Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
Jakarta – Indonesia, 06 September 2022

PENERAPAN ALGORITMA AES-128 UNTUK ENKRIPSI DOKUMEN DI PT CAVEO BIOMETRIC SECURITY

Raudatul Firdaus[1*], Reva Ragam Santika[2]

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

Email: [1*]raudatulfirdaus@outlook.com, [2]reva.ragam@budiluhur.ac.id
(* : corresponding author)

Abstrak-Perkembangan teknologi sangatlah berpengaruh terhadap keamanan data pada sebuah perusahaan untuk mencegah orang-orang yang tidak berwenang melihat dokumen tersebut. PT Caveo Biometric Security merupakan perusahaan yang salah satu produk yang dijual adalah pembuatan *Software*. Permasalahan mengamankan sebuah data pada sebuah aplikasi merupakan tanggung jawab penyedia *software*. Maka dari itu PT Caveo Biometric Security terus mengembangkan diri untuk menjaga kerahasiaan dan keamanan data dari setiap kliennya. Penelitian ini bertujuan melakukan pengujian untuk proses pengaman data yang dilakukan dengan menggunakan Algoritma Kriptografi yang mengadopsi sistem enkripsi dekripsi serta menggunakan metode *Advanced Encryption Standard* (AES-128). Algoritma ini sangat aman untuk mengamankan dokumen yang akan dimasukan kedalam aplikasi, sehingga aplikasi ini dapat menjaga dan mengamankan data data tersebut. Metode *Advanced Encryption Standard* (AES-128) dipilih karena algoritma ini sangat aman dalam melindungi data karena memiliki Teknik enkripsi dekripsi panjang kunci 128-bit, sehingga kecil kemungkinan untuk seseorang membobol dokumen ini walaupun sudah menggunakan kompuer yang cepat. Metode pengujian penelitian ini menggunakan metode *black box*, yang mana metode ini dipilih karena metode ini menggunakan struktur kontrol yang dirancang secara prosedural untuk melakukan pengujian dan melihat ke dalam perangkat lunak. Dari hasil pengujian dapat kami simpulkan bahwa aplikasi ini berhasil melakukan enkripsi terhadap dokumen – dokumen yang dimasukan kedalam aplikasi dan tidak dapat diakses secara langsung

Kata Kunci: Aes 128, Enkripsi, Dekripsi

APPLICATION OF AES-128 ALGORITHM FOR DOCUMENT ENCRYPTION AT PT CAVEO BIOMETRIC SECURITY

Abstract-*Technological developments greatly affect data security in a company to prevent unauthorized people from viewing the document. PT Caveo Biometric Security is a company whose one of the products it sells is software development. The problem of securing data in an application is the responsibility of the software provider. Therefore, PT Caveo Biometric Security continues to develop itself to maintain the confidentiality and security of data from each of its clients. This study aims to test the data security process using Cryptographic Algorithm which adopts a decryption encryption system and uses the Advanced Encryption Standard (AES-128) method. This algorithm is very safe for securing documents to be entered into the application, so this application can maintain and secure data. The Advanced Encryption Standard (AES-128) method was chosen because this algorithm is very safe in protecting data because it has a 128-bit key length decryption encryption technique, so it is impossible for someone to break into this document even if using a fast computer. This research testing method uses the black box method, this method was chosen because this method uses a procedurally designed control structure to test and look into the software. From the test results it can be concluded that this application has succeeded in encrypting the documents entered into the application and cannot be accessed directly.*

Keywords*: Aes 128, Encryption, Decrypt*

1. PENDAHULUAN

Di era ini teknologi sudah menjadi kebutuhan manusia, yang mana dengan perkembangan yang ada dapat memudahkan manusia untuk menyelesaikan permasalahan yang ada. Salah satu yang paling penting dalam teknologi informasi bagaimana data tersebut aman tersimpan dengan baik, mudah diakses serta faktor yang tidak kalah penting adalah keamanan data itu sendiri [1]. Pada dasarnya dokumen adalah file atau sekumpulan data yang sangat pening sebagai sumber informasi yang dibutuhkan oleh perusahaan [2].

PT. Caveo Biometric Security merupakan perusahaan yang bergerak dibidang *IT Security.* Adapun salah satu produk yang dijual yaitu *Software Crew Management System* atau biasa disebut juga dengan *software management crew* kapal yang mana *software* yang mana saat ini sedang mengalami kendala pada sistem keamanan data yang berupa dokumen pribadi *crew* kapal seperti kartu identitas, ijazah, sertifikat keahlian, *medical check up*, dan lain sebagainya. Karena pentingnya data ini, maka dari itu diperlukan teknologi keamanan pada dokumen tersebut untuk mencegah orang yang tidak berwenang atau tidak berkepentingan untuk melihat dokumen – document

tersebut. Untuk mengatasi masalah ini, diperlukan suatu cara untuk melidungi data dari penyalahgunaan orang lain dengan menggunakan teknik kriptografi/enkripsi-dekripsi.

Enkripsi adalah ilmu dan teknologi untuk menjaga keamanan[1]. Kriptografi adalah ilmu yang mempelajari metode matematika yang berkaitan dengan aspek keamanan informasi seperti kerahasiaan itegritas data dan otentikasi. Enkripsi adalah ilmu dan seni untuk menjaga kerahasiaan data dengan menggunakan kunci *(key)* dalam bentuk yang tidak lagi dapat dimengerti. Metode enkripsi yang digunakan untuk mengenkripsi data dokumen pada masalah diatas menggunakan metode AES (Advanced Encryption Standard). Algortima AES meurpakan algoritma type simetris yang menggunakan kunci (*key*) yang sama untuk proses enkripsi dan dekripsi [3]–[7]

Algoritma AES (Advanced Encryption Standard) dipilih karena dirancang khusus untuk memberikan tingkat keamanan dan ketahanan yang tinggi terhadap berbagai jenis serangan. Juga kesederhanaan desain, kekompakan kode dan kecepatan enkripsi dan dekripsi setiap file atau data. [2][8]–[10]

2. METODE PENELITIAN

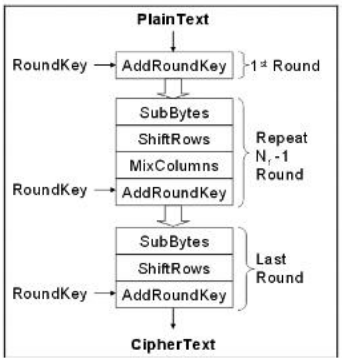
2.1. Algortima AES

Advanced Encryption Standard adalah standar enkripsi kunci simetris yang awalnya diterbitkan menggunakan algoritma Rijndael. Algoritma ini dikembangkan oleh dua kriptografer Belgia, Joan Daemen dan Vincent Rijmen. AES termasuk dalam algoritma cipher simetris dan cipher blok. AES memiliki panjang kunci 128, 192, dan 256 bit. Panjang kunci yang berbeda mempengaruhi jumlah putaran yang diimplementasikan dalam algoritma AES ini. Di bawah ini adalah tabel yang menunjukkan jumlah putaran yang diimplementasikan (Nr) untuk setiap panjang kunci.

Tabel 1. Perbandingan jumlah Round dan Key

	Key Length (Nk Words)	*Block Size (Nb words)*	*Number of Rounds (Nr)*
AES 128	4	4	10
AES 192	6	4	12
AES 256	8	4	14

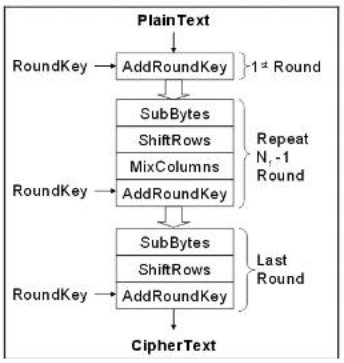
Proses enkripsi algoritma AES terdiri dari empat jenis transformasi byte: SubBytes, ShiftRows, Mixcolumns, dan AddRoundKey. Pada awal proses enkripsi, input yang disalin ke state mengalami konversi byte AddRoundKey. Kemudian mengulangi konversi SubBytes, ShiftRows, MixColumns, AddRoundKey sebannyak nr. Proses dalam algoritma AES ini disebut round fungsi. Babak akhir sedikit berbeda dengan babak sebelumnya, keadaan babak akhir tidak mengalami transformasi MixColumns. Dijelaskan dalam gambar 1[6]



Gambar 1. Diagram Alur Proses Enkripsi

Proses dekripsi algoritma AES menggunakan transformasi kebalikan dari proses enkripsi. Ciphertext yang dikembalikan akan menjadi plaintext, karena inverse transform digunakan untuk menghasilkan inverse cipher.

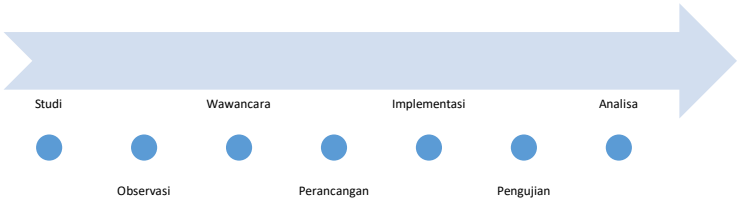
Deskripsi mendetail tentang transformasi InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey. Algoritma dekripsi dapat dilihat pada skema berikut [6].



Gambar 2. Diagram Alur Proses Dekripsi

2.2. Metode Penelitian

Dibawah ini adalah metode penelitian yang digunakan



Gambar 3. Metode Penelitian

2.3. Studi Pustaka

Pada titik ini, survei literatur dari berbagai literatur dilakukan. Penelitian kepustakaan dilakukan dengan cara mengumpulkan, membaca, dan memahami jurnal, artikel, dan referensi lain guna memperoleh informasi yang diperlukan untuk mendukung penelitian.

2.4. Observasi

Metode observasi dilakukan dengan observasi dan verifikasi pada PT Caveo Biometric Security untuk memperoleh data yang berkaitan dengan penelitian dan fakta yang terjadi di lapangan. Observasi ini dilakukan seiring berjalan dengan penelitian ini berlangsung.

2.5. Wawancara

Kegiatan ini terdiri dari serangkaian tanya jawab dan wawancara dengan karyawan untuk menemukan masalah atau kendala yang dihadapi dengan sistem keamanan dokumen saat ini.

2.6. Perancangan Aplikasi

Pada fase ini dilakukan perancangan aplikasi, dan membuat skema dari aplikasi yang akan dibuat, dan bahasa pemrograman yang ditentukan adalah ASP.Net dan menggunakan basis data Sql Server serta menentukan spesifikasi perangkat keras yang akan digunakan.

2.7. Implementasi Aplikasi

Tahap ini adalah pembuatan aplikasi pengamanan data menggunakan algoritma Kriptografi (enkripsi-dekripsi) dengan menggunakan algoritma AES-128.

2.8. Pengujian Aplikasi

Tingkat pengujian sistem bertujuan untuk mengetahui seberapa baik sistem bekerja. Tes integrasi membantu kami untuk mengetahui apakah sistem kami berfungsi seperti yang diharapkan dan mencari tahu di mana kekurangan sistem kami.

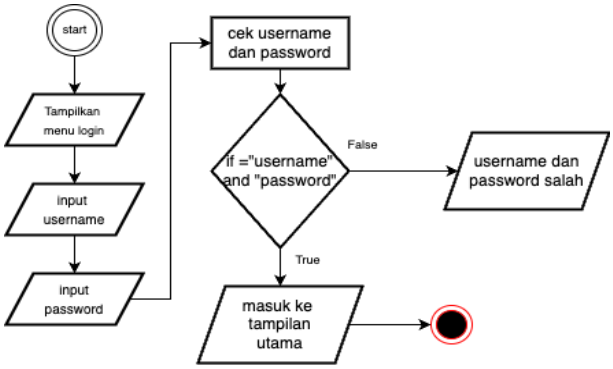
2.9. Analisa Hasil

Langkah ini meliputi analisis kebutuhan yang telah dilakukan.

3. HASIL DAN PEMBAHASAN

3.1 Cara Kerja Aplikasi

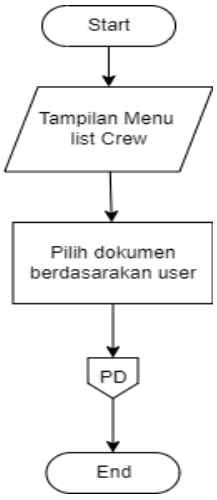
Pada awalnya *user* akan melakukan *login* terlebih dahulu dengan memasukan *username* dan *password* setelah itu aplikasi akan mengecek ke dalam *database* apakah pengguna dan kata sandi yang dimasukkan ada dan cocok



Gambar 4. *Flowchart Login*

dengan kata sandi yang dimasukkan. jika nama pengguna dan kata sandi yang dimasukkan benar maka berhasil pindah ke halaman utama. jika tidak berhasil atau gagal maka akan memunculkan notifikasi bahwa data yang di masukan tidak benar.

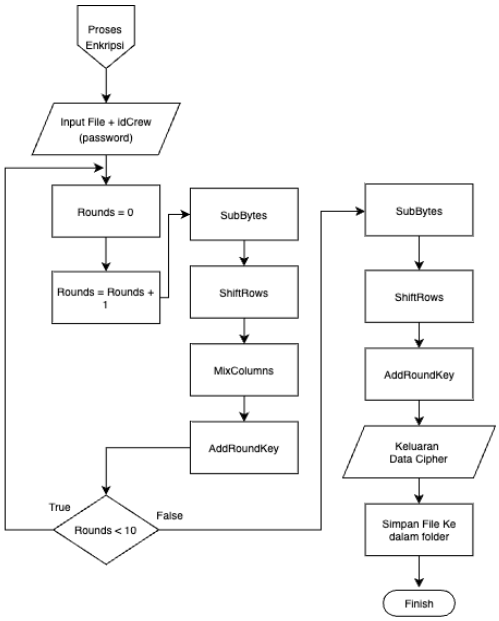
Setelah berhasil masuk kemudian akan diarahkan ke halaman dashboard. untuk melakukan upload dokumen harus masuk terlebih dahulu ke dalam form *crew* kemudian pilih registrasi *crew*



Gambar 5. *Flowchart* form enkripsi

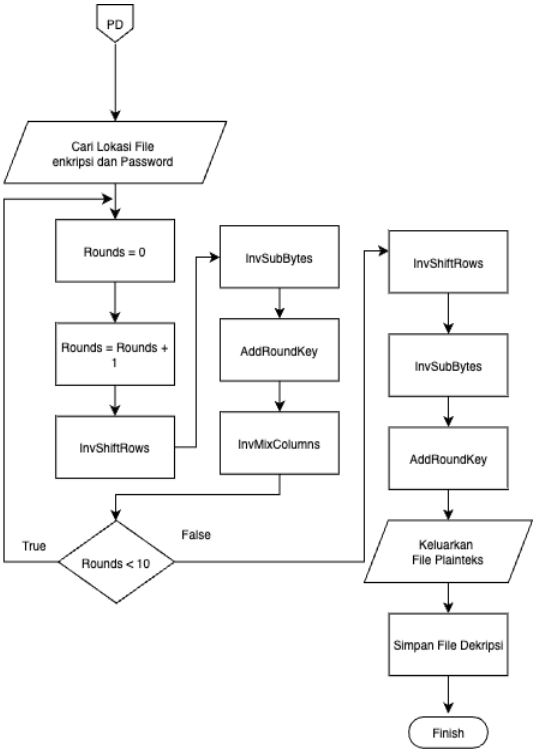
Pada Gambar 5 ini *user* akan diminta untuk memasukan data data pribadi dan jenis dokumen yang akan disertakan. untuk proses enkripsi *password* sudah di input otomatis oleh sistem berdasarkan *unique id* yang didapat pada saat setelah mengisi data pribadi

Berikut merupakan *flowchart* enkripsi AES-128 dari file pdf atau jpeg. Diagram skema dari proses enkripsi dapat ditunjukkan pada Gambar 6.



Gambar 6. Proses Enkripsi

Untuk dapat melihat file sertifikat yang sudah di masukan butuh dilakukan proses dekripsi file. Untuk proses dekripsi sudah digabungkan dengan proses download sertifikat pada menu crew kemudian masuk ke menu list of all crew



Gambar 7. Proses Deskripsi

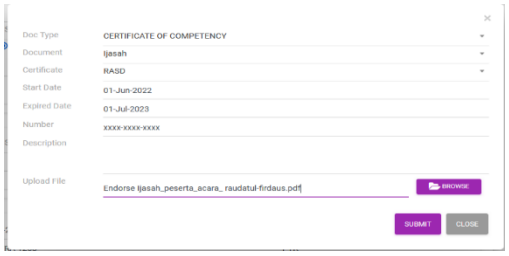
Gambar 7 merupakan *flowchart form* dekripsi ini, ditampilkan di menu menu *crew* untuk men *download* file dipilih berdasarkan user atau nama user yang akan di *download* berkasnya.

3.2 Tampilan Layar

Berikut merupkan tampilan layer dari aplikasi *crew management system:*

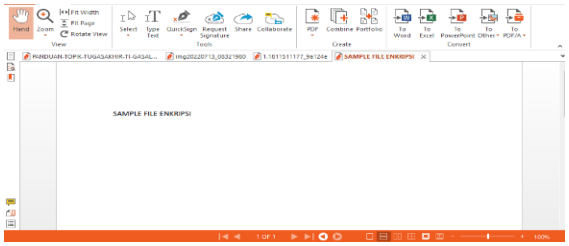
a. Proses *Upload* Sertifikat

Gambar 8 adalah isi form certifikat dengan keterangan dokument type, document, certificate type jika ada masa aktif sertifikat dan nomor seritifkat setelah itu masukan deskripsi kemudian masukan file.



Gambar 8. Form Upload Certificate

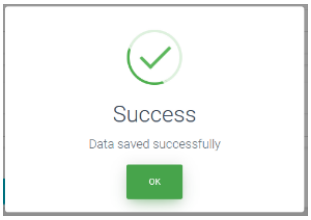
b. Proses Enkripsi File



Gambar 9. Sample data sebelum Dienkripsi

Pada gambar 9 Pada saat klik submit *system* akan menjalankan proses enkripsi file berikut adalah contoh file yang belum terenkripsi.

Setelah klik submit software akan otomatis melakukan enkripsi terhadap file tersebut dan kemudian lokasi file disimpan kedalam database. Setelah selesai akan muncul informasi data berhasil disimpan.



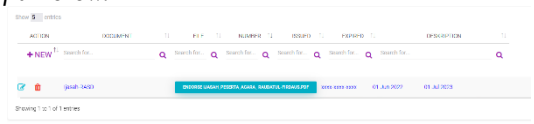
Gambar 10. Notifikasi Proses Enkripsi File Berasil

Setelah proses selesai maka data akan terenkripsi didalam local folder berikut contoh file yang sudah terenkripsi yang digambarkan pada gambar 11, Dari proses enkripsi file yang telah terenkripsi tidak dapat terbuka.

Gambar 11. Hasil File Setelah Terenkripsi

c. Proses Dekripsi File

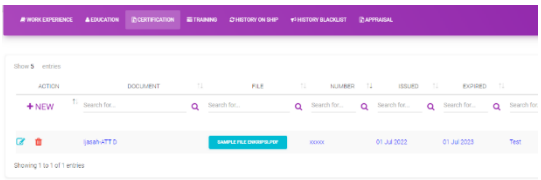
Gambar 12 menggambarkan untuk dapat melihat file sertifikat yang sudah dimasukan butuh dilakukan proses dekripsi file. Untuk proses dekripsi sudah digabungkan dengan proses download certifikat pada menu *crew* kemudian masuk ke menu *list of all crew.*



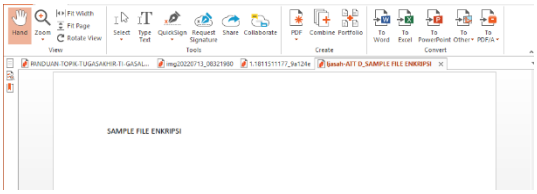
Gambar 12. Form Download Sertifikat**.**

Pada gambar 13 Pilih file yang akan didownload kemudian proses dekpripsi akan berjalan dengan mencari lokasi file tersebut yang tersimpan di dalam database berikut hasil dekripsi.

Setelah file di *download* kemudian file akan otomatis ter *download* dalam keadaan terdekrip seperti Digambar 15



Gambar 13. Proses Download File



Gambar 14. Hasil Proses Dekripsi

3.3 Pengujian Aplikasi

Setelah aplikasi selesai, pengujian fungsional aplikasi dilakukan dengan mencoba input dari data asli yang diberikan selama desain aplikasi. Data ini memberikan konfirmasi kepada pengguna tentang kebenaran algoritme aplikasi dan proses sistem, serta pemeriksaan kesalahan dan kesesuaian antarmuka aplikasi. Metode yang digunakan untuk menguji sistem ini menggunakan metode *black box*.

Pengujian *black box* adalah metodologi pengujian yang menggunakan struktur kontrol yang dirancang secara prosedural untuk melakukan pengujian dan melihat ke dalam perangkat lunak. Semua komponen internal perangkat lunak diuji untuk memastikan mereka berfungsi sesuai dengan spesifikasi dan desain.

Tabel 2. Pengujian *Black box*

Aktifitas Jenis Pengujian	Hasil Yang Diharapkan	Hasil Pengujian	Hasil Pengujian
Respon Waktu untuk koneksi kedalam database	Respon waktu yang diperlukan untuk pengaksesan dan database cepat	Aplikasi dapat mengakses server dan database dengan waktu respon rata-rata kurang dari 2 detik dalam pengujian menggunakan 3 PC klien.	Diterima

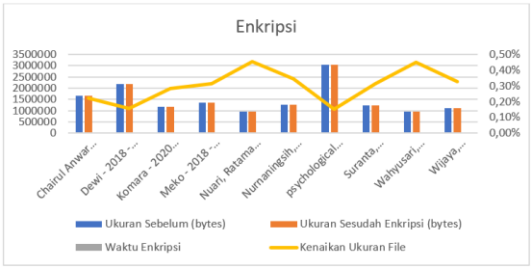
Form Menu Login	Data yang dimasukkan akan dialihkan ke halaman dashboard jika pengguna memasukkan username dan password dengan benar, dan jika username atau password salah akan ditampilkan notifikasi bahwa username atau password salah akan ditampilkan.	Aplikasi mampu memenirma username dan password mengecek ke dalam database apakah berdasarkan username yang dimasukan cocok dengan password yang ada didalam database dan memberikan informasi jika user salah memasukan username atau password	Diterima
Form Profile	Data yang ditampilkan adalah data yang terbaru dana apabila ada perubahan langsung terupdate pada database	Data yang ditampilkan sudah data yang terbaru dan ketika ada perubahan pada form data sudah terupdate ke dalam database	Diterima
Form Master Posisiton	Dapat menambahkan , menghapus dan merubah jenis-jenis jabatan yang terdaftar	Data yang dimasukan berhasil masuk kedalam database dan juga mengubah jenis-jenis jabatan dan dapat menghapus jeni-jenis jabatan yang ada didalam database	Diterima
Form Master Bank	Dapat menambahkan mengapus dan merubah nama nama bank	Data yang dimasukan kedalam database dan juga merubah daftar nama bank dan juga merubah dan menghapus nama-nama bank yang terdaftar didalam database	Diterima
Form Master Certificate	Dapat menambahkan menghapus dan merubah jenis-jenis kategori sertifikat	Data yang dimasukan kedalam database dan juga dapat merubah dan menghapus data yang ada didalam database	Diterima
Form Master Document	Dapat menambahkan menhapus dan merubah jenis-jenis kategori document	Data yang dimasukan kedalam database dan juga dapat merubah dan menghapus data yang ada didalam database	Diterima
Form Master Crew Type Test	Dapat menambahkan menghapus dan merubah type jenis-jenis type test untuk crew	Data yang dimasukan kedalam database dan juga dapat merubah dan menghapus data yang ada didalam database	Diterima
Form Master City	Dapat menambahakan menghapus dan merubah nama nama kota	Data yang dimasukan kedalam database dan juga dapat merubah dan menghapus data yang ada didalam database	Diterima
Menu Master Crew	Dapat menambahkan menghapus dan merubah para crew	Data yang dimasukan kedalam database dan juga dapat merubah dan menghapus identitas crew	Diterima
Master For Crew Registration	Dapat Menambahkan , menghapus dan merubah data – data crew	Data yang dimasukan kedalam database berhasil dan juga dapat merubah data dan juga menghapus data para crew	Diterima
Form Certificate	Dapat mengenkripsi file pdf,jpg yang diupload ke aplikasi	File yang diupload ke server bisa terenkripsi	Diterima
Crew Report	Dapat menampilkan semua data crew yang terdaftar	Data yang ditampilkan seusai dengan data yang ada didalam database	Diterima
Certificate Report	Dapat Menampilkan semua sertifikat berdasarkan crew yang sudah terdekripsi	Dapat menampilkan semua sertifikat yang terdaftar dan juga dapat mendownload sertifikat tersebut dalam keadaan ter dekripsi	Diterima

3.4 Analisis Pengujian

Setelah aplikasi dijalankan, dilakukan pengujian black box berupa pengujian jaringan aplikasi. Skema pengujian yang dibuat mengenkripsi 10 file dan mendekripsinya lagi. Pengujian ini tidak hanya mengukur keberhasilan enkripsi dan dekripsi, tetapi juga mengukur kecepatan proses enkripsi dan dekripsi yang sedang berlangsung dan juga memeriksa perubahan ukuran file setelah proses enkripsi dan dekripsi.

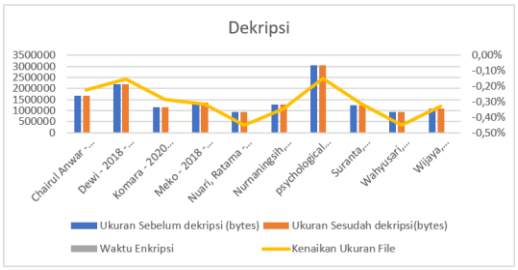
File yang digunakan pengujian rata – rata dibawah 3MB. Dan data yang digunakan adalah beberapa jurnal yang say abaca dan saya gunakan dan juga data yang diguanakan semua berupa file pdf Setelah pengujian untuk mengenkripsi file, aplikasi berjalan dengan baik. Berdasarkan uji kriptografi yang dilakukan, kami juga memperoleh data yang ditunjukkan pada Gambar 14. Proses enkripsi file yang diujikan masih kurang dari 1 detik, sehingga ternyata sangat cepat.

Persentase keaikan ukuran file terjadi pada proses enkripsi terjadi di 2 file yaitu " Nuari, Ratama - 2020 Implementasi Algoritma" dan "Wahyusari, Haryoko - 2014 - Penerapan Algoritma".



Gambar 15. Pengujian Enkripsi

Pengujian proses dekripsi menggunakan file yang telah melalui proses enkripsi sebelumnya. Berdasarkan uji dekripsi, kami memperoleh data yang ditunjukkan pada Gambar 15. Ternyata ukuran file yang didekripsi menurun seiring dengan ukuran file. Dari segi waktu proses dekripsi, masih terbilang cepat untuk waktu proses enkripsi. Namun, jika Anda menemukan bahwa beberapa file mempercepat dan beberapa file melambat.



Gambar 16. Pengujian Dekripsi

4. KESIMPULAN

Dari hasil analisis, tampaknya data material kru berhasil diamankan yang mana pada proses pengujian ini menggunakan metode blackbox yang mana metode ini melakukan pengujian secara prosedural dan melihat kedalam perangkat lunak sesuai dengan spesifikasi design yang telah dibuat. Oleh karena itu, kita dapat menarik kesimpulan bahwa kehadiran aplikasi enkripsi - dekripsi file menggunakan algoritma AES-128 dapat meningkatkan keamanan dokumen dari serangan pihak yang tidak berkepentingan. Rata-rata kurang dari 1 detik dari eksperimen enkripsi hingga 10 file,hasil eksperimen dekripsi dengan 10 file menunjukkan proses dekripsi rata-rata, yang memakan waktu hampir sama dengan proses enkripsi 1 detik.

DAFTAR PUSTAKA

[1] S. Waluyo, I. Susanti and A. I. Prasetyo, "Sistem Kriptografi Manajemen File Data Penutupan Asuransi Menggunakan Algoritma AES-128 Studi Kasus: PT . Asuransi Bringin Sejahtera Artamakmur (BRINS)," *Proceeding SENDIU*, Unisbank, pp. 347-350, 2020.

[2] R. Nuari and N. Ratama, "Implementasi Algoritma Kriptografi AES (Advanced Encryption Standard) 128

Bit Untuk Pengamanan Dokumen Shipping," 2020.
[3] M. Azhari, J. Perwitosari, and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," *J. Pendidik. Sains dan Komput.*, vol. 2, no. 1, pp. 2809–476, 2022.
[4] A. I. Suranta, D. Virgian, and S. Y. Sakti, "Penerapan Algoritma AES (Advance Encryption Standart) 128 untuk Enkripsi Dokumen di PT. Gunung Geulis Elok Abadi," *SKANIKA Sist. Komput. dan Tek. Inform.*, vol. 5, no. 1, pp. 1–10, 2022.
[5] R. Wijaya, K. Farandi, and S. Miharja, "Implementasi Algoritma Aes-128 Dan Sha-256 Dalam Perancangan Aplikasi Pengamanan File Dokumen," 2021.
[6] A. Fitriansyah and M. F. Andrika, "Aplikasi Penandatanganan Dokumen Secara Digital Menggunakan Metode Advanced Encryption Standard (AES)," pp. 1–12, 2021.
[7] R. I. Sardi, "Implementasi Algoritme AES 128 bit Pada Mikrokontroler NodeMCU Menggunakan Arsitektur Web Service Rest Untuk Keamanan Pengiriman Data," *Publ. Tugas Akhir S-1 PSTI FT-UNRAM*, 2020.
[8] L. A. Indrayani and I. M. Suartana, "Implementasi Kriptografi dengan Modifikasi Algoritma Advanced Encryption Standard (AES) untuk Pengamanan File Document," *JINACS: Journal of Informatics and Computer Science*, vol. 1, nol. 1, pp. 42-47, 2019.
[9] A. Prameshwari and N. P. Sastra, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen," *Eksplora Informatika*, vol. 8, no. 1, pp. 52-58, 2018.
[10] D. Nurnaningsih and A. A. Permana, "Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (AES)," *Jurnal Teknik Informatika*, vol. 11, no. 2, pp. 177–186, 2018.