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 ADVANCED ENCRYPTION STANDARD (AES-128) UNTUK PENGAMANAN DATA BERBASIS WEB

Alfiansyah Tri Purnomo[1*], Joko Christian Chandra[2]

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

Email: [1*]1911501763@student.budiluhur.ac.id, [2] joko.christian@budiluhur.ac.id
(* : corresponding author)

Abstrak- Ketika menggunakan jaringan internet, keamanan data atau informasi memiliki nilai yang sangat tinggi. Dalam konteks ini, penyadapan data atau informasi adalah tindakan yang sangat merugikan. Mengingat kemungkinan kejadian ini terjadi, kebutuhan untuk meningkatkan aspek keamanan pertukaran informasi menjadi lebih besar. Data yang digunakan dalam penelitian ini mencakup informasi mengenai Nasabah, data NPWP Perusahaan, serta beberapa data lainnya. Sumber data berasal dari dokumen yang diperoleh dari PT Asuransi Central Asia. Pentingnya menjaga keamanan pertukaran informasi saat ini menuntut perhatian khusus. Oleh karena itu, Penelitian ini akan melaksanakan penerapan algoritma kriptografi AES-128 dengan pendekatan metode waterfall untuk melakukan proses enkripsi dan dekripsi terhadap data dalam bentuk file dokumen yang berformat *(.doc, .docx, .xls, .xlsx, .ppt, .pptx, dan .pdf)*. Algoritma *Advanced Encryption Standard* (AES) dipilih karena memiliki tingkat keamanan yang baik. penelitian ini bertujuan untuk mengimplementasikan AES 128 pada PT Asuransi Central Asia untuk melindungi data sensitif dengan baik dan memenuhi standar keamanan yang tinggi. Implementasi ini merupakan solusi yang baik untuk memastikan data sensitif pada PT Asuransi Central Asia. Hasil dari penelitian ini kemudian diuji dengan metode *testing blackbox* dan berfungsi sesuai rancangan.

Kata Kunci: Kriptografi, AES-128, Pengamanan Data, Enkripsi, Dekripsi

ADVANCED ENCRYPTION STANDARD (AES-128) CRYPTOGRAPHY ALGORITHM IMPLEMENTATION FOR WEB-BASED DATA SECURITY

Abstract- *When using the internet network, data or information security has a very high value. In this context, wiretapping of data or information is a very detrimental action. Given the possibility of this incident happening, the need to improve the security aspects of information exchange becomes greater The data used in this study includes information about customers, company NPWP data, and some other data. The data source comes from documents obtained from PT Asuransi Central Asia. The importance of maintaining the security of information exchange currently demands special attention. Therefore, This study will carry out the application of the AES-128 cryptographic algorithm with the waterfall method approach to encrypt and decrypt data in the form of document files (.doc, .docx, .xls, .xlsx, .ppt, .pptx, and .pdf)).The Advanced Encryption Standard (AES) algorithm was chosen because it has a good level of security. This study aims to implement AES 128 at PT Asuransi Central Asia to properly protect sensitive data and meet high security standards. This implementation is a good solution to ensure sensitive data at PT Asuransi Central Asia. The results of this study were then tested using the blackbox testing method and functioned according to design.*

Keywords*: Cryptography, AES-128, Data Security, Encryption, Decryption*

1. PENDAHULUAN

Keamanan data adalah tindakan untuk menjaga dan mengamankan paket informasi saat dilakukan pertukaran data dalam lingkungan digital [1]. Tujuan dari penelitian ini adalah menciptakan suatu metode untuk meningkatkan keamanan transaksi data secara *daring*. [2]. Metode yang akan digunakan adalah literature review, yang akan membandingkan berbagai metode keamanan data yang telah ada dalam konteks pembelajaran online. [3]

Kriptografi (*cryptography*) adalah bidang ilmu dan seni yang bertujuan untuk menyimpan pesan, data, atau informasi dengan aman. Hal ini dicapai melalui proses enkripsi dan dekripsi menggunakan berbagai algoritma yang dikembangkan oleh para ahli kriptografi. Tujuan dari kriptografi adalah untuk menjaga kerahasiaan data (*confidentiality*), keutuhan data (*data integrity*), otentikasi (*authentication*), serta mencegah penyangkalan informasi (*non-repudiation*)[4]. Kriptografi berasal dari bahasa Yunani yaitu ‘kryptos’ yang berarti tersembunyi dan ‘graphein’ yang bermakna tulisan. Kriptografi adalah ilmu menulis pesan rahasia yang mana bertujuan untuk menyembunyikan makna sesungguhnya dari pesan tersebut [5]. Algoritma AES memiliki ukuran blok tetap, yaitu 128 bit, namun memiliki panjang kunci yang bervariasi. Untuk menggunakan kunci AES-128, algoritma ini

melibatkan serangkaian perulangan yang disebut "*round*" yang terdiri dari 10 putaran. Dalam setiap putaran, dilakukan operasi enkripsi dan dekripsi dengan menggunakan matriks 4 x 4. Setiap elemen dalam matriks tersebut berukuran 1 byte atau 8 bit.[6]

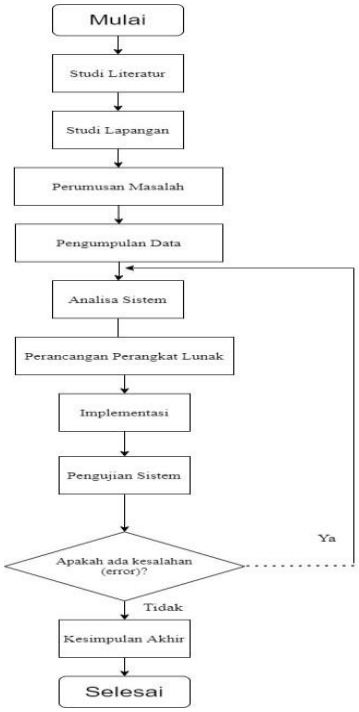
PT Asuransi Central Asia adalah Perusahaan asuransi properti dan kecelakaan yang didirikan pada tanggal 29 Agustus 1956 dan berlokasi di Jl. Prof. Dr. Latumenten No.28 abc, Jakarta Barat. Dengan data yang dihasilkan berupa data Nasabah, data NPWP Perusahaan dan data lainnya. Saat ini, data tersebut masih berupa file biasa yang dapat dibaca oleh orang yang tidak berwenang yang disimpan dalam format *doc,*docx, *pdf, *xls dan lainnya. Hanya karyawan PT dan Manager cabang yang memiliki akses ke data dari PT Asuransi Central Asia cabang Latumenten.

Berdasarkan latar belakang yang terjadi di atas, kontribusi penelitian ini penulis melakukan penelitan untuk mengamankan data pada PT Asuransi Central Asia hasil kinerja karyawan perusahaan terkait dalam penggunaan *algoritme kriptografi Advanced Encryption Standard* (AES-128).

Penelitian ini melakukan penerapan langsung dari algoritma kriptografi AES-128 setelah sebelumnya melakukan riset yang menggunakan algoritma RC4 untuk tujuan mengamankan file [7]. Penelitian ini mengevaluasi perbandingan kecepatan proses enkripsi dan dekripsi menggunakan algoritme AES dan RC4 pada LSB dengan menggunakan Microsoft Visual Studio 2008. Hasil penelitian menunjukkan bahwa algoritme AES memiliki kecepatan yang lebih baik daripada algoritme RC4 dalam proses enkripsi dan dekripsi. Selain itu, nilai MSE dan PSNR dari gambar-gambar yang dienkripsi dengan algoritme AES dan RC4 tidak menunjukkan perbedaan nilai yang signifikan atau stabil. Secara keseluruhan, penelitian ini menyimpulkan bahwa algoritme AES lebih unggul dalam hal kecepatan ketika diterapkan pada LSB dibandingkan dengan algoritme RC4 jika diterapkan pada LSB.[8].

2. METODE PENELITIAN

Penelitian ini merekomendasikan mengikuti tahapan fungsional sebagai panduan dalam menjalankan penelitian, sehingga hasil yang dicapai tetap sesuai dengan tujuan yang telah ditetapkan sebelumnya. Ilustrasi metode yang diterapkan dalam penelitian ini dapat dilihat pada Gambar 1 yang menggambarkan langkah-langkah penerapan metode penelitian yang digunakan.



Gambar 1. Metodologi penilitian

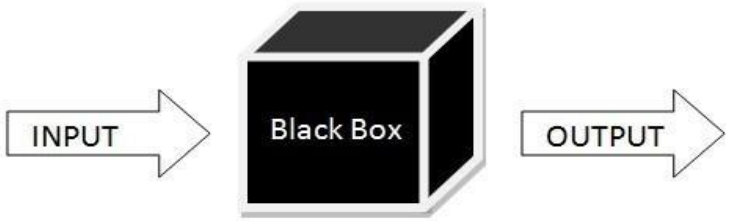
2.1 Pengumpulan Data

Pada tahap ini, dilakukan pengumpulan data. Proses pengumpulan data dilakukan melalui wawancara dan observasi. Berikut adalah penjelasan mengenai kedua metode pengumpulan data tersebut [9]:

a. Wawancara (*Interview)*. Dilakukan proses interaksi dengan semua pihak yang terlibat dalam pengembangan aplikasi dan program melalui wawancara, Dengan maksud untuk mendapatkan pengetahuan tentang aplikasi dan perangkat keamanan yang digunakan.
b. Pengamatan (*Observation*). Metode pengamatan digunakan sebagai salah satu pendekatan yang efektif dalam mengumpulkan data dengan cara melakukan pengamatan langsung terhadap operasi sistem tersebut secara mendalam.

2.2 Metode *Blackbox Testing*

Metode Blackbox Testing adalah metode yang sederhana dan mudah digunakan karena hanya memerlukan batas bawah dan batas atas dari data yang diharapkan. Estimasi jumlah data yang diuji dapat dihitung berdasarkan jumlah field data entry yang akan diuji. Selama proses ini, aturan entry harus dipatuhi, dan kasus uji untuk batas bawah dan batas atas harus dipertimbangkan. Metode ini membantu mengidentifikasi apakah fungsionalitas sistem masih dapat menerima masukan data yang tidak diharapkan, yang dapat mengakibatkan data yang tidak valid disimpan.



Gambar 2. Metode *Blackbox Testing*

2.3 Kriptografi

Kriptografi bertujuan untuk menyediakan layanan keamanan informasi, yang juga dikenal sebagai aspek-aspek keamanan informasi, yaitu:

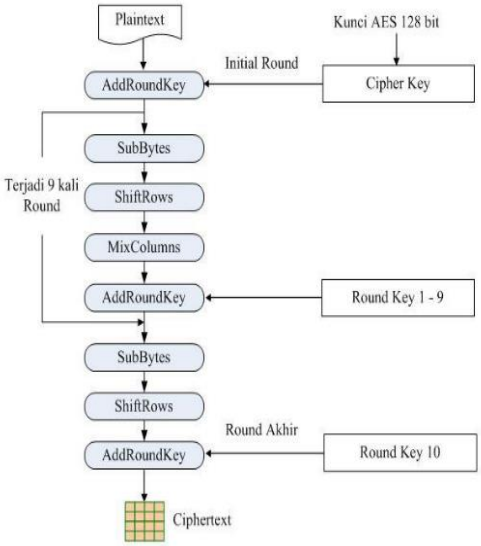
a. Kerahasiaan (*confidentiality*) adalah salah satu layanan yang bertujuan untuk melindungi pesan agar tidak dapat diakses atau dibaca oleh pihak-pihak yang tidak memiliki hak atau otoritas untuk melakukannya.
b. Integritas Data (*integrity data*) adalah sebuah fasilitas yang bertujuan untuk memastikan bahwa pesan tetap utuh dan asli, serta tidak mengalami manipulasi selama proses pengiriman pesan.
c. Otentikasi (*authentication*) adalah suatu fasilitas terkait dengan proses identifikasi, digunakan untuk memverifikasi keaslian pihak-pihak yang berkomunikasi (autentikasi pengguna atau autentikasi entitas) serta memverifikasi keaslian sumber pesan (autentikasi asal data).
d. Nir Penyangkalan (*Non-Repudiation*) adalah Suatu fasilitas yang dimaksudkan untuk mencegah entitas yang berkomunikasi untuk menolak atau menyangkal tindakan yang telah dilakukan, seperti pengirim pesan menyangkal telah melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

Agar proses kriptografi dapat berjalan dengan baik, empat elemen utama harus ada di dalamnya, yang erat kaitannya satu sama lain, yaitu [10]:

a. *Plain Text*, yang mengacu pada pesan asli atau pesan awal yang dikirim dalam proses komunikasi. Pesan *Plain text* ini akan melalui proses enkripsi dan dekripsi.
b. *Cipher Text* yang merupakan pesan yang tersembunyi. *Cipher Text* adalah hasil dari enkripsi pesan asli (*Plain Text*) selama proses kriptografi. Untuk mengembalikan pesan ke bentuk aslinya (*Plain Text*), kita memerlukan *Key* yang sesuai.
c. *Cryptography Key* yang berfungsi sebagai kunci untuk melakukan proses enkripsi dan dekripsi dalam kriptografi. Tanpa kunci yang sesuai, proses enkripsi dan dekripsi tidak dapat berjalan dengan baik. Kunci kriptografi ini adalah informasi yang padat dan mengontrol seluruh proses kriptografi.
e. *Encryption Decryption Algorithm* memiliki peran khusus dalam proses kriptografi. Algoritma ini digunakan untuk melakukan enkripsi dan dekripsi data.

2.4 *Advanced Encryption Standard* (AES)

Advanced Encryption Standard (AES) adalah sebuah algoritma kriptografi blok simetris yang menggantikan *Data Encryption Standard* (DES). Algoritma AES memiliki ukuran blok yang tetap yaitu 128 bit, namun panjang kunci yang digunakan bisa bervariasi. Pada mode AES-128, proses enkripsi dan dekripsi melibatkan iterasi yang disebut "*round*" dengan total 10 putaran. Setiap putaran melibatkan sebuah matriks berukuran 4 x 4, dimana setiap elemen matriks terdiri dari 1 Byte atau 8 bit.[6]**.**

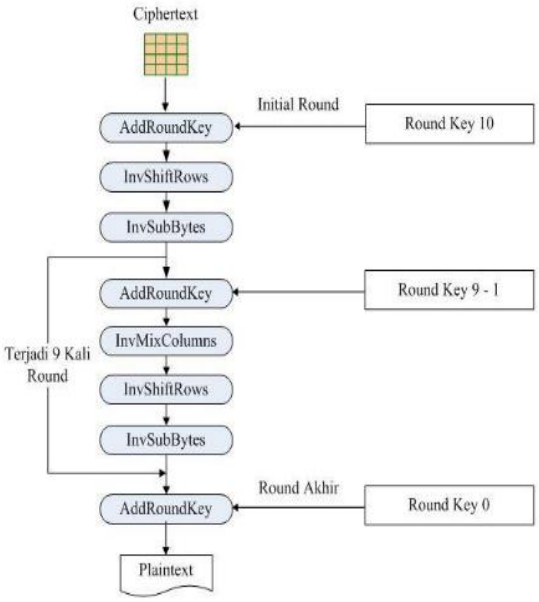


Gambar 3. Proses Enkripsi menggunakan Algoritma AES

Pada gambar 3 Secara garis besar, langkah-langkah untuk melakukan enkripsi menggunakan AES 128 dengan kunci 128 bit adalah sebagai berikut :

1. *AddRoundKey*: Melakukan operasi XOR antara state awal (*Plaintext)* dengan *Ciphertext*. Tahap ini juga dikenal sebagai tahap awal (*Initial Round*).
2. Putaran (*Round*): Dilakukan sebanyak *Nr*-1 kali. Setiap putaran melibatkan langkah-langkah berikut:
   1) *SubBytes*: Menggantikan setiap byte dalam blok dengan byte yang sesuai dari tabel substitusi (*S-Box*).
   2) *ShiftRows*: Melakukan pergeseran pada baris-baris Array State dengan cara melakukan *wrapping* atau penggeseran sirkular.
3. *MixColumns*: Merandom data pada setiap kolom *Array State* dengan menerapkan persamaan berikut
   A(x) = {03}x2 + {01}x2 + {01}x2 + {0}
4. *AddRoundKey*: Melakukan operasi XOR antara *Array State* saat ini dengan *Round Key* yang sesuai.
5. Tahap terakhir (*Final Round*): Tahap ini merupakan putaran terakhir dan melibatkan langkah-langkah berikut:
   1) *SubBytes*
   2) *ShiftRows*
   3) *AddRoundKey*
6. Pada langkah ini, akan dihasilkan karakter atau teks dalam bentuk *CipherText*.

Langkah-langkah ini menjelaskan proses enkripsi AES-128 dengan menggunakan *AddRoundKey*, *SubBytes*, *ShiftRows*, *MixColumns* dan langkah-langkah terakhir untuk menghasilkan *Chipertext*.



Gambar 4. Proses Dekripsi menggunakan AES

2.5 Pengujian Sistem

Pada tahap ini, dilakukan pengujian untuk memastikan bahwa sistem yang telah dibangun sesuai dengan analisis dan perancangan awal dan menghasilkan hasil yang diinginkan. Dalam pengujian ini, digunakan metode blackbox testing, di mana peneliti mengamati hasil eksekusi melalui data uji dan memeriksa fungsionalitas perangkat lunak. Tujuan dari pengujian ini adalah untuk memastikan bahwa sistem yang sedang dikembangkan sesuai dengan harapan dan kebutuhan yang telah ditetapkan sebelumnya.

2.6 Kesimpulan

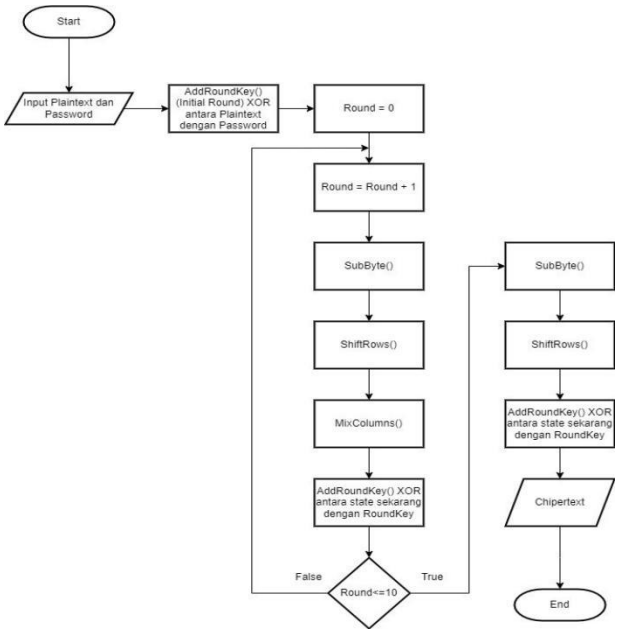
Dari hasil pengujian, terbukti bahwa penerapan metode enkripsi AES-128 dalam keamanan file berhasil dengan baik. Evaluasi dilakukan untuk memverifikasi kemampuan implementasi Advanced Encryption Standard (AES) dalam menjaga keamanan file secara efektif. Selain itu, dalam tahap ini, rekomendasi dan saran-saran disusun untuk meningkatkan kualitas dan efisiensi implementasi metode tersebut, serta untuk memperbaiki sistem agar lebih baik di masa depan.

3. HASIL DAN PEMBAHASAN

Bagian ini akan melaksanakan penerapan program kriptografi berbasis web untuk dokumen dengan format **.doc*, **.xls*, **.docx*, **.xlsx*, **.ppt*, **.pptx*, dan **.txt*. Implementasi ini akan menggunakan algoritma AES-128 guna menjamin keamanan data. Di bawah ini tercantum spesifikasi perangkat lunak (*software*) dan perangkat keras (*hardware*) yang diperlukan untuk pelaksanaan implementasi ini.

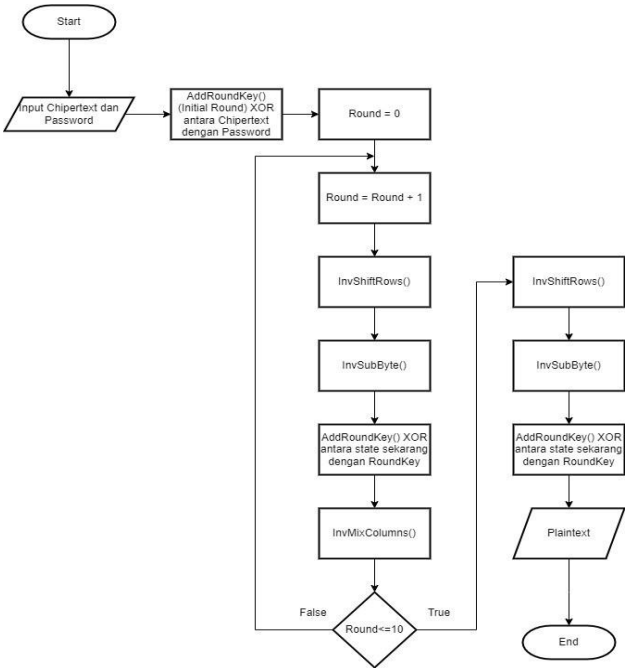
3.1 *Flowchart*

Gambar 5 adalah sebuah *Flowchart* Enkripsi. Ketika aplikasi berjalan, sistem akan menerima input dari Pengguna berupa kunci dan file dokumen yang akan dienkripsi. Selanjutnya, sistem akan segera memulai proses enkripsi dengan mengambil langkah pertama yaitu *AddRoundKey*. Transformasi *AddRoundKey* ini dilakukan pada langkah pertama proses enkripsi dengan nilai *Round* awal adalah 0, dan kemudian nilai *Round* akan diincrement (ditambah 1) setiap kali langkah ini dilakukan. Setelah itu, sistem akan melakukan putaran pertama yang terdiri dari proses *SubBytes*, *ShiftRows*, *MixColumns*, dan terakhir *AddRoundKey*.



Gambar 5. *Flowchart* Proses Enkripsi

Gambar 6 adalah *Flowchart* proses Dekripsi. Proses dekripsi dimulai dengan langkah pada *round*=10, dan kemudian nilai *round* akan dikurangi satu setiap langkahnya (*round* = *round*-1). Selanjutnya, sistem akan menjalankan putaran pertama, yang mencakup langkah-langkah *InvShiftRows, InvSubBytes*, dan *AddRoundKey*. Pada langkah ini, nilai (*Round*) tetap sama dengan Nr 1, dan dalam algoritme AES, proses ini melibatkan total 10 putaran. Ketika jumlah putaran dikurangi satu atau mencapai 0 putaran, sistem akan melanjutkan ke proses final round, yang terdiri dari langkah-langkah *InvShiftRows, InvSubBytes*, dan *AddRoundKey*.

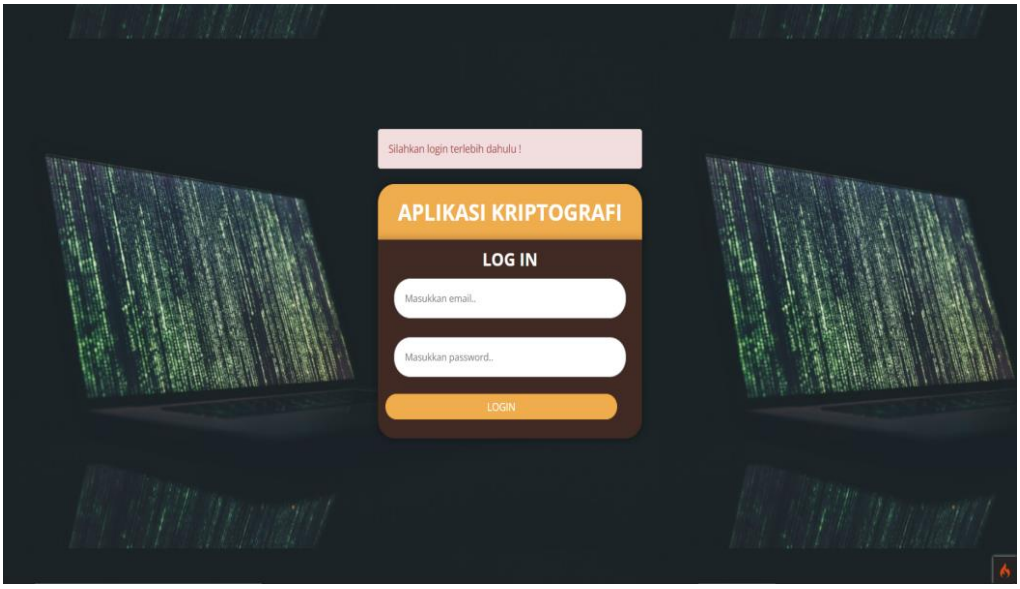


Gambar 6. *Flowchart* Proses Dekripsi AES

3.2 Tampilan Layar

a. Tampilan Layar *Login*

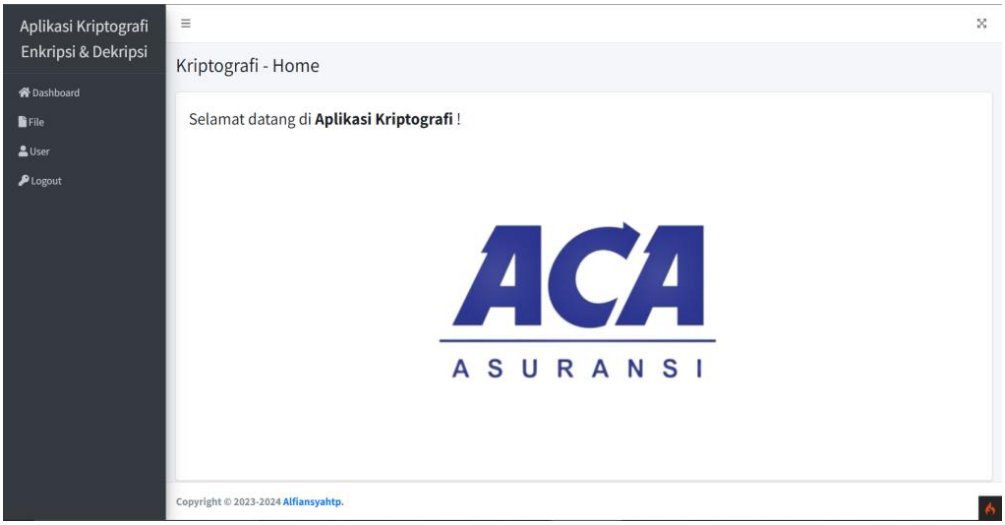
Halaman ini menampilkan tampilan layar pada menu *Login* yang muncul saat mengakses *website* pertama kali. Untuk mengakses menu berikutnya, pengguna harus memasukkan *username* dan *password* yang sudah terdaftar. Saat sudah berhasil masuk, pengguna akan dilanjutkan ke proses selanjutnya yaitu ke tampilan halaman *Dashboard*.



Gambar 7. Tampilan Layar *Login*

b. Tampilan Layar halaman *Dashboard*

Halaman ini menampilkan sambutan Selamat Datang di dalam aplikasi, lengkap dengan logo dari PT Asuransi Central Asia. Dengan tampilan lainnya yaitu ada beberapa pilihan menu lain seperti *File* untuk melakukan enkripsi dan dekripsi file, menu *User* untuk menambahkan atau menghapus "*User*" dan terakhir *Logout* ketika *User* sudah mengakhir sistem. Berikut adalah Gambar 8 yang menggambarkan tampilan halaman tersebut.

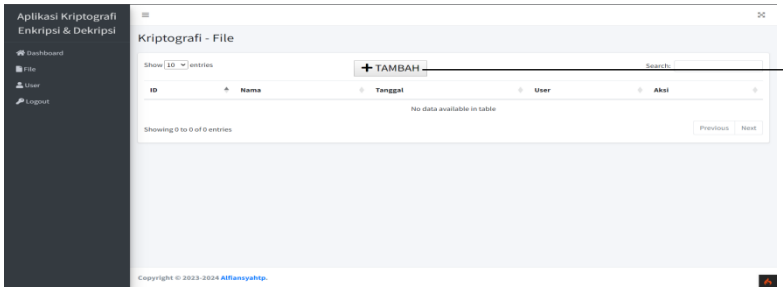


Gambar 8. Tampilan Layar *Dashboard*

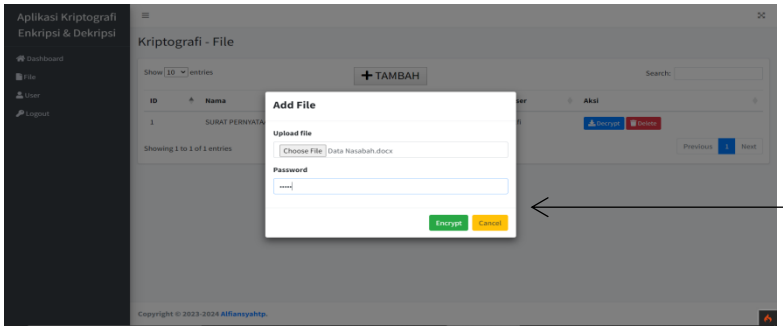
c. Tampilan Layar halaman menu *File*

Di halaman menu File, terdapat tabel untuk pengguna melakukan enkripsi dan dekripsi file. Pengguna diberikan opsi untuk memilih beberapa file yang ingin dienkripsi. Jika pengguna ingin mengenkripsi file, langkah awal adalah dengan memilih tombol "Tambah", kemudian memilih file-file yang ingin dienkripsi dalam form "Add File". Setelah itu, pengguna diminta untuk memasukkan *password* sesuai dengan keinginannya.

Kemudian, pengguna juga dapat melakukan proses dekripsi pada sub menu yang sama setelah melakukan proses enkripsi. Untuk melakukan dekripsi, cukup dengan memasukkan password yang sama seperti yang digunakan saat melakukan enkripsi. Tampilan layar sub menu File dapat dilihat pada Gambar 9. Sedangkan Gambar 10 menunjukkan tampilan layar proses enkripsi data pada aplikasi.

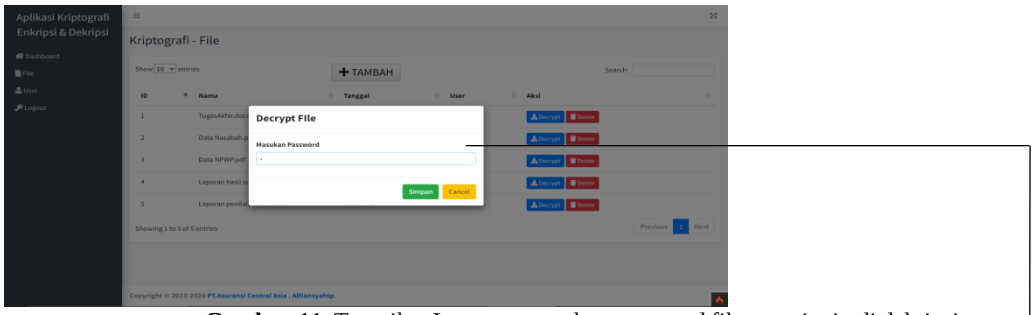


Gambar 9. Tampilan Layar menu Enkripsi

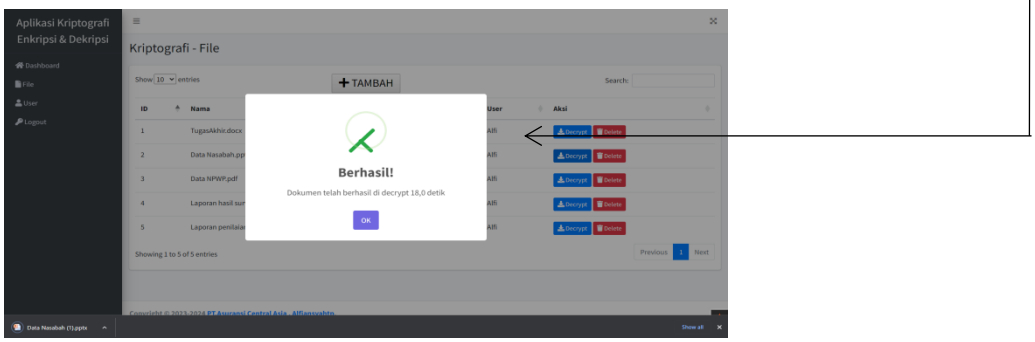


Gambar 10. Tampilan Layar menu *Add File*

Gambar 11. Untuk memulai proses *Decrypt*, *User* hanya perlu memilih file yang ingin di *Decrypt* yang berada di sub menu *File* , kemudian *User* dapat memilih berkas yang ingin di *Decrypt* dengan memilih tombol *Decrypt* berkas, setelah itu akan dilanjutkan ke halaman *Decrypt File*. dihalaman tersebut *User* diminta memasukan *Password* yang sudah dimasukan pada saat melakukan *Encrypt*. Untuk melakukan *Decrypt*, *User* bisa memilih tombol *Decrypt* dan *User* sudah mendapatkan berkas yang sudah di *Decrypt* karena sistem langsung mendownload secara otomatis setelah menekan tombol *Decrypt* dapat dilihat pada gambar 12.



Gambar 11. Tampilan Layar memasukan password file yang ingin di dekripsi



Gambar 12. Tampilan Layar File telah berhasil di dekripsi

3.3 Hasil Pengujian Enkripsi dan Dekripsi File

Di bawah ini terdapat hasil pengujian dari program aplikasi Enkripsi dan Dekripsi AES-128, yang bertujuan untuk mengevaluasi keberhasilan implementasinya. Tabel 1 menyajikan hasil pengujian Enkripsi, sementara Tabel 2 menampilkan hasil pengujian Dekripsi pada program aplikasi Enkripsi dan Dekripsi AES-128. Hasil dari kedua tabel tersebut dapat disimpulkan bahwa *File* yang telah dilakukan Enkripsi dan Dekripsi tidak mengubah Ukuran *File*. Kemudian dalam melakukan proses Enkripsi, nama dan format *File* akan berubah dan akan kembali lagi seperti semula ketika proses Dekripsi dilakukan. Proses Enkripsi dan Dekripsi akan berlangsung lebih cepat tergantung dari ukuran *File*, kebalikan jika melakukan proses Enkripsi dan Dekripsi pada ukuran *File* yang lebih besar maka waktu yang dibutuhkan akan meningkat.

Tabel 1. Hasil Pengujian Enkripsi

No	Nama Asli File	Ukuran File asli per(kb)	Nama File setelah di enkripsi	Ukuran File setelah di enkripsi per(kb)	Waktu Per(Detik)
1.	Laporan penilaian Bank.docx	52 kb	62206-laporan-penilaian-bank.rda	52 kb	0,170 detik
2.	Laporan hasil Survey.xls	438 kb	80311-laporan-hasil-survey.rda	438 kb	10,1 detik
3.	Data NPWP.pdf	1.789 kb	58849-data-npwp.rda	1.789 kb	42,9 detik
4.	Data Nasabah.pptx	1.023 kb	97851-data-nasabah.rda	1.023 kb	24,9 detik
5.	Tugas Akhir.docx	8.329 kb	48105-tugasakhir.rda	8.329 kb	152,5 detik

Tabel 2. Hasil Pengujian Dekripsi

No	Nama File Enkripsi	Ukuran File Asli per kb(KB)	Nama File setelah di Dekripsi	Ukuran file setelah di Dekripsi per (kb)	Waktu per (detik)
1.	62206-laporan-penilaian-bank.rda	52 kb	Laporan penilaian bank.docx	52 kb	0,145 detik
2.	80311-laporan-hasil-survey.rda	438 kb	Laporan hasil Survey.xls	438 kb	10,7 detik
3.	58849-data-npwp.rda	1.789 kb	Data NPWP.pdf	1.789 kb	45,1 detik
4.	97851-data-nasabah.rda	1.023 kb	Data Nasabah.pptx	1.023 kb	25,7 detik
5.	48105-tugasakhir.rda	8.329 kb	Tugas Akhir.docx	8.329 kb	173,1 detik

4. KESIMPULAN

Setelah melakukan analisis, perancangan, dan uji coba program aplikasi kriptografi, dapat disimpulkan bahwa penelitian berhasil mengimplementasikan Algoritma kriptografi *Advanced Encryption Standard* (AES-128) di aplikasi pengamanan file berbasis web di PT Asuransi Central Asia. Implementasi ini dilakukan dengan menggunakan metodologi *Waterfall* dan metode pengujian *Blackbox Testing*.

Dalam pengujian, terlihat bahwa waktu yang dibutuhkan untuk melakukan proses enkripsi dan dekripsi berbanding lurus dengan ukuran file yang sedang diproses. Dengan kata lain, Proses enkripsi dan dekripsi akan berlangsung lebih cepat jika ukuran file yang sedang dienkripsi atau didekripsi semakin kecil. Namun, jika ukuran *file* semakin besar, waktu yang diperlukan untuk proses enkripsi dan dekripsi juga akan meningkat.

DAFTAR PUSTAKA

[1] D. Widyawan and I. Imelda, "Pengamanan File Menggunakan Kriptografi Dengan Metode Aes-128 Berbasis Web Di Komite Nasional Keselamatan Transportasi," *Skanika*, vol. 4, no. 1, pp. 15–22, 2021, doi: 10.36080/skanika.v4i1.2216.

[2] R. Nuari and N. Ratama, "Implementasi Algoritma Kriptografi AES (Advanced Encryption Standard) 128 Bit Untuk Pengamanan Dokumen Shipping," *J. Artif. Intell. Innov. Appl.*, vol. 1, no. 2, pp. 2716–1501, 2020, [Online]. Available: http://openjournal.unpam.ac.id/index.php/JOAIIA.

[3] S.- Sallu and Q. Qammaddin, "Keamanan Data Pembelajaran Online Jaringan Komputer Di Perguruan Tinggi," *Instruksional*, vol. 2, no. 1, p. 35, 2020, doi: 10.24853/instruksional.2.1.35-40.

[4] Yusfrizal, "Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper Dan Rsa Berbasis Android," *J. Tek. Inform. Kaputama*, vol. 3, no. 2, pp. 29–37, 2019.

[5] M. Ziaurrahman, E. Utami, and F. W. Wibowo, "Modifikasi Kriptografi Klasik Vigenere Cipher Menggunakan One Time Pad Dengan Enkripsi Berlanjut," *J. Inform. dan Teknol. Inf.*, vol. 4, no. 1, p. (halaman 2), 2019.

[6] H. Wijaya, "Implementasi Kriptografi AES-128 Untuk Mengamankan URL (Uniform Resource Locator) dari SQL Injection," *Akad. J.*, vol. 17, no. 1, pp. 8–13, 2020.

[7] P. Data, "IMPLEMENTASI ALGORITMA AES DAN RC4 TERHADAP KEAMANAN DATA PRODUK BENIH SAYURAN DI PT . EWINDO Raja Sari Novica Aswita , Indra Gunawan , Zulaini Masruro Nasution , Sumarno , Heru Satria Tambunan *STIKOM* Tunas Bangsa Pematangsiantar Diterima : Direvisi : Dis," vol. 1, pp. 461–468, 2021.

[8] Y. Yanuardi and A. A. Permana, "Rancang Bangun Sistem Informasi Keuangan Pada Pt. Secret Discoveries Travel and Leisure Berbasis Web," *JIKA (Jurnal Inform.*, vol. 2, no. 2, 2019, doi: 10.31000/.v2i2.1513.

[9] M. Azhari, D. I. Mulyana, F. J. Perwitosari, and F. Ali, "Jurnal Pendidikan Sains dan Komputer Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES) *Jurnal Pendidikan Sains dan Komputer*," vol. 2, no. 1, pp. 163–171, 2022.

[10] D. Nurnaningsih and A. A. Permana, "Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (Aes)," *J. Tek. Inform.*, vol. 11, no. 2, pp. 177–186, 2018, doi: 10.15408/jti.v11i2.7811.