3rd Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
30 Agustus 2023 – Jakarta, Indonesia
Volume 2, Nomor 2, September 2023 - ISSN 2962-8628 (*online*)

IMPLEMENTASI ALGORITMA KRIPTOGRAFI ADVANCE ENCRYPTION STANDARD DENGAN COUNTER MODE UNTUK MENGAMANKAN DATA KEUANGAN PADA RC CAFE

Muchammad Agung Saputra, Pipin Farida Ariyani

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

Email: [1*]saputra1526@gmail.com, [2]pipin.faridaariyani@budiluhur.ac.id
(* : corresponding author)

Abstrak- Dalam industri jasa makanan, RC Cafe adalah usaha mikro, kecil, atau menengah (UMKM) yang membantu banyak *food court* yang bekerja sama untuk menjual produk mereka. Karena RC Cafe menggunakan mesin kasir terpusat dan membagi pendapatan mereka di antara staf, dan yang lainnya terutama pemilik *food court*. Bisnis ini harus menjamin keamanan dan keandalan semua transaksi keuangan dan informasi rekan kerja mereka. Tujuan dari penelitian ini adalah untuk menggunakan teknologi yang mencegah kejahatan dunia maya, yang biasa dikenal pencurian, peretasan, dan eksploitasi informasi keuangan yang sifatnya sensitif, terjadi pada pemilik RC Cafe. Berbagai metode ataupun algoritme telah banyak digunakan, untuk kali ini penulis menggunakan teknik kriptografi dengan algoritme *Advanced Encryption Standard-Counter* (AES-CTR). Sudah banyak dikenal algoritme AES ini tapi masih sedikit yang membahas ataupun menggunakan mode mode yang ada pada AES ini. Dari 5 mode yang ada pada AES ini penulis memilih menggunakan mode *counter* karena bentuk enkripsinya yang unik, berlapis, dan juga sangat terjamin keamanannya. Dan hasil pengujian dari file yang rata-rata memiliki ukuran 363,363.8*byte* dapat di enkripsi dengan memakan waktu 0,00136747143 milidetik, sedangkan untuk proses dekripsinya dari file yang mempunyai ukuran rata-rata 363,371.2*byte* setelah di enkripsi hanya memakan waktu 7,4312e-5 milidetik untuk kembali ke file aslinya atau proses dekripsi.

Kata Kunci: Keamanan,Keamanan data,cybercrime,AES-CTR,*advance encryption standard, counter mode*

IMPLEMENTATIONS OF ADVANCED ENCRYPTION STANDARD CRYPTOGRAPHY ALGORITHM WITH COUNTER MODE TO SECURE FINANCIAL DATA AT RC CAFE

Abstract- *In the food service industry, RC Cafe is a micro, small, or medium enterprise (MSMEs) that helps many food courts work together to sell their products. Because RC Cafe uses a centralized cash register and divides their revenue among the staff, and others especially the food court owner. These businesses must guarantee the security and reliability of all financial transactions and the information of their colleagues. The aim of this research is to use technology to prevent cybercrimes, commonly known as theft, hacking, and exploitation of sensitive financial information, from happening to RC Cafe owners. Various methods or algorithms have been widely used, this time the author uses cryptographic techniques with the Advanced Encryption Standard-Counter (AES-CTR) algorithm. The AES algorithm is well known, but only a few discuss or use the AES modes. Of the 5 modes in AES, the author chooses to use counter mode because of its unique, layered form of encryption, and also very secure security. And the test results of files with an average size of 363,363.8 bytes can be encrypted in 0.00136747143 milliseconds, while the decryption process for files with an average size of 363,371.2 bytes after encryption only takes 7.4312e-5 milliseconds to return to the original file or the decryption process..*

Keywords*: Security, Data Security, cybercrime, AES-CTR, advanced encryption standard, counter mode*

1. PENDAHULUAN

RC Cafe merupakan UMKM dibidang kuliner yang memfasilitasi beberapa *tenant/foodcourt* untuk bekerja sama dengan mereka untuk berjualan di tempat mereka. Dengan sistem satu pintu atau satu kasir dan sistem bagi hasil, tentu sang pemilik RC Cafe tersebut harus memastikan data penjualan dan pembagian hasil kepada rekan kerja mereka benar-benar transparan dan aman. Tujuan dari penelitian ini adalah untuk menerapkan teknologi mengamankan data keuangan dari RC Cafe, oleh karena itu diperlukan mekanisme pengamanan data dengan mengenkripsi serta mendeskripsi data yang biasa dikenal dengan kriptografi[1].

Tujuan kriptografi adalah untuk memastikan kerahasiaan komunikasi dengan menyandikannya dengan cara yang hanya dapat diuraikan oleh penerima yang dimaksud. Enkripsi dan dekripsi adalah dua langkah utama dalam bidang kriptografi. Secara khusus enkripsi melibatkan pengubahan dokumen menjadi komunikasi yang tidak dapat dipahami (*ciphertext*)[2], proses deskripsi melibatkan pengubahan *ciphertext* menjadi dapat dibaca (*plaintext*)[3]. Berdasarkan uraian tersebut, untuk mencegah penyalahgunaan data oleh pihak yang tidak bertanggung jawab, RC Cafe harus mengintegrasikan keamanan kriptografi untuk meningkatkan keamanan data. Oleh karena itu, algoritma *AES* (*Advanced Encryption Standard*)[4] dengan mode *CTR* (*Counter*)[5] dipilih untuk penelitian kali ini. *Advanced Encryption Standard* (*AES*)[6] adalah algoritma enkripsi populer yang digunakan dalam implementasi kunci simetris. Ini adalah turunan dari *DES* (*Data Encryption Standard*)[7].

2. METODE PENELITIAN

2.1 Data Penelitian

Data yang akan digunakan dalam penelitian ini (Tabel 1) adalah data keuangan dan beberapa file yang dimana data berupa dokumen RC Cafe. Tanpa perantara, peneliti mendapatkan data langsung dari sumbernya. Data yang didapatkan sebagai proses uji coba pengamanan *file* menggunakan Teknik metode *Advanced Encryption Standar*[8]–*Counter*[9] (AES-CTR)[10].

Tabel 1. Data Penelitian

Nama File	Jenis File	Ukuran File
Laporan Keuangan Mei 2023	.xlsx	100kb
Laporan Keuangan Koperasi Mei 2023	.xlsx	96kb
Contoh Tenant	.jpg	301kb
Flyer Foodcourt	.pdf	2,668kb
Laporan Keuangan Koperasi April 2023	.xlsx	84kb
Laporan Keuangan April 2023	.xlsx	86kb
Laporan Keuangan Perusahaan Dagang	.xlsx	11kb
Laporan Keuangan Perusahaan Manufaktur	.xlsx	90kb
Logo	.png	109kb
Skema Detail Database	.docx	10kb

2.2 Rancangan Pengujian

Saat ingin menggunakan aplikasi ini, pengguna akan diminta untuk masuk menggunakan nama pengguna dan kata sandi saat pertama kali meluncurkan program. Saat masuk, pengguna dikirim langsung ke beranda tempat menu dapat diakses. Halaman beranda juga dilengkapi menu *logout* yang ketika diaktifkan, langsug mengarahkan pengguna kembali ke halaman *login*, serta tombol tambah data di halaman beranda yang dapat digunakan untuk menggunggah file atau data yang akan dienkripsi atau di dekripsi.

Tabel 2. Rancangan Pengujian

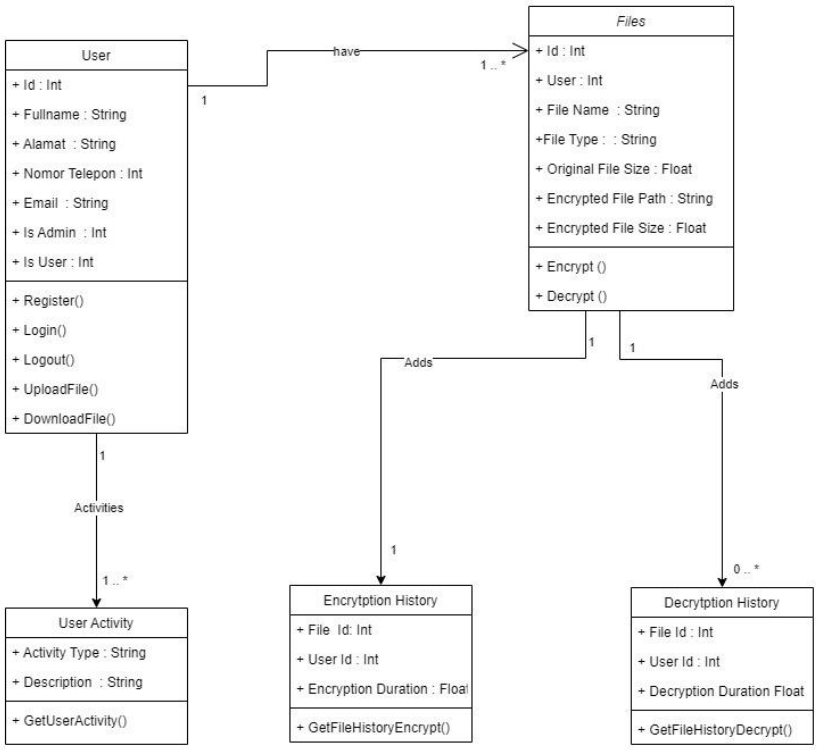
No	Kasus Uji	Hasil yang Di Harapkan
1	Tombol Masuk	Tampil halaman menu utama
2	Tombol Choose File	Dapat memilih file yang ingin di enkripsi
3	Tombol Enkripsi file	Dapat mengakses file yang ingin di enkripsi
4	Tombol Dekripsi dan Download	Dapat mendekripsi lalu mengunduh hasil enkripsi
5	Tombol Hapus	Dapat menghapus file yang telah di enkripsi dan dekripsi
6	Tombol Logout	Kembali ke halaman Login

2.3 Rancangan Basis Data

Dalam hal ini dibahas mengenai *Class Diagram*, dan Spesifikasi Basis Data.

2.3.1 Class Diagram

Class Diagram pada Gambar 1 menghubungkan struktur dan hubungan antar objek yang ada di dalam aplikasi.



Gambar 1. Class Diagram

2.3.2 Spesifikasi Basis Data

Dalam spesifikasi ini terdapat basis data, berikut adalah struktur basis data yang akan digunakan. Tabel 3, Tabel 4, Tabel 5, dan Tabel 6 akan menyimpan *record* yang telah dimanipulasi oleh program sesuai dengan spesifikasinya masing masing.

1. Nama Database : db_kripto
   Nama Tabel : *account_user*
   Media : Harddisk
   Primary Key : Id

Tabel 3. Spesifikasi Tabel Account User

Field	Type	Panjang	Keterangan
id	Int (pk)	4	Unique identifier
email	varchar	50	Email user
password	varchar	255	Password hash sha256
name	varchar	50	Nama user
is_user	boolean	1	Is user
is_active	boolean	1	Aktif atau tidak user
last_login	datetime	5	Terakhir login
date_joined	datetime	5	Tanggal Join

2. Nama Database : db_kripto
   Nama Tabel : *account_user_activity_log*
   Media : Harddisk

Primary Key : Id

Tabel 4. Spesifikasi Tabel Account User Activity Log

Field	Type	Panjang	Keterangan
Id	Int (pk)	5	Unique identifier
Activity	varchar	255	Aktivitas yang dilakukan
user_id	Int (fk)	4	User yang melakukan
created_at	datetime	5	Tanggal Melakukan

3. Nama Database : db_kripto
   Nama Tabel : *file_files*
   Media : Harddisk
   Primary Key : Id

Tabel 5. Spesifikasi Tabel File Files

Field	Type	Panjang	Keterangan
Id	Int (pk)	5	Unique identifier
file_name	varchar	255	Nama original file
file_type	varchar	50	Type dari file
original_size	int	4	Ukuran file original
encrypted_size	int	4	Ukuran file enkripsi
user_id	Int (fk)	5	User yang melakukan enkripsi
file_upload	varchar	100	Path file di simpan
Nonce	byte	16	Nonce (16 character) unique per file
encryption_time	float	8	Waktu enkripsi
key_size	int	3	Panjang Kunci yang dipakai
created_at	datetime	5	Waktu Upload
deleted_at	datetime	5	Waktu Download

4. Nama Database : db_kripto
   Nama Tabel : *file_activity_log*
   Media : Harddisk
   Primary Key : Id

Tabel 6. Spesifikasi Tabel File Activity Log

Field	Type	Panjang	Keterangan
Id	Int (pk)	5	Unique identifier
file_id	Int (fk)	5	File yang di tuju
user_id	Int (fk)	4	User yang melakukan
Activity	Varchar	255	Aktivitas yang dilakukan
created_at	Datetime	5	Tanggal Melakukan

3. HASIL DAN PEMBAHASAN

3.1 Lingkungan Percobaan

Penyiapan eksperimental dalam penelitian ini menggunakan alat penelitian dan desain untuk membuat antarmuka aplikasi, termasuk perangkat keras dan perangkat lunak. Ruang percobaan penelitian ini akan memiliki dimensi sebagai berikut:

3.1.1 Spesifikasi Perangkat Keras (Hardware)

Perangkat keras (*hardware*) yang akan digunakan untuk mendukung jalannya suatu sistem aplikasi ini secara maksimal yaitu sebagai berikut:

1. *Processor Intel Core i*5-4200U CPU@ 1.60GHz (4 CPUs), ~2,3GHz
2. RAM 4GB
3. HDD 1TB

3.1.2 Spesifikasi Perangkat Lunak (Software)

Perangkat lunak (*software*) yang akan digunakan untuk mendukung jalannya suatu sistem aplikasi ini secara maksimal adalah sebagai berikut:

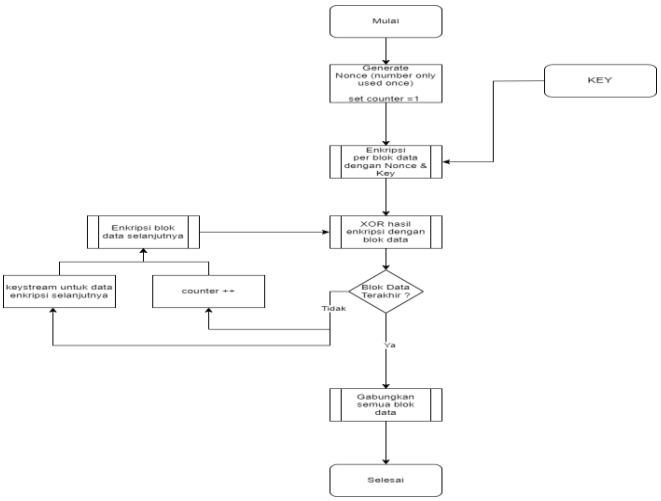
1. Sistem Operasi *Windows* 11
2. Visual Studio Code
3. Python 3.9
4. Django 4.1.7
5. PostgreSQL 11

3.2 Flowchart

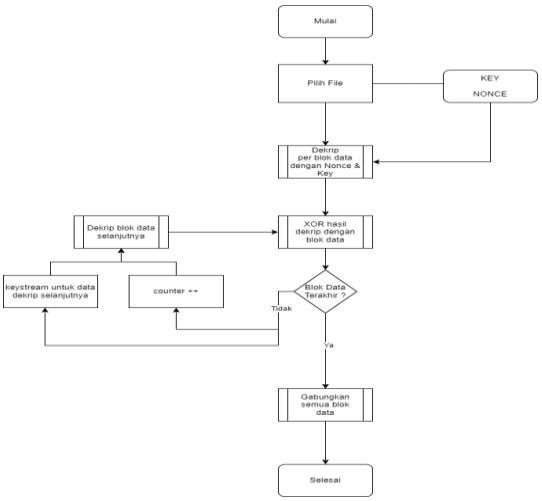
Flowchart ,sering dikenal sebagai diagram alir, adalah diagram yang digunakan untuk mengilustrasikan tahapan, proses, dan pilihan suatu proses. Setiap langkah ditampilkan sebagai diagram, dan hubungan diantara langkah-langkah tersebut ditunjukkan dengan garis atau panah.

3.2.1 *Flowchart* Algoritma Enkripsi dan Dekripsi AES-CRT

Flowchart pada gambar 4 adalah penjelasan tentang bagaimana proses enkripsi dengan metode AES-CRT ini berjalan di dalam aplikasi ini. *Flowchart* pada gambar 5 adalah penjelasan tentang bagaimana proses dekripsi dengan metode AES-CRT ini berjalan di dalam aplikasi ini.



Gambar 4. *Flowchart* Algoritma Enkripsi AES-CRT



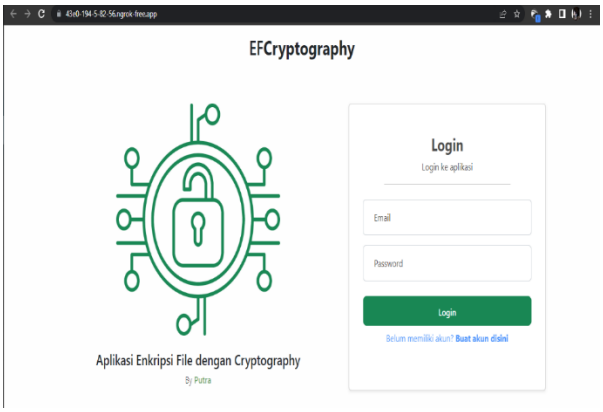
Gambar 5. *Flowchart* Algoritma Dekripsi AES-CRT

3.3 Implementasi *Advanced Encryption Standard* Mode *Counter* (AES-CTR)

Berikut adalah hasil implementasi algoritma *Advanced Encryption Standard* dengan mode *Counter* dalam bentuk aplikasi berbasis web.

3.3.1 Tampilan Layar Login

Gambar 6 merupakan tampilan awal layar pada aplikasi ini yaitu menu *login*. Gambar 7 merupakan tampilan layar registrasi untuk *user* yang belum memiliki akun *login*.

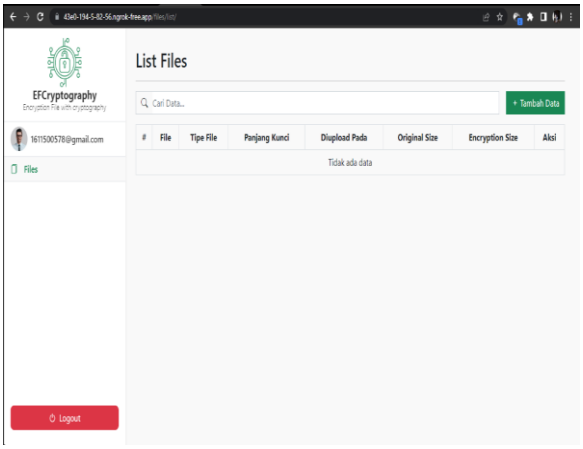


Gambar 6. Tampilan Layar Login

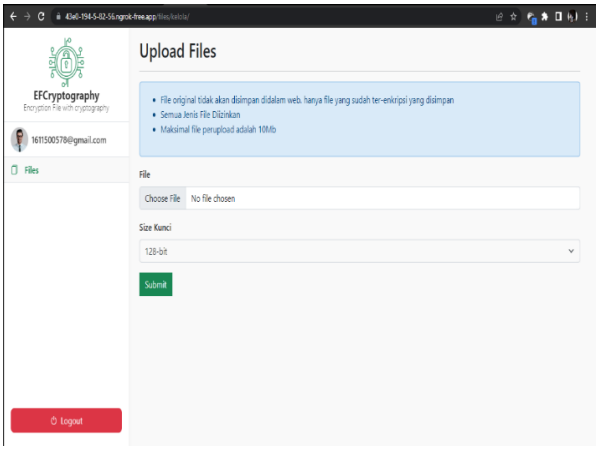
Gambar 7. Tampilan Layar Registrasi

3.3.2 Tampilan Layar Menu

Gambar 8 adalah tampilan awal yang muncul setelah *login* yang berupa tampilan beranda. Gambar 9 adalah tampilan dimana pengguna menggunakan tombol tambah data pada halaman utama, yang berupa tampilan untuk mengunggah file yang akan di enkripsi berikut dengan memilih ukuran kunci yang akan digunakan untuk mengenkripsi data tersebut



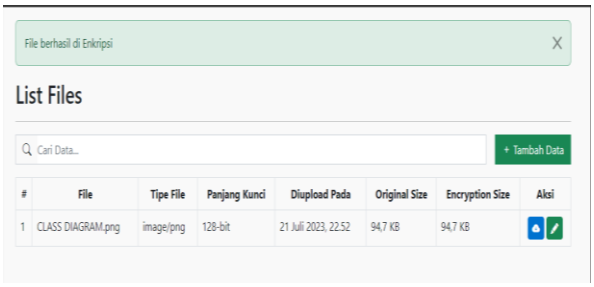
Gambar 8. Tampilan Layar Dashboard



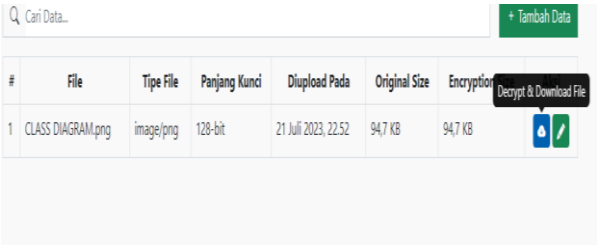
Gambar 9. Tampilan Layar Menu Tambah Data

3.3.3 Tampilan Layar Menu Enkripsi dan Dekripsi File

Pada gambar 10 muncul tampilan *message box* di menu utama setelah mengunggah file yang akan dienkripsi yang berupa berhasil atau tidaknya proses enkripsi tersebut, bila berhasil akan muncul deskripsi data tersebut di menu utama yang berupa ukuran maupun waktu yang digunakan saat proses enkripsi tersebut. Gambar 11 merupakan tombol *decrypte & download file* bila pengguna ingin mengembalikan file yang telah dienkripsi, file akan terotomatis diunduh di perangkat tanpa perlu melakukan aksi tambahan.



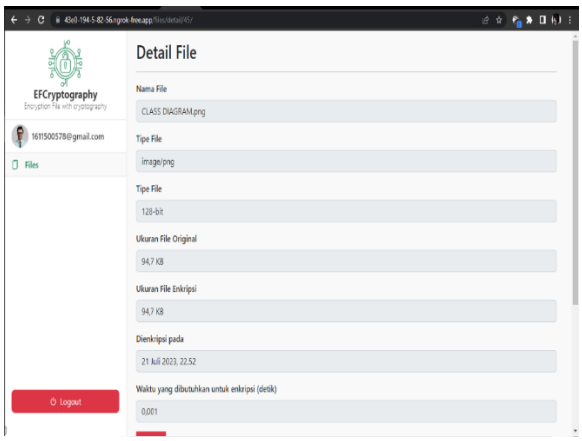
Gambar 10. Tampilan Layar Menu Enkripsi File



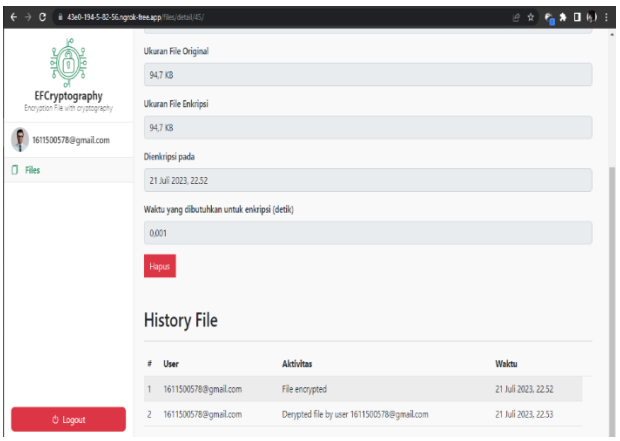
Gambar 11. Tampilan Layar Menu Dekripsi File

3.3.4 Tampilan Layar Menu *Detail File*

Gambar 12 menampilkan deskripsi file atau data yang telah dienkripsi, berisikan jenis file, pilihan kunci yang digunakan, ukuran file, ukuran file yang telah di enkripsi, serta waktu yang dibutuhkan untuk melakukan sebuah proses enkripsi. Untuk gambar 13 masih di menu yang sama namun terdapat tombol hapus untuk menghapus file yang dituju, dan juga ada *history file* yang terdapat *record* pengguna yang mana yang melakukan aktifitas di aplikasi ini serta waktu yang digunakan pada saat pengembalian file atau dekripsi.



Gambar 12. Tampilan Menu Detail



Gambar 13. Tampilan Menu Hapus

3.4 Hasil Pengujian

Hasil pengujian menunjukkan bahwa program berfungsi sebagaimana mestinya. Telah ditentukan melalui pengujian bahwa ukuran file data berpengaruh pada jumlah waktu yang diperlukan untuk mengenkripsi dan mendekode file tersebut. Waktu yang dibutuhkan untuk mengenkripsi dan mendekripsi file meningkat secara proporsional dengan ukurannya sesuai dengan hasil pengujian pada tabel 7 dan tabel 8. Dan juga untuk pengujian programnya sesuai dengan yang diharapkan sesuai dengan yang tertera hasil pada tabel 9.

Tabel 7. Hasil Pengujian Enkripsi File

No	Nama Asli File	Ukuran Asli File (byte)	Ukuran file setelah di enkripsi (byte)	Waktu (milidetik)	Kinerja Enkripsi (byte per milidetik)
1.	Laporan Keuangan Mei 2023.xlsx	97,577byte	97,584byte	0.0000050759	187.742.632
2.	Laporan Keuangan Koperasi Mei 2023.xlsx	101,466byte	101,472byte	0,00000100255	98.841.691
3.	Contoh Tenant.jpg	307,987byte	308,000byte	0,00000052023	578.170.486
4.	Flyer Foodcourt .pdf	2,731,631byte	2,731,632byte	0.00136214375	1.958.390
5.	Laporan Keuangan Koperasi April 2023 .xlsx	85,302byte	85,312byte	0,00000099897	83.398.079
6	Laporan Keuangan April 2023 .xlsx	87,676byte	87,680byte	0,00000100160	85.488.522
7.	Laporan Keuangan Perusahaan Dagang .xlsx	10,479byte	10,480byte	0,00000099969	10.237.558
8.	Laporan Keuangan Perusahaan Manufaktur .xlsx	91,431byte	91,440byte	0,00000099993	89.303.348
9.	Logo .png	110,736byte	110,752byte	0,00000100017	108.138.306
10.	Skema Detail Database .docx	9,353byte	9,360byte	0,00000099826	9.156.570
Rata-rata :		**363,363.8byte**	**363,371.2byte**	**0,00136747143ms**	**1,08344021e9byte/ms**

Tabel 8. Hasil Pengujian Dekripsi File

No	Nama File	Ukuran File (byte)	Ukuran file setelah di dekripsi (byte)	Waktu (milidetik)
1.	Laporan Keuangan Mei 2023 .xslx	97,584byte	97,577byte	0.00002077
2.	Laporan Keuangan Koperasi Mei 2023 .xlsx	101,472byte	101,466byte	0.00001199
3.	Contoh Tenant .pdf	308,000byte	307,987byte	0.00001151
4.	Flyer FoodCourt .png	2,731,632byte	2,731,631byte	0.00002498
5.	Laporan Keuangan Koperasi April 2023 .xlsx	85,312byte	85,302byte	0.00000100
6.	Laporan Keuangan April 2023 .xlsx	87,680byte	87,676byte	0.00000101
7.	Laporan Keuangan Perusahaan Dagang .xlsx	10,480byte	10,479byte	0.00000100
8.	Laporan Keuangan Perusahaan Manufaktur .xlsx	91,440byte	91,431byte	0.00000100
9.	Logo .png	110,752byte	110,736byte	0.00000102
10.	Skema Detail Database .docx	9,360byte	9,353byte	0.00000102
Rata-rata :		**363,371.2byte**	**363,363.8byte**	**7,4312e-5ms**

Tabel 9. Pengujian Program

No	Skenario Pengujian	Hasil yang diharapkan	Hasil Pengujian
1.	User mengisi form login	Tampil halaman menu Dashboard	Sesuai Harapan
2.	User memilih menu berkas Enkripsi	Tampil halaman menu Enkripsi	Sesuai Harapan
3.	User memilih menu Dekripsi	Tampil halaman menu Dekripsi	Sesuai Harapan
4.	Memasukan file dan mengkilk tombol enkripsi dan dekripsi	Tampil halaman proses enkripsi atau dekripsi	Sesuai Harapan
5.	Mengunduh file yang sudah terdekripsi	Berhasil otomatis mengunduh file	Sesuai Harapan
6.	User memilih menu informasi daftar berkas	Tampil halaman daftar berkas yang sudah terenkripsi dan di dekripsi dan tampil halaman Hapus berkas	Sesuai Harapan
7.	User mengklik Hapus	Tampil alert box untuk meyakinkan user menghapus file dan muncul message box bisa berhasil	Sesuai Harapan
8.	User memilih tombol Logout	Tampil kembali ke halaman Login	Sesuai Harapan
9.	Proses Enkripsi	Rata-rata memakan waktu 0,00136747143 milidetik	Sesuai Harapan
10.	Proses Dekripsi	Rata-rata memakan waktu 7,4312e-5 milidetik	Sesuai Harapan

4. KESIMPULAN

Aplikasi berbasis web di RC Cafe ini menerapkan teknik kriptografi AES-CTR dengan benar, seperti yang ditentukan oleh hasilnya. Waktu yang diperlukan untuk mengenkripsi atau mendekripsi file berbanding lurus dengan ukuran file, bahkan lebih cepat dibanding mode lain ataupun tanpa mode. Selain itu semua jenis file yang diketahui telah berhasil diuji dengan program ini, oleh karena itu, tidak hanya melindungi catatan keuangan RC Cafe, tetapi juga informasi lain yang sama pentingnya, dan untuk hasil pengujian dari file yang rata-rata memiliki ukuran 363,363.8 *byte* dapat di enkripsi dengan memakan waktu 0,00136747143 milidetik, sedangkan untuk proses dekripsinya dari file yang mempunyai ukuran rata-rata 363,371.2 *byte* setelah di enkripsi hanya memakan waktu 7,4312e-5 milidetik untuk kembali ke file aslinya atau proses dekripsi. Dilihat dari data tersebut bahwa proses enkripsi AES dengan mode *counter* ini sangat cepat dan efisien dibanding menggunakan algortima kriptografi yang lain.

DAFTAR PUSTAKA

[1] H. Irsyad, A. Taqwiym, and N. Wijaya, "Implementasi Algoritma Rivest Code 4 (Rc4) Untuk Penyandian Sms Pada Telepon Selular," *Kurawal - J. Teknol. Inf. dan Ind.*, vol. 5, no. 1, pp. 16–30, 2022.

[2] W. K. Lee, H. J. Seo, S. C. Seo, and S. O. Hwang, "Efficient Implementation of AES-CTR and AES-ECB on GPUs With Applications for High-Speed FrodoKEM and Exhaustive Key Search," *IEEE Trans. Circuits Syst. II Express Briefs*, vol. 69, no. 6, 2022.

[3] S. Setti, I. Gunawan, B. E. Damanik, S. Sumarno, and I. O. Kirana, "Implementasi Algoritma Advanced Encryption Standard dalam Pengamanan Data Penjualan Ramayana Department Store," *JURIKOM*

(Jurnal Ris. Komputer), vol. 7, no. 1, p. 182, 2020.

[4] S. J. H. Pirzada, A. Murtaza, T. Xu, and L. Jianwei, "Initialization Vector Generation for AES-CTR Algorithm to Increase Cipher-text Randomness," in *2019 2nd International Conference on Information Systems and Computer Aided Education, ICISCAE 2019*, 2019.

[5] Y. Kim and S. C. Seo, "Efficient Implementation of AES and CTR_DRBG on 8-Bit AVR-Based Sensor Nodes," *IEEE Access*, vol. 9, 2021.

[6] K. E. Y. Sha-, "Enkripsi File Dalam Zip Dengan Aes Ctr Menggunakan Derivation Key Sha-256," no. January 2020, 2019.

[7] U. P. Indonesia, T. Informatika, and I. Email, "PENGAMANAN DATA AKTA DENGAN METODE AES BERBASIS CLOUD COMPUTING Kahfi Fadhlil Khaliq," *J. Teknol. Dan Ilmu Komput. …*, vol. 4, no. April, pp. 2019–2022, 2021.

[8] K. Kim, S. Choi, H. Kwon, H. Kim, Z. Liu, and H. Seo, "PAGE-Practical AES-GCM encryption for low-end microcontrollers," *Appl. Sci.*, vol. 10, no. 9, 2020.

[9] R. Saidi, T. Bentahar, N. Cherrid, A. Bentahar, and H. Mayache, "Evaluation and analysis of interferograms from an insar radar encrypted by an AES-based cryptosystem with the five encryption modes," *Int. J. Electr. Eng. Informatics*, vol. 12, no. 4, 2020.

[10] K. Kim, S. Choi, H. Kwon, Z. Liu, and H. Seo, "FACE–LIGHT: Fast AES–CTR Mode Encryption for Low-End Microcontrollers," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2020, vol. 11975 LNCS.