang kriptografi dan keamanan Komputer) dan dipublikasikan tahun 1994. Blowfish termasuk dalam enkripsi block *Cipher* 64-bit dangan panjang kunci yang bervariasi antara 32-bit sampai 448-bit [5].

Algoritma Blowfish terdiri atas dua bagian :

a. Key-Expansion

Berfungsi merubah kunci (Minimum 32-bit, Maksimum 448-bit) menjadi beberapa array subkunci (subkey) dengan total 4168 byte.

b. Enkripsi Data

Terdiri dari iterasi fungsi sederhana (*Feistel Network*) sebanyak 16 kali putaran. Setiap putaran terdiri dari permutasi kunci-*dependent* dan substitusi kunci- dan data-*dependent*. Semua operasi adalah

penambahan (*addition*) dan XOR pada variabel 32-bit. Operasi tambahan lainnya hanyalah empat penelusuran tabel (*table lookup*) *array* berindeks untuk setiap putaran.

3. METODE PENELITIAN

a. Jenis Penelitian

Model/jenis penelitian dalam penelitian ini adalah menggunakan metode penelitian komparatif yaitu penelitian membandingkan persamaan dan perbedaan dua atau lebih fakta-fakta dan sifat-sifat objek yang diteliti berdasarkan kerangka pemikiran tertentu. Pada penelitian ini variabelnya masih mandiri tetapi untuk sampel yang lebih dari satu atau dalam waktu yang berbeda.

Penelitian komparatif dapat juga diartikan sebagai sejenis penelitian deskriptif yang ingin mencari jawaban secara mendasar tentang sebab-akibat, dengan menganalisis faktor-faktor penyebab terjadinya ataupun munculnya suatu fenomena tertentu.

Jadi penelitian komparatif adalah jenis penelitian yang digunakan untuk membandingkan antara dua kelompok atau lebih dari suatu variabel tertentu. Sehingga model penelitian ini berusaha memberikan gambaran perbandingan algoritma cipher DES, AES, IDEA dan Blowfish dalam proses enkripsi dan dekripsi data dilihat dari kecepatan proses

b. Antarmuka Perangkat Lunak

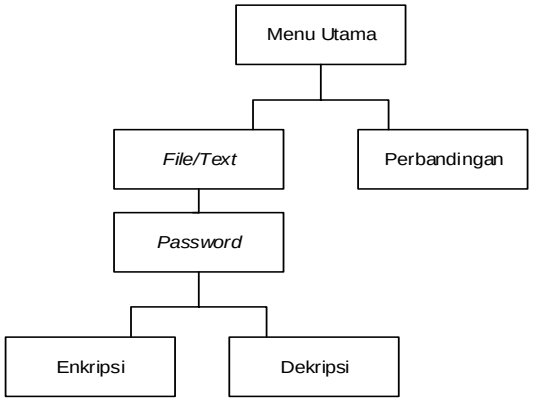
Dalam penelitian ini, adapun spesifikasi perangkat lunak yang digunakan:

d. *Microsoft Visual Basic* 6.0 sebagai Bahasa pemrograman.
e. StarUML sebagai media perancangan system

c. Perancangan dan Konstruksi Sistem

Tahapan dalam pembuatan perangkat lunak ini terdiri atas beberapa bagian utama sebagai berikut:

i. Hirarki Proses

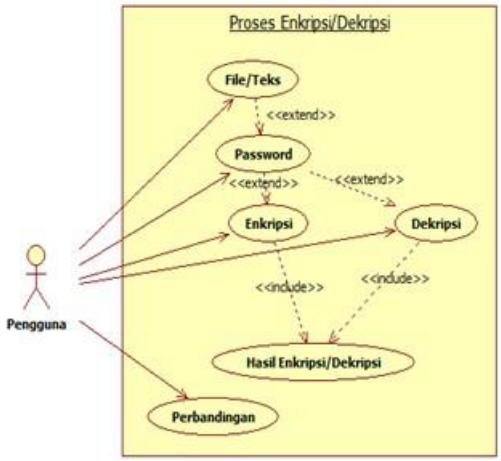


Gambar 3. Hirarki Proses

Dari aplikasi yang dibuat terdapat beberapa menu utama yakni file/text yang digunakan untuk enkripsi dan dekripsi teks ataupun file yang dipilih oleh user. Menu perbandingan untuk menampilkan form perbandingan dimana didalam form ini dapat menampilkan hasil dari perbandingan algoritma yang ada.

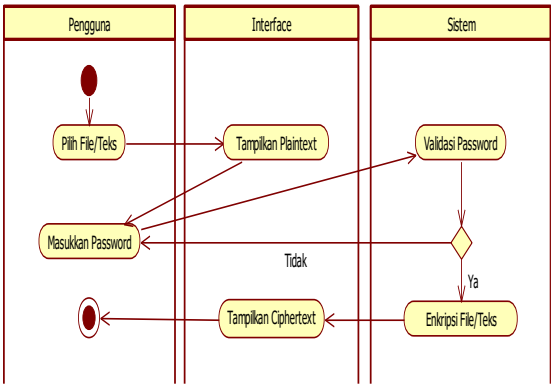
ii. *Usecase Diagram*

Usecase menggambarkan interaksi yang terjadi dalam sistem, yang memberi gambaran user atau actor yang berhubungan dengan sistem dan hal-hal yang berhubungan dengan user di dalam sistem.



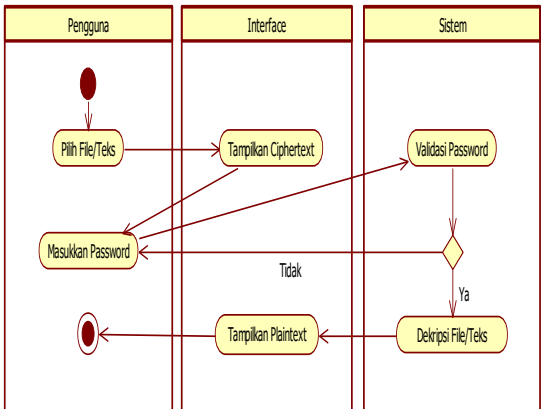
Gambar 4. *Usecase Diagram*

iii. Activity Diagram Enkripsi



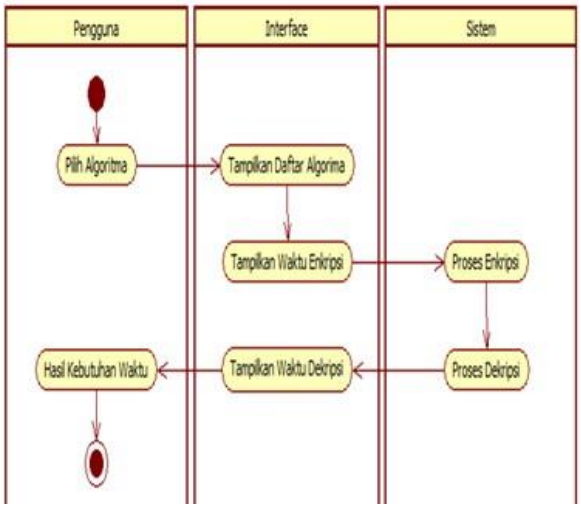
Gambar 5. *Activity Diagram Enkripsi*

iv. Activity Diagram Dekripsi



Gambar 6. *Activity Diagram Dekripsi*

***v. Activity Diagram* Perbandingan**

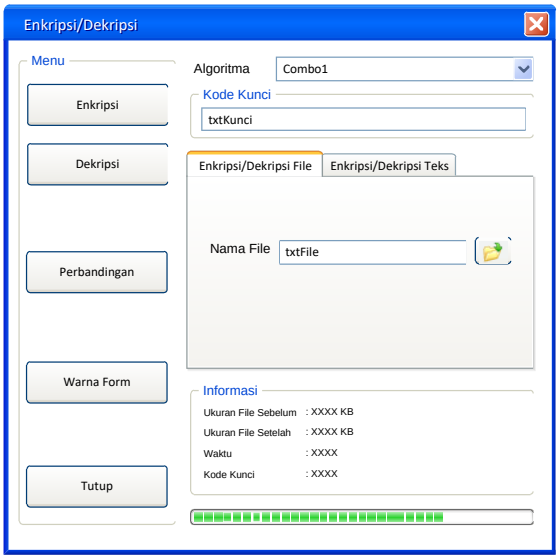


Gambar 7. *Activity Diagram* Perbandingan

vi. Perancangan Antarmuka

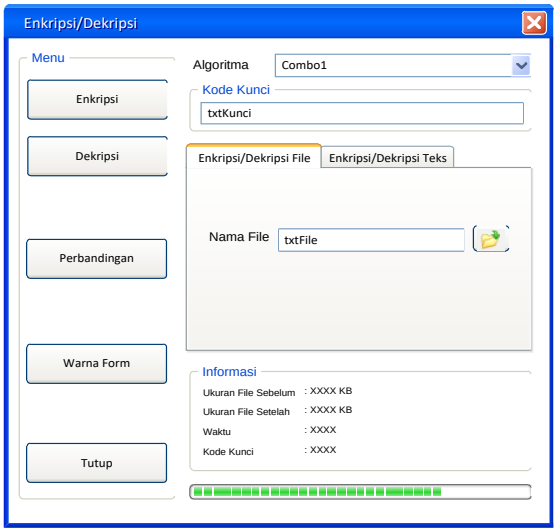
Bagian ini akan merupakan implementasi atau kontruksi tampilan dari program yang akan dibuat

g. Perancangan *Form* Enkripsi/Deskripsi File



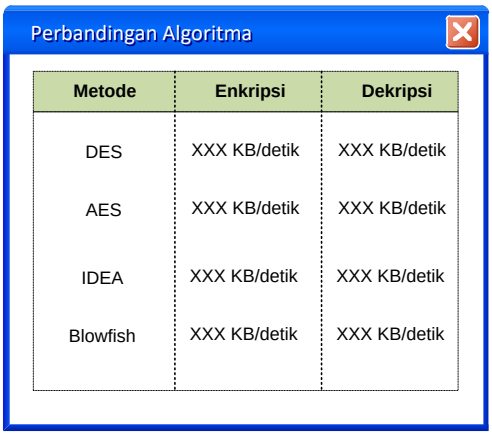
Gambar 8. Perancangan *Form* Enkripsi/Deskripsi File

h. Perancangan *Form* Enkripsi/Deskripsi Teks



Gambar 9. Perancangan *Form* Enkripsi/Deskripsi Teks

i. Perancangan Form Perbandingan Algoritma



Gambar 10. Perancangan Form Perbandingan Algoritma

4. HASIL DAN PEMBAHASAN

a. Implementasi Sistem

Aplikasi dapat berjalan dengan baik apabila memiliki *file-file* pendukung untuk menunjang proses yang akan dijalankan.

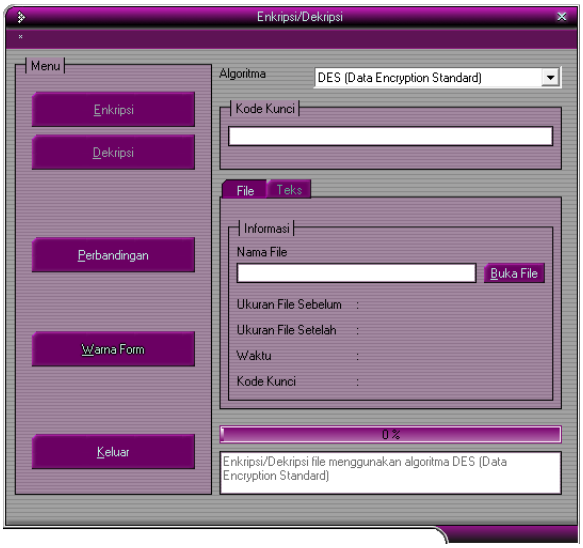
Berikut adalah beberapa *file* pendukung dalam implementasi program ini yaitu:

Tabel 1. File pendukung implementasi program

No	Nama Folder	Nama / Tipe File	Deskripsi
1	Enkripsi-Dekripsi	Enkripsi-Dekripsi.exe	File executable untuk menjalankan aplikasi Enkripsi-Dekripsi
2	\Classes	*.cls	Berisi file-file class untuk keempat algoritma
3	\Skins	*.skn	Berisi file-file skin/kulit form
4	\Forms	*.frm dan *.frx	Berisi file-file form aplikasi
5	\Modules	*.bas	Berisi file-file modul untuk mendukung desain aplikasi dimana didiklarasikan berbagai fungsi pendukung program
6	\Package	*.*	Berisi file-file setup untuk menginstalkan komponen-komponen pendukung seperti file-file *.dll, file *.ocx dan file-file komponen pendukung lainnya

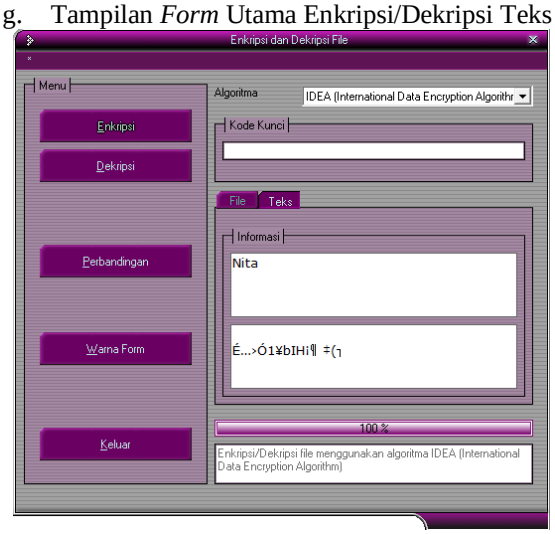
b. Antarmuka Sistem

f. Tampilan *Form* Utama



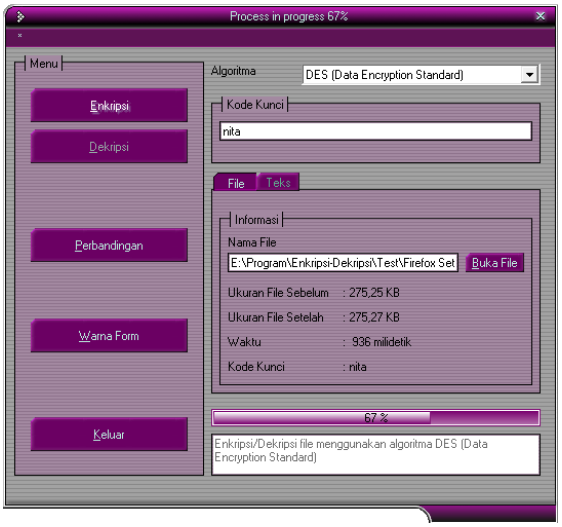
Gambar 11. Tampilan form utama

g. Tampilan *Form* Utama Enkripsi/Dekripsi Teks



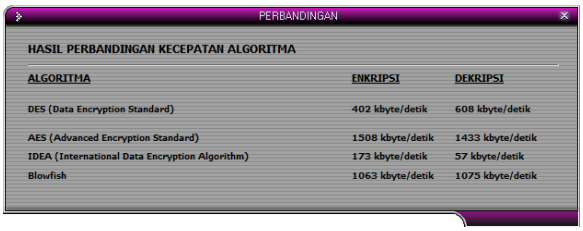
Gambar 12. Tampilan *Form* Utama Enkripsi/Dekripsi Teks

h. Tampilan *Form* Utama Enkripsi/Dekripsi File



Gambar 13. Tampilan *Form* Utama Enkripsi/Dekripsi File

i. Tampilan Form Perbandingan Algoritma



Gambar 14 Tampilan form Jenis Motif

c. **Pengujian Validitas**

Pengujian validitas ini dilakukan untuk menguji keabsahan dari aplikasi yang dibuat untuk membuktikan hipotesis. Penulis menggunakan dua teknik untuk menguji validitas aplikasi yang dibuat yaitu pengukuran berdasarkan kecepatan dekripsi dan enkripsi file dan pengukuran berdasarkan besar file yang dihasilkan

Untuk melakukan pengujian ini maka penulis menggunakan beberapa tipe file dengan berbagai macam ukuran seperti tampak pada tabel berikut ini

Tabel 2. File-file uji aplikasi

No	Nama File	Tipe File	Ukuran (byte)
1	BAB I.doc	Microsoft Office Word Document (.doc)	110.592
2	BAB I.pdf	PDF Document (.pdf)	77.824
3	BAB I.txt	Text Document (.txt)	8.192
4	Enkripsi-Dekripsi.exe	Application (.exe)	405.504
5	Enkripsi-Dekripsi.rar	WinRAR archive (.rar)	86.016
6	Enkripsi-Dekripsi.zip	WinRAR ZIP archive (.zip)	114.688
7	logo.bmp	BMP File (.bmp)	69.632
8	logo.gif	GIF File (.gif)	12.288
9	logo.jpg	JPG File (.jpg)	24.576
10	logo.png	PNG File (.png)	45.056
11	olah data.xls	Microsoft Office Excel Worksheet (.xls)	69.632
12	Pororo.mp4	MPEG-4 File Format (.mp4)	13.885.440
13	Tom and Jerry.flv	Flash Video File (.flv)	21.344.256

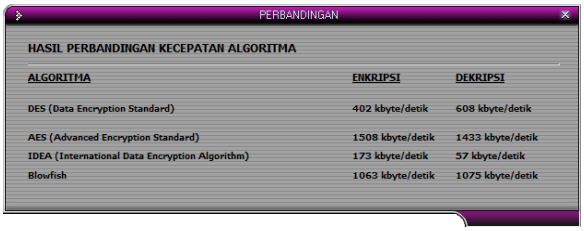
Dari beberapa tipe file di atas maka dapat dilakukan proses pengujian enkripsi dan dekripsi data dengan menggunakan algoritma DES, AES, IDEA dan Blowfish dan hasil yang diperoleh dapat dilihat pada tabel berikut ini:

Tabel 3. Hasil pengujian implementasi program

Algoritma	Tipe File	Enkripsi		Dekripsi	
		Ukuran (byte)	Kecepatan	Ukuran (byte)	Kecepatan
DES	Doc	110.592	531	110.592	515
	Pdf	77.824	484	77.824	4.306
	Txt	8.192	764	8.192	2.215
	Exe	409.600	920	405.504	1.045
	Rar	86.016	484	86.016	1.996
	Zip	114.688	484	114.688	1.622
	Bmp	69.632	437	69.632	421
	Gif	12.288	359	12.288	1.359
	Jpg	24.576	468	24.576	100
	Png	45.056	405	45.056	1.248
	Xls	69.632	437	69.632	468
	Mp4	13.885.440	18.190	13.885.440	19.563
	Flv	21.344.256	27.768	21.344.256	30
Rata-rata		**2.789.061**	**3.979**	**2.788.746**	**2.684**
AES	Doc	110.592	390	110.592	390
	Pdf	77.824	406	77.824	405
	Txt	8.192	390	8.192	390
	Exe	409.600	468	405.504	624
	Rar	409.600	499	86.016	561
	Zip	409.600	530	114.688	499
	Bmp	69.632	374	69.632	375
	Gif	69.632	375	12.288	390
	Jpg	69.632	374	24.576	374
	Png	69.632	405	45.056	390
	Xls	69.632	375	69.632	406
	Mp4	3.885.440	5.679	13.885.440	5.834
	Flv	21.344.256	8.783	21.344.256	8.938
Rata-rata		**2.077.174**	**1.465**	**2.788.746**	**1.506**
IDEA	Doc	110.592	983	110.592	200
	Pdf	110.596	927	77.824	2.184
	Txt	8.192	893	8.192	2.215
	Exe	409.600	2.512	405.504	7.066
	Rar	409.600	2.574	86.016	6.942
	Zip	409.600	2.559	114.688	6.989
	Bmp	69.632	733	69.632	1.498
	Gif	69.632	796	12.288	1.482
	Jpg	69.632	718	24.576	1.466
	Png	69.632	764	45.056	1.467

Cara mengukur kecepatan enkripsi dan dekripsi data selain dilakukan secara menual, juga dapat dilakukan dangan teknik *benchmarking* yaitu salah satu fitur pengujian kecepatan yang disediakan di dalam aplikasi untuk mengukur kecepatan enkripsi dan dekripsi data dari setiap algoritma dalam satuan kilobyte per dektik.

Pada teknik *benchmarking* ini dilakukan *buffering* data di memori dengan ukuran sebesar 1.000.000 bytes atau kurang lebih berukuran 1 GB sehingga diperoleh informasi dari aplikasi seperti gambar berikut:



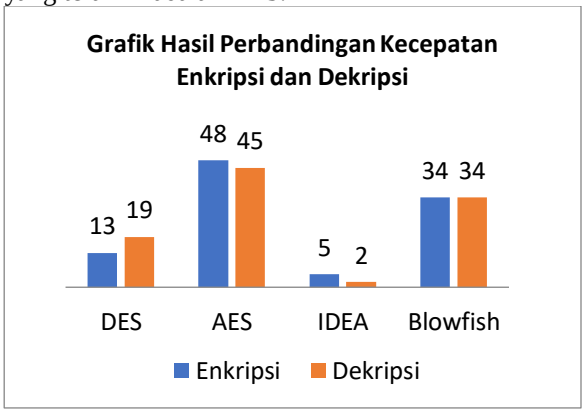
Gambar 15. Hasil perbandingan kecepatan enkripsi dan dekripsi data dengan teknik *benchmark*

Dari form perbandingan algoritma maka dapat dirangkum hasil kecepatan proses enkripsi/dekripsi data dari keempat algoritma seperti pada tabel 4 berikut ini

Tabel 4 Hasil analisis perbandingan kecepatan algoritma

Algoritma	Enkripsi (kbyte/detik)	Dekripsi (kbyte/detik)
DES	402	608
AES	1.508	1.433
IDEA	173	57
Blowfish	1.063	1.075

Berdasarkan hasil analisis Perbandingan Kecepatan dekripsi algoritma keempat algoritma di atas dapat dilihat bahwa persentasi tertinggi dari algoritma AES 45%, Blowfish 34%, DES 19% dan terakhir adalah algoritma IDEA yang hanya memiliki kecepatan 2%. Sehingga dapat disimpulkan bahwa algorima AES jauh lebih cepat dari algoritma dari ketiga algoritma lainnya dalam hal proses enkripsi dan dekripsi data diikuti oleh Blowfish, DES, IDEA dan yang terakhir adalah AES.



Gambar 16. Grafik Persentasi Perbandingan Kecepatan Enkripsi dan Dekripsi dari Algoritma

5. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan maka dapat disimpulkan bahwa :

a. Kecepatan enkripsi dan dekripsi data dengan menggunakan algoritma DES lebih cepat dibanding algoritma IDEA dimana untuk persentasi kecepatan algoritma DES adalah 13% untuk proses enkripsi data dan 19% untuk dekripsi data. Sedangkan algoritma IDEA memiliki kecepatan enkripsi sebesar 5% dan dekripsi sebesar 2%
b. Kecepatan enkripsi dan dekripsi data dengan menggunakan algoritma Blowfish lebih baik dari DES dimana untuk persentasi kecepatan algoritma Blowfish memiliki kecepatan yang sama antara proses enkripsi dan dekripsi data yaitu sebesar 34%. Sedangkan algoritma DES memiliki kecepatan enkripsi sebesar 13% dan dekripsi sebesar 19%
c. Kecepatan enkripsi dan dekripsi data dengan menggunakan algoritma AES lebih baik dibanding algoritma Blowfish dimana untuk persentasi kecepatan algoritma AES adalah 48% untuk proses enkripsi data dan 45% untuk dekripsi data. Sedangkan algoritma Blowfish memiliki kecepatan enkripsi dan dekripsi data sama yaitu 34%
d. Kecepatan enkripsi dan dekripsi data dengan menggunakan algoritma AES lebih baik dibanding algoritma IDEA dimana untuk persentasi kecepatan algoritma AES adalah 48% untuk proses enkripsi data dan 45% untuk dekripsi data. Sedangkan algoritma IDEA memiliki kecepatan enkripsi dan dekripsi data sama yaitu 34%
e. Kecepatan enkripsi dan dekripsi data dengan menggunakan algoritma AES lebih baik dibanding algoritma ketiga algoritma lainnya yaitu DES, Blowfish dan IDEA dimana kecepatan tertinggi untuk proses enkripsinya adalah 48% dan kecepatan dekripsinya adalah 45% dan kecepatan terendah dimiliki oleh algoritma IDEA yaitu kecepatan enkripsi sebesar 5% dan dekripsi sebesar 2%

DAFTAR PUSTAKA

[1] Kromodimoeljo, S. 2009. Teori dan Aplikasi Kriptografi. SPK IT Consulting
[2] Arrijal, I. M, Efendi. R, dan Susilo. B. 2016. Penerapan Algoritma Kriptografi Kunci Simetris dengan Modifikasi Vigenere Cipher dalam Aplikasi Kriptografi Teks. Jurnal Pseudocode. Vol. III. No. 1. Pp. 69-82
[3] Anoop MS. Public Key Cryptography (Applications Algorithm and mathematical Explanations)
[4] Steven S. 2006. Studi Perbandingan Algoritma IDEA dengan DES. Proyek Akhir. ITB
[5] E.Utami, S. Erikawaty, dan A. Tambunan. 2010. Pendahuluan Cryptosystem. Jurnal Dasi, Vol. 11. No. 2. Pp. 33-44