2nd Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
21 Maret 2023 – Jakarta, Indonesia
Volume 2, Nomor 1, April 2023 - ISSN 2962-8628 (*online*)

IMPLEMENTASI ALGORITME *ADVANCED ENCRYPTION STANDAR* (AES-128) UNTUK MENGAMANKAN DOKUMEN PADA PT. JIA DREAMS COMMUNICATIONS

Shafa Ibnu Hafiz Abimanyu[1*], Purwanto[2], Windarto[3], Dewi Kusumaningsih[4]

[1,2,3,4] Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, DKI Jakarta, Indonesia

Email: [1*]2011500507@student.budiluhur.ac.id, [2]purwanto@budiluhur.ac.id, [3]windarto@budiluhur.ac.id, [4]dewi.kusumaningsih@budiluhur.ac.id
(* : corresponding author)

Abstrak-Perkembangan teknologi semakin pesat disegala bidang khususnya teknologi informasi. Sehingga kerahasiaan data atau informasi merupakan suatu kelengkapan pelayanan yang dibuat untuk menjaga agar informasi yang tersimpan tidak dapat dibaca atau dibuka oleh pihak yang tidak berhak.PT. JIA Dreams Communications yang berlokasi di Jl.Antene I, Gandaria Utara, Kec. Kebayoran Baru, Kota Jakarta Selatan. Dimana selama ini menjalani bisnis inti penjualan dan promosi. Dengan seiring waktu, pengalaman dan kompetensi yang terus bertambah hingga daftar keahlian bisnis meluas ke *event management*, *activation*, *sales force service*, branding, *production* dan *customer retention.* PT. JIA Dreams Communications selama ini masih menggunakan pengamanan *file* yang dapat mudah diakses oleh siapapun, untuk menjaga agar informasi yang tersimpan tidak dapat dibaca atau dibuka oleh pihak yang tidak berhak, konsep perlindungan informasi data dapat dilakukan dengan sistem enkripsi dan deskripsi menggunakan *algoritma Advanced Encryption Standard* (AES-128). Proses enkripsi dapat diartikan sebagai proses pesan asli (*plaintext*) menjadi suatu pesan yang tersandi (*chipertext*). Dengan itu muncul suatu ide yang tertuju yaitu merancang sistem keamanan yang dapat digunakan untuk melindungi data berupa *file* dengan menerapkan kriptografi pada sebuah program mengamankan *file* dalam menyimpan data dengan cara dienkripsi dan didekripsi. Sehingga data file yang asli tidak terbaca jika telah dienkripsi, file yang lebih besar durasi waktu proses enkripsi dan dekripsi file akan lebih lama. Pada hasil pengujian file tidak berubah ukurannya, sehingga dari hasil implementasi disimpulkan bahwa algoritma kriptografi AES-128 dapat mengimplementasikan dalam pengamanan isi file.

Kata Kunci: Algoritma *Advanced Encryption Standard*(AES-128), Dekripsi, Enkripsi, Kriptografi

IMPLEMENTATION OF STANDARD ADVANCED ENCRYPTION ALGORITHMS (AES-128) TO SECURE DOCUMENTS ON PT. JIA DREAMS COMMUNICATIONS

Abstrak-*The development of technology is increasingly rapid in all fields, especially information technology. So that the confidentiality of data or information is a completeness of services made to keep the stored information unreadable or opened by parties who do not berhak.PT. JIA Dreams Communications is located on Jl.Antene I, Gandaria Utara, Kebayoran Baru District, South Jakarta City. Where so far it has been running the core business of sales and promotion. With time, experience and competencies continue to grow until the list of business expertise extends to event management, activation, sales force service, branding, production and customer retention. PT. JIA Dreams Communications so far still uses file security that can be easily accessed by anyone, to keep stored information unreadable or opened by unauthorized parties, the concept of data information protection can be done with an encryption and description system using the Advanced Encryption Standard (AES-128) algorithm. The encryption process can be interpreted as the process of the original message (plaintext) into an encoded message (chipertext). With that, an idea emerged that was to design a security system that could be used to protect data in the form of files by applying cryptography to a program to secure files in storing data by encrypting and decrypting. So that the original file data is not read if it has been encrypted, files that have a larger duration of time for encrypting and decrypting files will be longer. In the test results, the file does not change in size, so from the implementation results it is concluded that the AES-128 cryptographic algorithm can implement in securing the contents of the file.*

Keywords*: Advanced Encryption Standard Algorithm(AES-128), Cryptography, Decryption, Encryption*

1. PENDAHULUAN

Perkembangan teknologi terkini telah memungkinkan orang untuk berkomunikasi dan berbagi data dan informasi tanpa batasan jarak atau waktu. Seiring dengan berkembangnya tuntutan akan keamanan yang kerahasiaan informasi yang dipertukarkan, ketersediaan informasi dan sistem keamanan informasi yang lebih baik untuk melindungi data terhadapat pencurian data. Karena perkembangan metode pembelajaran ilmiah, privasi adalah efek positif adanya sistem keamanan untuk melindungi data yang dikirimkan melalui jaringan telekomunikasi, konsep perlindungan informasi data dapat dilakukan dengan sistem enkripsi dan deskripsi

menggunakan *algoritma Advanced Encryption Standard* (AES-128) dalam menyimpan data. Proses enkripsi dapat diartikan sebagai proses perubahan dari suatu pesan asli (*plaintext*) menjadi suatu pesan yang terlindungi dalam hal ini pesan yang tersandi (*chipertext*), sedangkan untuk proses deskripsi adalah suatu proses pengembalian pesan tersandi yang terlindungi menjadi bentuk data asli pesan tersebut, teknik penyandian tersebut dikenal dengan kriptografi.

PT. JIA Dreams Communications selama ini belum menggunakan pengamanan *file* sehingga dapat mudah diakses oleh siapapun. Terkait dengan masalah yang ada dan pentingnya pengamanan *file* maka dalam penelitian ini akan direncanakan untuk mengimplementasikan konsep pengamanan isi *file* yang digunakan untuk melindungi *file* PT. JIA Dreams Communications dan informasi penting demi menjaga kerahasiaan isi *file* dengan kriptografi. PT. JIA Dreams Communications didirikan pada Agustus 2001 yang saat ini kantor terletak di Jl.Antene I, Gandaria Utara, Kec. Kebayoran Baru, Kota Jakarta Selatan. Dimana selama ini menjalani bisnis inti penjualan dan promosi. Dengan seiring waktu, pengalaman dan kompetensi yang terus bertambah hingga daftar keahlian bisnis meluas ke *event management*, *activation*, *sales force service*, branding, *production* dan *customer retention.*

PT. JIA Dreams Communications memiliki dokumen, dokumen tersebut penting dan bersifat rahasia karena terdapat data perusahaan. Dokumen tersebut harus dijaga dengan baik sehingga tidak bisa disalah gunakan oleh orang lain yang tidak perlu mengetahui informasi tersebut. Dengan itu muncul suatu ide yang tertuju dari permasalahan yang ada, yaitu merancang sistem keamanan yang dapat digunakan untuk melindungi data berupa *file* dengan menerapkan kriptografi dengan metode algoritme *Advanced Encryption Standard* (AES-128) pada sebuah program, mengamankan *file* PT. JIA Dreams Communications dalam menyimpan data, denga cara di enkripsi dan di deskripsi. *Advanced Encryption Standard* (AES-128) secara garis besar beroperasi pada blok 128-bit atau 16 karakter, yang berarti dapat digunakan untuk enkripsi teks. File dokumen terdiri dari barisan teks yang tentu saja berukuran lebih dari 16 karakter.

2. METODE PENELITIAN

2.1 Penerapan Metode

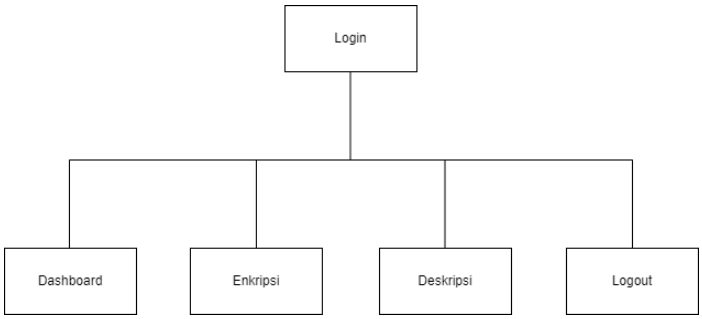
Pada proses penerapan dalam membangun sistem enkripsi keamanan file, dalam topik ini akan menggunakan keamanan yang telah ditentukan untuk menyimpan *file* data dengan menggunakan algoritma *Advanced Encryption Standard* (AES-128). Pengujian ini menggunakan metode *blackbox testing,* yaitu salah satu metode yang menguji perangkat lunak yang difokuskan untuk menguji fungsi-fungsi dari web yang akan dibangun. Ada beberapa tahapan dalam pengujian yang dilakukan untuk mengetahui dari setiap fungsi-fungsi dari elemen yang terdapat pada aplikasi dapat bekerja dengan baik. Rencana pengujian pada penelitian, terdapat pada Tabel 1.

Tabel 1. Tahapan Pengujian

No.	Pengujian	Hasil yang diharapkan
1	Tombol *Login*	Dapat mengakses ke halaman menu utama
2	Tombol Menu *Dashboard*	Bisa menampilkan halaman *dashboard*
3	Tombol Menu Enkripsi	Bisa menampilkan halaman enkripsi
4	Tombol Menu Enkripsi *File*	Bisa mengenkripsi *file*
5	Tombol *Choose File*	Dapat menambahkan *file*
6	Tombol Dekripsi	Bisa menampilkan halaman dekripsi
7	Tombol Dekripsi *File*	Bisa mengdekripsi *file*
8	Tombol *Download*	Bisa mengunduh *file*
9	Tombol *Delete*	Bisa menghapus data yang muncul di tabel
10	Tombol *About*	Dapat menampilkan tentang aplikasi program
11	Tombol *Help*	Dapat menampilkan cara menjalankan aplikasi program
12	Tombol *Logout*	Dapat mengakses kembalik ke halaman *login*

2.2 Rancangan Menu

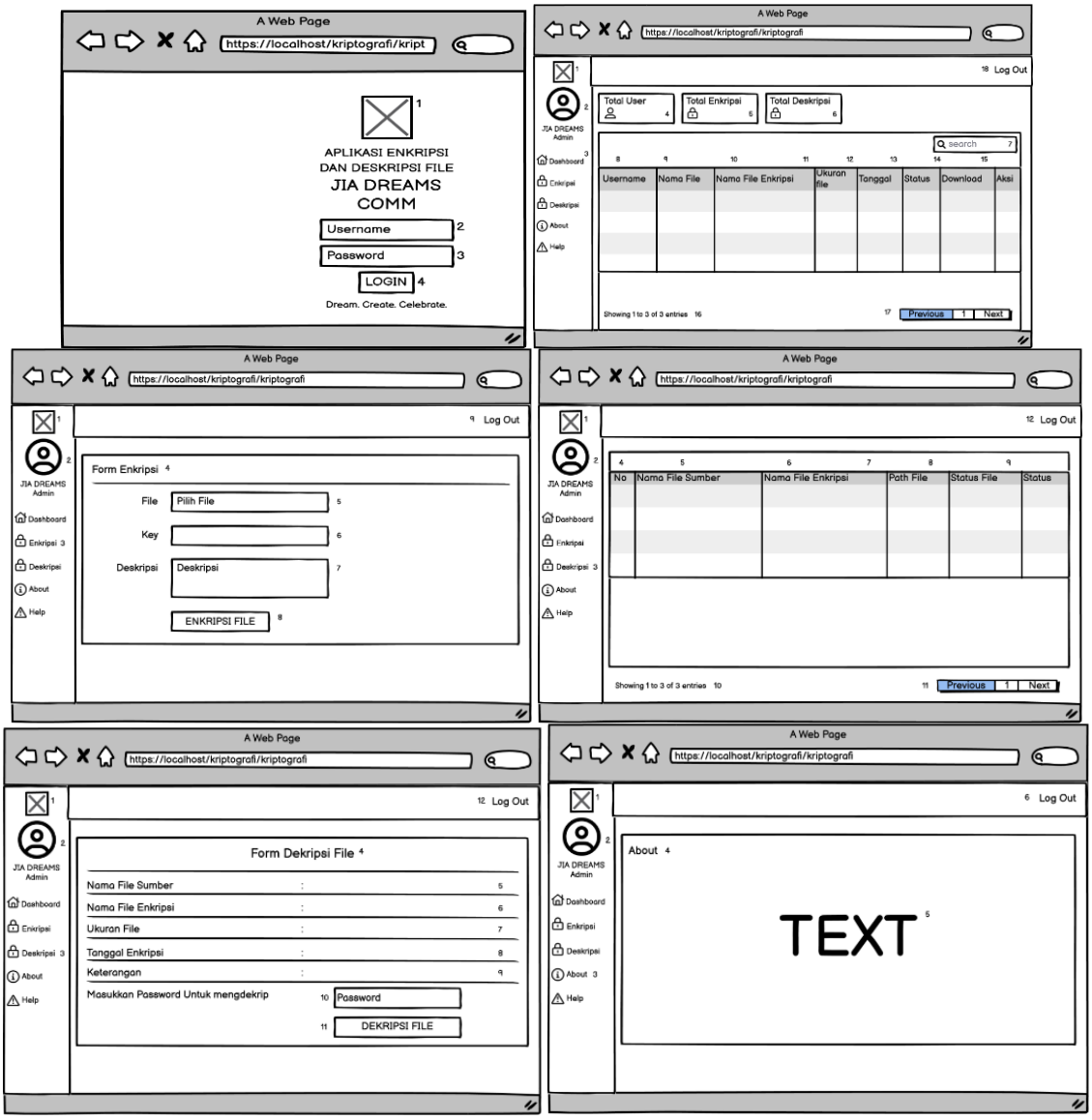
Rancangan menu dalam aplikasi yang akan dibuat terdiri dari beberapa tampilan menu yang dapat dilihat pada gambar berikut:



Gambar 1. Rancangan Menu

2.3 Rancangan Layar

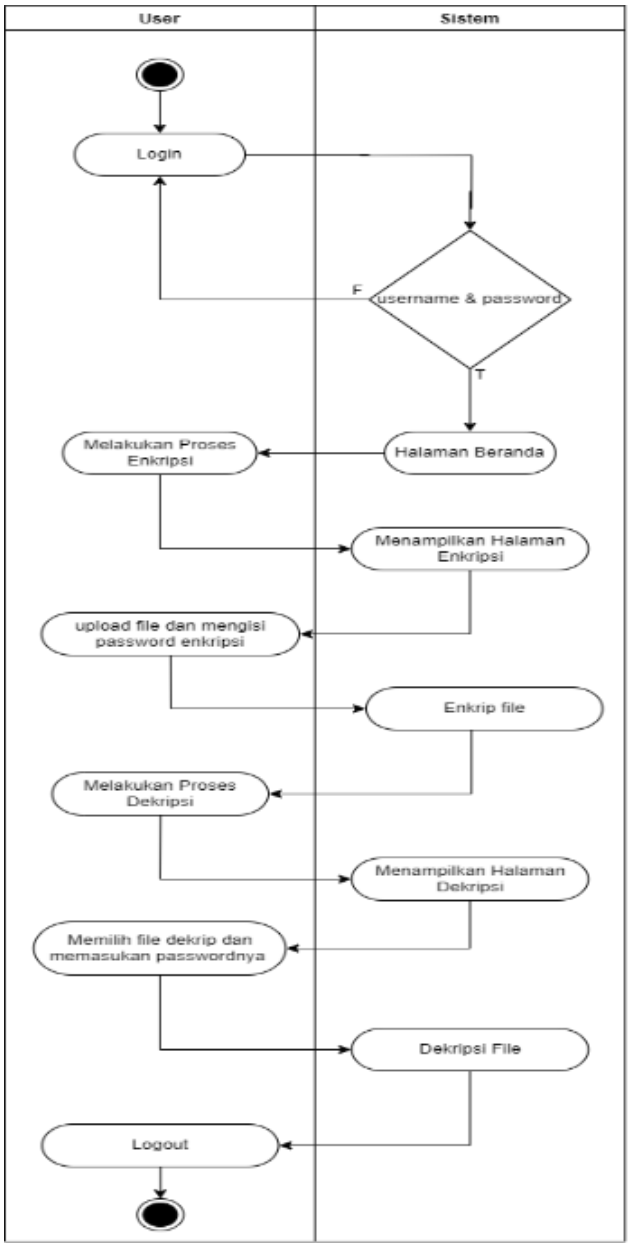
Rancangan layar merupakan suatu hal yang sangat penting. Selain itu, rancangan layar juga harus mudah dimengerti oleh pengguna, karena jika tidak,user akan tidak tertarik dengan sistem aplikasi yang telah dibuat. Pada Gambar 2 adalah beberapa rancangan sistem aplikasi yang akan dibuat.



Gambar 2. Rancangan Layar

2.4 Activity Diagram

Activity Diagram adalah rancangan aliran dari suatu aktivitas atu alur kerja dalam sebuah sistem yang akan berjalan. Activity Diagram memiliki komponen dengan bentuk tertentu yang dihubungkan oleh anak panah yang berarah dengan urutan aktivitas dari awal sampai akhir. Pada Gambar 3 adalah gambar activity diagram dari proses pengaman dokumen.



Gambar 3. Activity Diagram

2.5 Metode Kriptografi *Advanced Encryption Standard* (AES-128)

Algoritma block cipher dengan sifat simetris yang menggunakan kunci simetris selama proses enkripsi dan dekripsi. Enkripsi AES menggunakan proses berulang yang disebut loop. Jumlah putaran yang digunakan oleh AES bergantung pada panjang kunci yang digunakan. Setiap putaran membutuhkan kunci dan masukan dari putaran berikutnya. Kunci yang dihasilkan didasarkan pada kunci yang ditentukan. Algoritma AES dapat melakukan enkripsi dan dekripsi dengan panjang kunci yang berbeda yaitu 128 bit, 192 bit dan 256 bit. Jumlah lilitan mempengaruhi panjang kunci, perbedaan ketiga kunci dapat dilihat pada Tabel 2. Perbandingan jumlah kunci AES

Tabel 1. Tahapan Pengujian

Tipe.	Panjang Kunci (NK *Words*)	Ukuran Blok (Nb *Words*)	Jumlah Putaran (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Garis besar algoritma Rijndael yang beroperasi pada blok 128-bit dengan kunci 128-bit adalah sebagai berikut:

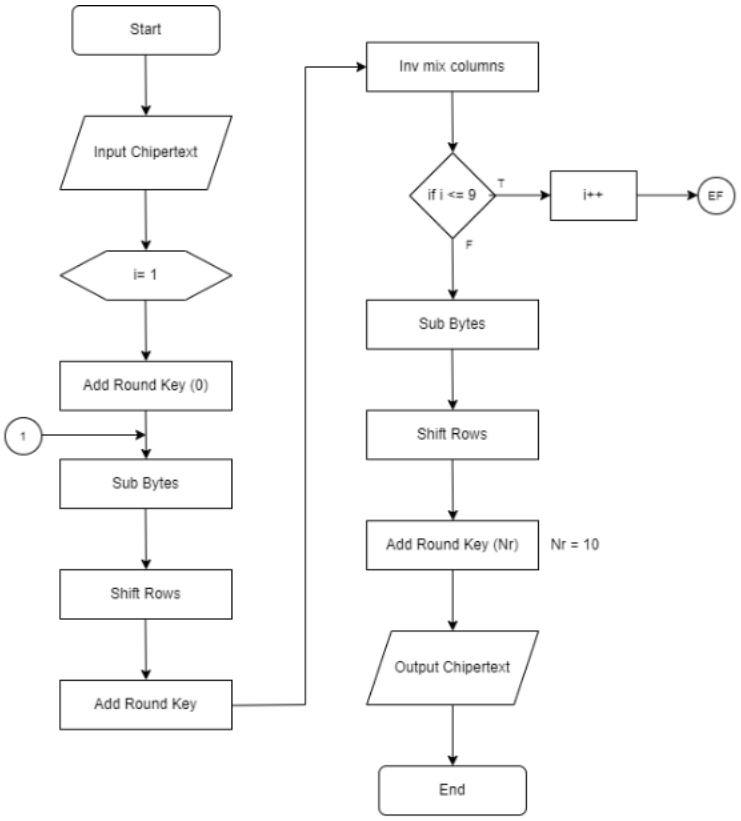
1. *AddRoundKey* : Melakukan XOR antara *state* awal (*plaintext*) dengan chiperkey, tahapan ini disebut juga initial round.
2. Putaran sebanyak Nr – 1 kali. Proses yang dilakukan pada setiap putaran adalah:
   a. *SubBytes* : subtitusi byte dengan menggunakan tabel subtitusi (S-box).
   b. *ShiftRows* : pergeseran baris-baris *array state* secara wrapping.
   c. *MixColumns* : mengacak data di masing-masing kolom *array state.*
   d. *AddRoundKey* : melakukan XOR antara *state* sekarang dengan *round key*.
   3. Final Round : proses untuk putaran terakhir :
   a. *SubBytes*
   b. *ShiftRows*
   c. *AddRoundKey*

3. HASIL DAN PEMBAHASAN

Pada bagian ini berisi analisis, hasil implementasi ataupun pengujian serta pembahasan dari topik penelitian, yang bisa dibuat terlebih dahulu metodologi penelitian. Bagian ini juga merepresentasikan penjelasan yang berupa penjelasan, gambar, tabel dan lainnya.

3.1 Flowchart Enkripsi AES-128

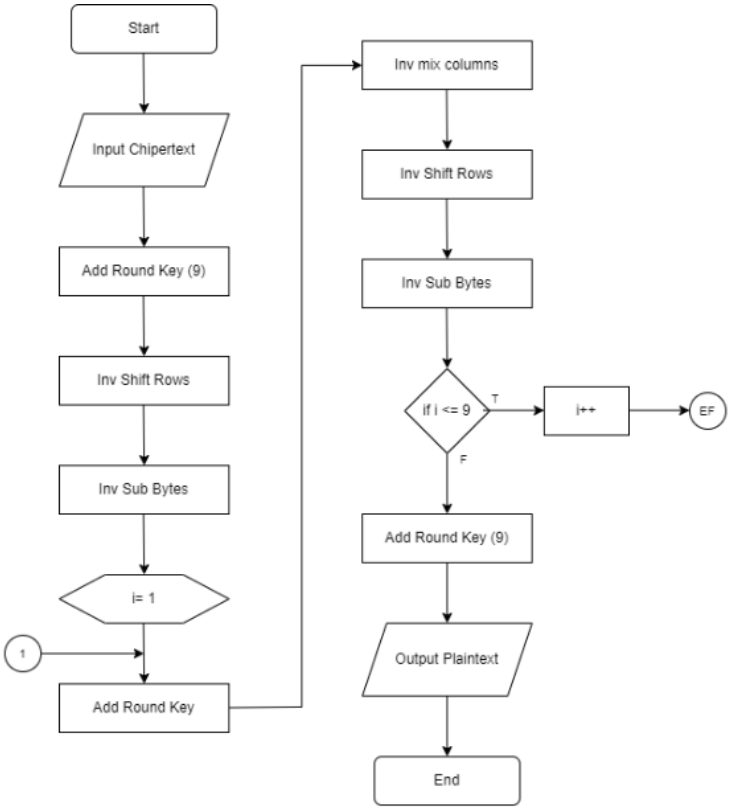
Alur pada proses enkripsi AES-128 ini terdapat pada Gambar 4. Pada halaman enkripsi AES-128 ini menjelaskan tentang melakukan alur dari enkripsi dalam aplikasi ini.



Gambar 4. Flowchart Enkripsi AES-128

3.2 *Flowchart* Dekripsi AES-128

Alur pada proses dekripsi AES-128 ini terdapat pada gambar 5. Pada halaman dekripsi AES-128 ini menjelaskan tentang melakukan alur dari pendekripsian file yang sudah terenkripsi untuk dikembalikan seperti semua.



Gambar 5. Flowchart Dekripsi AES-128

3.3 Algoritme Proses Enkripsi & Dekripsi AES-128

Algoritme ini menjelaskan bagaimana tentang alur proses enkripsi dan dekripsi AES-128 yang terjadi waktu pengenkripsian dan pendekripsian pada sistem aplikasi yang dibangun.

Algoritme 1. Algoritme Proses Enkripsi AES-128

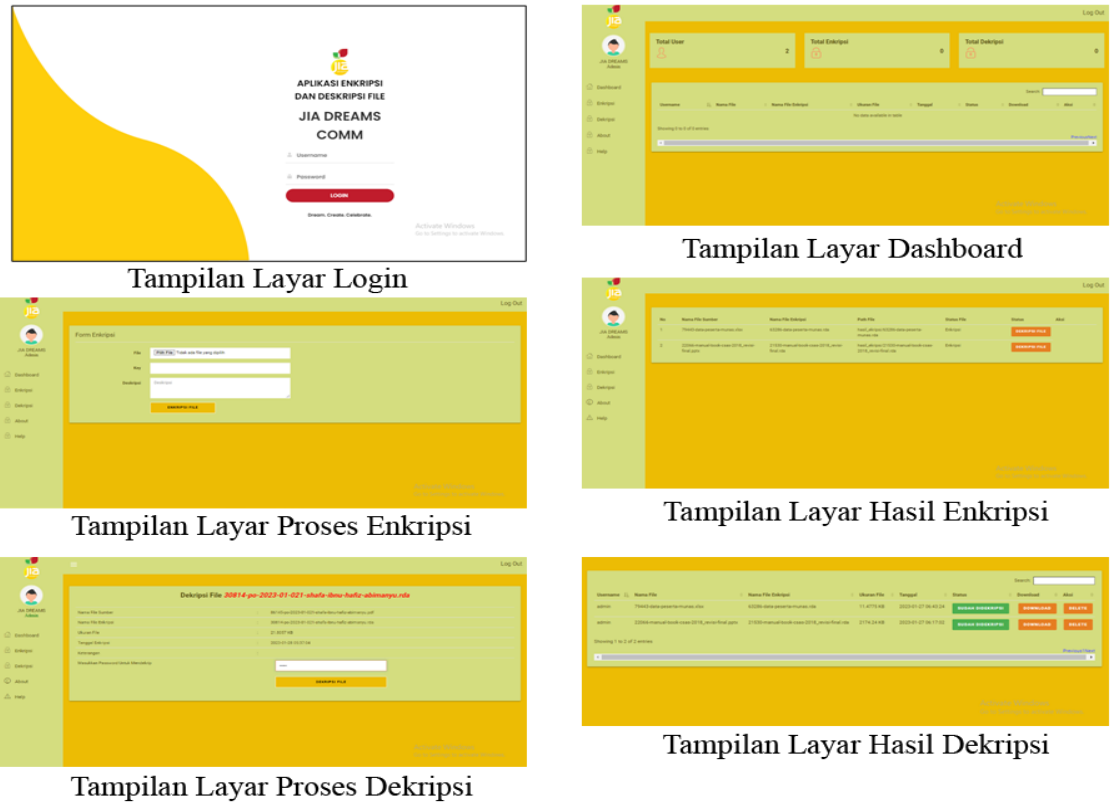
1	Start
2	Input plaintext
3	i=1
4	add round key (0)
5	sub bytes
6	shift rows
7	mix column
8	if<=9
9	i++
10	kembali ke baris 5
11	end if

Algoritme 2. Algoritme Proses Dekripsi AES-128

```
1   Start
2       Input chipertext
3       add round key (9)
4       inverse shift rows
5       inverse sub bytes
6       i=1
7       add round key (8)
8       inverse mix column
9       inverse shift rows
10      inverse sub bytes
11  if<=9 then
12      i++
13      kembali ke baris 7
14  end if
15      add round key (0)
16      output plaintext
17  end
```

3.4 Tampilan Layar

Berikut ini adalah tampilan layar dari sistem aplikasi yang telah dibuat, implementasi sistem aplikasi ini bertujuan untuk melakukan uji coba sistem aplikasi yang telah dirancang apakah sudah sesuai dengan rancangan yang telah dibuat.



Gambar 6. Tampilan Layar

3.5 Hasil Pengujian

Pada tahap pengujian terhadap sistem aplikasi dengan perencanaan alat uji yang telah direncanakan pada tahap sebelumnya. Tahap pertama pada pengujian ini adalah menguji fungsi sistem aplikasi sekaligus tampilan dari setiap pengujian menggunakan *black box testing*. Tabel dibawah merupakan proses dari pengujian aplikasi.

Tabel 3. Tahapan Uji Hasil Enkripsi

No	Nama File	Ukuran File	Nama File Hasil Enkripsi	Ukuran File Setelah Enkripsi	Keterangan dan Durasi Enkripsi
1	Data Peserta Munas.xlsx	12 KB	93887-data-peserta-munas.rda	12 KB	Berhasil 0.2 detik
2	MOM LOREAL CSR 2018.docx	34 KB	48105-mom-loreal-csr-2018.rda	34 KB	Berhasil 0.57 detik
3	FWIS BFBL 2018 Brief EO Pitching.pdf	1,181 KB	18445-fwis-bfbl-brief-2018-eo-pitching.rda	1,181KB	Berhasil 23.31 detik
4	Final Fix Compro Split 1-1.png	256KB	69757-final-fix-compro-split-1-1.rda	256KB	Berhasil 4.51 detik
5	SalesMissionAustrali.pptx	2,692 KB	54383-salesmissionaustrali.rda	2,692 KB	Berhasil 50.55 detik
6	JFW 2019 by JIA Comm 08082018.pptx	9,829 KB	63707-jfw-2019-by-jia-comm-08082018.rda	9,829 KB	Berhasil 194.56 detik
7	DATA BPJS KESEHATAN KARYAWAN JIA	15 KB	86467-data-bpjs-kesehatan-karyawan-jia.rda	15KB	Berhasil 0.24 detik
8	Iwan Fals – Kota (official-audio).mp3	2,984 KB	99843-iwan-fals---kota-(official-audio).rda	2,984 KB	Berhasil 54.72 detik

Tabel 4. Tahapan Uji Hasil Dekripsi

No	Nama File Enkripsi	Ukuran File Enkripsi	Nama File Hasil Dekripsi	Ukuran File Dekripsi	Keterangan dan Durasi Enkripsi
1	9388747839-data-peserta-munas.rda	12 KB	93887-data-peserta-munas.xlsx	12 KB	Berhasil 0.22 detik
2	4810570369-mom-loreal-csr-2018.rda	34 KB	48105-mom-loreal-csr-2018.docx	34 KB	Berhasil 0.62 detik
3	71307-fwis-bfbl-brief-2018-eo-pitching.rda	1,181 KB	18445-fwis-bfbl-brief-2018-eo-pitching.pdf	1,181 KB	Berhasil 20.8 detik
4	69757-final-fix-compro-split-1-1.rda	256 KB	15488-final-fix-compro-split-1-1.png	256 KB	Berhasil 4.76 detik
5	44779-salesmissionaustrali.rda	2,692 KB	54383-salesmissionaustrali.pptx	2,692 KB	Berhasil 45.99 detik
6	63707-jfw-2019-by-jia-comm-08082018.rda	9,829 KB	62748-jfw-2019-by-jia-comm-08082018.pptx	9,829 KB	Berhasil 198.95 detik
7	87523-data-bpjs-kesehatan-karyawan-jia.rda	15 KB	86467-data-bpjs-kesehatan-karyawan-jia.xlsx	15 KB	Berhasil 0.27 detik
8	99843-iwan-fals---kota-(official-audio).rda	2,984 KB	73743-iwan-fals---kota-(official-audio).mp3	2,984 KB	Berhasil 52.93 detik

4. KESIMPULAN

Berdasarkan hasil evaluasi dari penelitian yang berjudul "Implementasi Kriptografi Menggunakan Algoritme *Advanced Encryption Standar* (Aes-128) Untuk Mengamankan File Dokumen Pada Pt. Jia Dreams Communications Berbasis Web", kesimpulan dari penelitian ini adalah algoritme *Advanced Encryption Standard* (AES-128) dapat di terapkan pada aplikasi pengamanan file di PT. JIA DREAMS COMMUNICATIONS, pada proses pengujian terhadap beberapa data file yang berukuran kurang dari 5MB durasi enkripsi dan dekripsi lebih cepat, dan ukuran file asli tidak berubah setelah dienkripsi ataupun dekripsi.

DAFTAR PUSTAKA

[1] Azhari, M., Mulyana, D. I., Perwitosari, F. J., & Ali, F. (2022). Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). *Jurnal Pendidikan Sains Dan Komputer*, *2*(01), 163–171. https://doi.org/10.47709/jpsk.v2i01.1390.

[2] Chandra, R. V. H., Kusyanti, A., & Data, M. (2019). Analisis Performa Proses Enkripsi dan Dekripsi Menggunakan Algoritme AES-128 Pada Berbagai Format File. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *3*(1), 481–486. http://j-ptiik.ub.ac.id.

[3] Dian Widyawan, I. (2021). *Pengamanan File Menggunakan Kriptografi Dengan Metode Aes-128 Berbasis Web Di Komite*. *4*(1), 15–22.

[4] Eka Putri, A., Kartikadewi, A., & Abdul Rosyid, L. A. (2021). Implementasi Kriptografi dengan Algoritma Advanced Encryption Standard (AES) 128 Bit dan Steganografi menggunakan Metode End of File (EOF) Berbasis Java Desktop pada Dinas Pendidikan Kabupaten Tangerang. *Applied Information System and Management (AISM)*, *3*(2), 69–78. https://doi.org/10.15408/aism.v3i2.14722.

[5] Hanadwiputra, S. (2018) Implementasi Enkripsi Dalam Pengamanan File Data Karyawan Dengan Metode Algoritma Des (Data Encryption Standard) Pada Cv. Sinergi Informasi Global. Jurnal "Gema Kampus", 13(02), Pp. 61-69.

[6] Hulu, D., Nadeak, B., & Aripin, S. (2020). Implementasi Algoritma AES (Advanced Encryption Standard) Untuk Keamanan File Hasil Radiologi di RSU Imelda Medan. *KOMIK (Konferensi ...*, *4*, 78–86. https://doi.org/10.30865/komik.v4i1.2590.

[7] Ignasius, A., & Shaka Yudha Sakti, D. V. (2022). Penerapan Algoritma Aes (Advance Encryption Standart) 128 Untuk Enkripsi Dokumen Di Pt. Gunung Geulis Elok Abadi. *Skanika*, *5*(1), 1–10. https://doi.org/10.36080/skanika.v5i1.2118

[8] Mulyadi, A. Y., Nugroho, E. P., & P, R. R. J. (2018). Implementasi Algoritma AES 128 dan SHA – 256 Dalam Pengkodean pada Sebagian Frame Video CCTV MPEG-2. *JATIKOM: Jurnal Teori Dan Aplikasi Ilmu Komputer*, *1*(1), 33–39.

[9] Nurnaningsih, D., & Permana, A. A. (2018). Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (AES). *Jurnal Teknik Informatika*, *11*(2). https://doi.org/10.15408/jti.v11i2.7811.

[10] Sari, M., Purnomo, H. D., & Sembiring, I. (2022). Review : Algoritma Kriptografi Sistem Keamanan SMS di Android. *Journal of Information Technology*, *2*(1), 11–15. https://doi.org/10.46229/jifotech.v2i1.292.

[11] Widodo, B. E., & Purnomo, A. S. (2020). Implementasi Advanced Encryption Standard Pada Enkripsi Dan Dekripsi Dokumen Rahasia Ditintelkam Polda Diy. *Jurnal Teknik Informatika (Jutif)*, *1*(2), 69–77. https://doi.org/10.20884/1.jutif.2020.1.2.21.