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

IMPLEMENTASI ALGORITME AES 128 BERBASIS WEB DALAM PROYEK PEMBANGUNAN PERUMAHAN ANGGANA SENTUL PT. ADHI KARYA

Muchammad Faisal Nu'man[1*], Reva Ragam Santika[2]

[1,2]Program Studi Teknik Informatika, Fakultas Teknologi Infomasi, Universitas Budi Luhur, Jakarta, Indonesia

Email: [1*]1711503068@student.budiluhur.ac.id, [2*] reva.ragam@budiluhur.ac.id
(* : *corresponding author*)

Abstrak-Pada era digitalisasi adanya kemajuan pesat dalam teknologi informasi dan telekomunikasi, semua orang sangat bisa untuk bertukar informasi dengan mudah dan efisien. Ini sangat penting untuk bisnis dan organisasi. Manfaat teknologi ialah untuk mengolah serta bertukar data dapat membawa risiko bagi pengguna yang tidak mengerti tentang keamanan data. Oleh karena itu, diperlukan teknologi keamanan data yang dapat melindungi data dari penyalahgunaan oleh pihak-pihak yang tidak bertanggung jawab, dan salah satu solusinya adalah melalui sistem enkripsi. Data yang digunakan dalam penelitian ini meliputi data RAB, dan Penawaran RAB yang berupa dokumen dari PT. Adhi Karya (Persero) Tbk. Sumber data ini diperoleh langsung oleh peneliti dari sumbernya sendiri tanpa melibatkan pihak ketiga, dengan cara mengumpulkan data asli langsung dari responden. Dalam proses pengujian keamanan *file*, digunakan metode *Advanced Encryption Standard* 128-Bit (AES 128-Bit). Penggunaan algoritma enkripsi AES telah berhasil diimplementasikan pada aplikasi keamanan *file* berbasis web di PT. Adhi Karya (Persero) Tbk. Waktu yang dibutuhkan untuk melakukan proses enkripsi dan dekripsi sebanding dengan ukuran *file* yang diproses, sehingga semakin kecil *file* yang diproses maka semakin cepat proses enkripsi dan dekripsi yang dilakukan. Namun, ukuran *file* menjadi lebih besar, maka semakin lama waktu yang dibutuhkan untuk melakukan enkripsi dan dekripsi. Hasil penelitian menunjukkan bahwa analisis perancangan, pembuatan, dan pengujian program aplikasi kriptografi dapat menggunakan Kriptografi AES 128 dalam aplikasi dimana berhasil mengamankan dokumen pada proyek pembangunan perumahan Anggana Sentul PT. Adhi Karya (Persero) tbk.

Kata Kunci: Kriptografi, aes-128, *file*, *advanced encryption standard*, keamanan data

IMPLEMENTATION OF WEB-BASED AES 128 ALGORITHM FOR ANGGANA SENTUL HOUSING DEVELOPMENT PROJECT PT. ADHI KARYA

Abstract-*In the era of digitalization of rapid advances in information and telecommunications technology, everyone is very able to exchange information easily and efficiently. This is very important for businesses and organizations. The benefit of technology is that processing and exchanging data can bring risks for users who do not understand about data security. Therefore, data security technology is needed that can protect data from misuse by irresponsible parties, and one solution is through an encryption system. The data used in this study includes RAB data, and RAB Offers in the form of documents from PT. Adhi Karya (Persero) Tbk. This data source is obtained directly by researchers from their own sources without involving third parties, by collecting original data directly from respondents. In the process of testing file security, the Advanced Encryption Standard 128-Bit (AES 128-Bit) method is used. The use of AES encryption algorithm has been successfully implemented in web-based file security applications at PT. Adhi Karya (Persero) Tbk. The time needed to carry out the encryption and decryption process is proportional to the size of the file processed, so the smaller the file processed, the faster the encryption and decryption process is carried out. However, the larger the file size, the longer it takes to encrypt and decrypt. The results showed that the analysis of designing, creating, and testing cryptographic application programs can use AES 128 Cryptography in applications that successfully secure documents in the Anggana Sentul housing development project of PT. Adhi Karya (Persero) Tbk.*

Keywords*: Cryptography, aes-128, file, advanced encryption standard, data security*

1. PENDAHULUAN

Di era ini teknologi sudah menjadi kebutuhan manusia, yang mana dengan perkembangan yang ada dapat memudahkan manusia untuk menyelesaikan permasalahan yang ada [1]. Kriptografi adalah salah satu bidang pengembangan teknologi informasi untuk mengamankan data atau pesan bersifat pribadi dan rahasia [2]. Untuk menjaga kerahasiaan dan integritas dokumen tersebut, diperlukan penggunaan algoritma enkripsi yang kuat. Salah satu algoritma enkripsi yang paling popular dan terkenal adalah Advanced Encryption Standard 128 (AES 128). *Advanced Encryption Standard* (AES) menggantikan *Standard Data Encryption* (DES). Salah satu yang paling

penting dalam teknologi informasi bagaimana data tersebut aman tersimpandengan baik, mudah diakses serta faktor yang tidak kalah penting adalah keamanan data itu sendiri [3]. Dipilihnya algoritma AES (Advanced Encryption Standard) karena dirancang khusus untuk keamanan tingkat tinggi serta ketahanan terhadap berbagai jenis serangan, bahkan kesederhanaan rancangan, kekompakan kode dan kecepatan men-enkripsi dan deskripsi setiap *file* atau data [4].

Tujuan dari penggunaan AES128 berbasis web untuk mengamankan dokumen proyek pembangunan perumahan Anggana Sentul PT. Adhi Karya (Persero) tbk adalah untuk memastikan bahwa dokumen proyek tersebut disimpan dan dikirim dengan aman. Kriptografi, menurut [5], adalah bidang yang menyelidiki metode matematika yang berkaitan dengan keamanan data dan informasi, seperti autentikasi, integritas, dan keabsahan data. Untuk mengamankan dokumen proyek, AES128 berbasis web diharapkan dapat menggunakan temuan penelitian sebelumnya dan teknik yang telah teruji untuk memaksimalkan keamanan dokumen proyek, termasuk informasi rahasia dan data penting. Dalam prosesnya, informasi sensitif ini akan dilindungi sepenuhnya, memberikan kepercayaan.

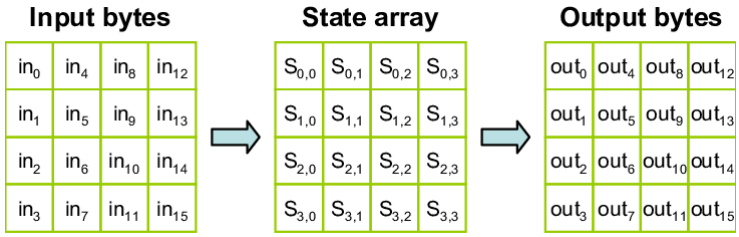
Penelitian ini menggunakan teori keamanan data dan teori kriptografi. Lebih lanjut, keamanan data merupakan keadaan yang menunjukkan bahwa segala sesuatunya aman. Keamanan sistem informasi adalah komponen yang sangat penting. Perancang dan manajer sistem informasi sering mengabaikan masalah keamanan. Masalah keamanan sering berada di urutan setelah tampilan atau bahkan di urutan terakhir dalam daftar hal – hal yang dianggap penting. Seringkali, kata “keamanan” dan “proteksi” digunakan untuk merujuk pada hal yang sama: “keamanan” mengarah pada seluruh masalah keamanan, dan “mekanisme proteksi” mengacu pada mekanisme sistem yang digunakan untuk melindungi informasi yang terkandung dalam sistem komputer [6].

Adapun salah satu teori yang dikemukakan oleh Menezes bahwa kriptografi adalah sebuah ilmu yang membahas teknik matematis yang berkaitan dengan topik keamanan informasi. *Advanced Encryption Standard* (AES), sebuah algoritma kriptografi, adalah blok chipertext simetrik yang dapat mengenkripsi (*encipher*) dan dekripsi (*decipher*). Kriptografi adalah bidang yang menyelidiki metode matematika yang berkaitan dengan elemen keamanan informasi seperti kerahasiaan, integritas, otentikasi, dan anti penyangkalan. Kriptografi juga dapat didefinisikan sebagai bidang yang mempelajari cara menjaga kerahasiaan informasi dengan menggunakan metode seperti kerahasiaan, integritas, dan autentikasi. Keamanan informasi merupakan hal yang paling penting yang tidak boleh bocor ke publik atau segelitir orang, jika informasi ini bocor maka akan merugikan bagi penerima dan pengirim informasi [7]. Berdasarkan dari penelitian, diharapkan dapat melindungi data berupa *file* dan *file* perusahaan dengan keamanan yang tinggi, waktu yang cepat dan efisien sehingga tidak perlu khawatir atas kebocoran data maupun pencurian data penting pada perusahaan oleh pihak yang tidak memiliki wewenang [8]. Sebenarnya, kriptografi adalah penelitian tentang metode matematis yang berkaitan dengan fitur keamanan sistem informasi, seperti kerahasiaan, integritas data, autentikasi, dan ketiadaan penyangkalan. Salah satu algoritma kriptografi yang dapat digunakan untuk mengamankan data adalah *Advance Encryption Standard* (AES). Kriptografi dilakukan dengan dua tahap yaitu proses enkripsi dan dekripsi [9]. Kunci kriptografi 128, 192, dan 256 bit digunakan dalam algoritma AES untuk mengenkripsi dan dekripsi data [10]. Ketiga varian panjang kunci AES terletak pada jumlah putaran (*rounds*) yang dapat dilihat pada tabel 1 berikut:

Tabel 1 *Advanced Encryption Standard*

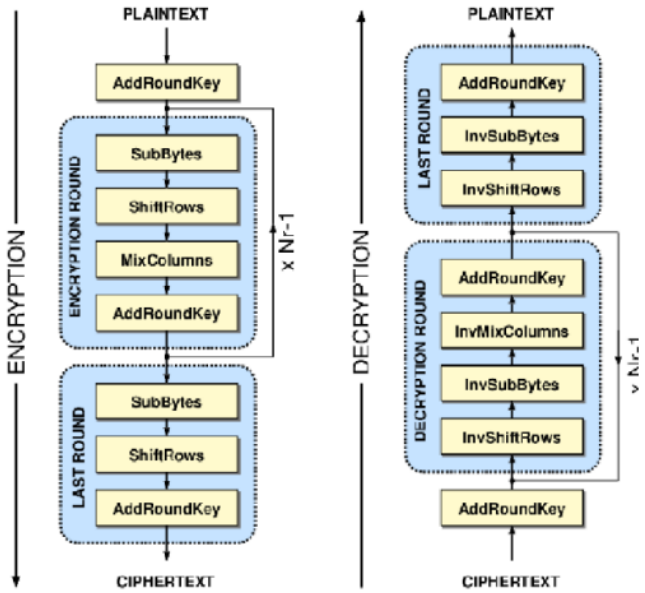
	Panjang Kunci	Panjang Blok	Jumlah Putaran
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Pada Tabel 1 Menjelaskan jenis algoritma AES dengan Panjang kunci, panjang blok, dan jumlah putaran yang berbeda, Sepuluh putaran bit AES-128 digunakan untuk penelitian ini. Ada empat transformasi putaran dalam proses enkripsi dan dekripsi, yaitu *SubBytes*, *ShiftRowns*, *MixColumn*, dan *AddRoundKey* [10].



Gambar 1 Transformasi

Dari Gambar 1 terlihat AES memiliki struktur dasar yang di sebut sebagai *array of bytes* dengan dua dimensi yang disebut *state*. Ukuran dari *state* ditentukan oleh parameter NROWS (jumlah baris) dan NCOLS (jumlah kolom). *State* ini merupakan tempat di mana proses enkripsi dan dekripsi dilakukan, dan hasilnya akan disimpan kembali ke dalam *array of state.* Proses enkripsi melibatkan transformasi *AddRoundKey*, *SubBytes, ShiftRows, MixColumns,* dan *AddRoundKey* secara berulang sesuai dengan jumlah putaran (Nr). Pada putaran terakhir, tidak dilakukan transformasi *MixColumns*. Hasil enkripsi disimpan dalam *output bytes*. Gambar 2 memberikan ilustrasi visual tahap awal enkripsi menggunakan AES128.



Gambar 2 Enkripsi dan Dekripsi

2. METODE PENELITIAN

2.1 Data Penelitian

Data yang digunakan pada penelitian ini adalah Tabel 2 yaitu data Rencana Angaran Biaya (RAB) dan beberapa data penting lainnya dari PT. Adhi Karya (Persero) tbk. Penelitian mengumpulkan data ini secara langsung dari sumbernya tanpa melibatkan pihak ketiga, dengan melakukan penggalian langsung dari responden ke sumber asli. Data yang diperoleh digunakan dalam pengujian kemanan *file* dengan menerapkan metode *Advanced Encryption Standard 128Bit* (AES-128).

Tabel 2 Data Penelitian

Nama *File*	Ukuran *File*	Jenis *File*
RAB	12MB	.xlsx
Penawaran RAB	118kb	.pdf

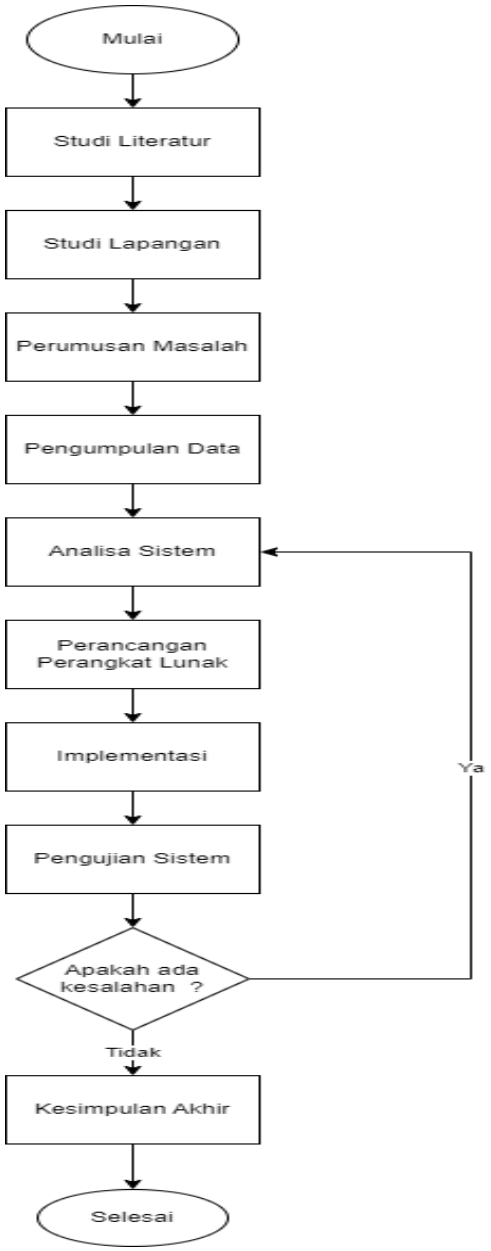
2.2 Metode Pembanding

Penelitian ini membandingkan penggunaan dua metode enkripsi dalam mengamankan *file*, yaitu algoritma kriptografi AES-128 yang digunakan dalam penelitian inim dengan metode algoritma RC4. Perbandingan antara kedua metode tersebut adalah sebagai berikut:

a. Tingkat kemananan antara AES dengan RC4
b. AES memiliki algoritma yang lebih kompleks, sedangkan enkripsi dengan RC4 relatif lebih sederhana.
c. AES menggunakan panjang kunci 128, 192 dan 256 bit, sementara RC4 menggunakan panjang kunci 64 bit dan 128 bit.

2.3 Penerapan Metode

Metode penelitian ini berfungsi sebagai pedoman untuk melakukan penelitian untuk mencapai tujuan. Gambar 3 menunjukkan proses yang akan dilakukan untuk menerapkan metode dalam penelitian ini.



Gambar 3 Tahapan Penelitian

2.4 Rancangan Tes

Algoritma kriptografi *Advanced Encryption Standard* 128 (AES128) akan digunakan untuk menjalankan pengujian. Aplikasi ini akan membuat menu login di mana orang harus memasukkan *username* dan *password* mereka saat ingin menggunakannya. Setelah masuk ke akun, pengguna akan langsung dibawa ke menu dashboard, yang berisi informasi tentang informasi PT. Adhi Karya (Persero) Tbk. Di bagian bawah halaman, ada tombol menu yang menampilkan submenu, yang memiliki tombol untuk enkripsi, deskripsi, dan daftar berkas. Tombol enkripsi dapat digunakan untuk memulai enkripsi *file* tertentu, dan tombol dekripsi dapat digunakan untuk

mendekripsi *file* yang telah dienkripsi sebelumnya. Tombol *History* untuk melihat hasil *file* yang sudah dienkripsi atau didekripsi dan didalam daftar berkas juga bisa mengunduh hasil enkripsi dan dekripsi. Menu *logout* jika di klik, maka akan langsung diarahkan kembali ke halaman *login*.

Pada penelitian ini penulis menggunakan *blackbox Testing* untuk proses pengujian pada program (Tabel 3), dimana dilakukan dengan mengamati hasil eksekusi menggunakan data uji perangkat lunak dan uji fungsional.

Tabel 3 Rancangan Pengujian

No.	Kasus Uji	Hasil yang diharapkan
1.	Tombol Masuk	Tampil halaman menu *dashboard*
2.	Tombol Enkripsi	Menampilkan tampilan halaman Enkripsi
3.	Tombol *Choose File*	Memilih *file* yang ingin dienkripsi
4.	Tombol Ekripsi Berkas	Dapat Mengenkripsi berkas yang sudah di*upload*
5.	Tombol Dekripsi	Menampilkan tampilan halaman Enkripsi
6.	Tombol Dekripsi Berkas	Dapat Mengdekripsikan berkas yang sudah di*upload*
7.	Tombol *History*	Menampilkan *File* yang sudah dienkripsi / dekripsi
8.	Tombol *Logout*	Kembali ke halaman *login*

2.5 Rancangan Basis Data

Desain basis data mencakup diagram kelas, *logical record structure* (LRS), dan spesifikasi basis data. Penelitian ini menggunakan diagram kelas. Diagram kelas menjelaskan struktur dan hubungan antar objek dalam aplikasi Anda. Struktur ini berisi atribut dan metode kelas..

2.6 Konsep Menu

Beberapa halaman yang dibuat oleh program ini termasuk halaman login, halaman menu mulai, halaman menu *file* dengan submenu enkripsi dan dekripsi, dan halaman menu daftar *file*. Di halaman login, pengguna harus memasukkan *username* dan *password* mereka sebelum dapat melanjutkan ke tugas lain dalam aplikasi.

Untuk melakukan enkripsi *file*, pengguna harus mengisi semua informasi yang diperlukan, termasuk *file* yang akan dienkripsi, kapasitas aplikasi, *password*, dan keterangan. Setelah itu, mereka dapat memilih opsi "enkripsi *file*" untuk memulai proses enkripsi. Namun, untuk mengembalikan *file* yang sudah terenkripsi ke keadaan aslinya, pengguna dapat memilih submenu dekripsi pada status. Ini akan mengarahkan pengguna ke data yang akan didekripsi, dengan hanya memasukkan kata sandi untuk dekripsi dan memilih opsi "dekripsi *file*". Setelah itu, program akan memproses pengembalian data ke keadaan aslinya.

3. HASIL DAN PEMBAHASAN

3.1 Tempat Percobaan

Perangkat lunak dan perangkat keras yang digunakan dalam lingkungan laboratorium penelitian ini membantu melakukan penelitian dan merancang aplikasi. Lingkungan percobaan yang digunakan untuk penelitian ini adalah sebagai berikut:

a. Spesifikasi Perangkat Keras, perangkat yang digunakan untuk mendukungnya jalan suatu sistem aplikasi ini secara maksimal yaitu Processor Intel Core i3-6100U CPU @ 2.30GHz 2.30 GHz, RAM 4Gb, dan HardDisk 1Tb.
b. Spesifikasi Perangkat Lunak, perangkat lunak yang digunakan untuk mendukung jalannya suatu sistem aplikasi secara maksimal yaitu Operating System Windows 10, Visual Studio Code, XAMPP, dan Chrome.

3.2 Proses Kerja dari AES 128

Berdasarkan pendekatan metodelogi yang telah diuraikan pada bab sebelumnya, peneliti menerapkan algoritma kriptografi AES 128 untuk melindungi keamanan data termasuk RAB dan Penawaran RAB.

a. Untuk memulai proses enkripsi, orang harus menemukan menu enkripsi di submenu berkas. Kemudian, mereka harus memilih *file* yang ingin dienkripsi. Setelah memilih *file*, mereka harus memasukkan sandi dan keterangan untuk *file* tersebut.
b. Proses Dekripsi, untuk memulai proses dekripsi, pengguna harus masuk ke sub menu enkripsi, kemudian pengguna dapat memilih berkas yang ingin didekripsi dengan menekan tombol Dekripsi berkas, kemudian akan diarahkan ke halaman Dekripsi Berkas, dihalaman tersebut pengguna disuruh memasukan sandi yang

sudah di masukan di *form* enkripsi, untuk mendekripsi pengguna bisa menekan tombol dekripsi berkas dan pengguna juga bisa mengunduh berkas yang sudah dienkripsi dengan menekan tombol *download* berkas

3.3 *Flowchart*

Flowchart atau bagan alir adalah diagram yang menunjukkan langkah – langkah dan keputusan yang terlibat dalam menjalankan proses suatu program. Setiap Langkah yang ditampilkan dalam bentuk diagram dan dihubungkan dengan garis atau panah. Ada beberapa jenis *flowchart* sebagai berikut:

a. *Flowchart Login*, sebelum menggunakan aplikasi ini, pengguna harus mengisi form login terlebih dahulu dengan memasukkan *username* dan *password*. Jika *username* atau *password* salah akan kembali ke *form login* dan jika benar akan masuk ke halaman beranda.
b. *Flowchart Algoritma Enkripsi, proses enkripsi yang terjadi pada sistem aplikasi dapat di lihat seperti Gambar. Pengguna dapat memberikan kunci dan file dokumen yang dienkripsi ke sistem saat program dimulai. Proses AddRoundKey akan berjalan kemudian. Dalam langkah perama proses enkripsi, transformasi AddRoundKey adalah round = 0 kemudian round = round + 1. Sistem kemudian memproses SubByte, ShiftRows, MixColumns, dan AddRoundKey untuk putaran pertama. Nr(round) tetap sama dengan Nr-1 dan pada AES ada 10 putaran. Ketika jumlah putaran yang diminus satu atau mencapai 0 putaran, sistem melanjutkan proses untuk putaran terakhir yang tersisa.*
c. *Algoritma Flowchart Dekripsi: Proses dekripsi dimulai dengan putaran = 10 dan kemudian putaran = -1. Sistem kemudian melakukan putaran pertama dan memproses InvShiftRows, InvSubByte, AddRoundKey, dan InvMixColumns. Proses ini diulang sampai Nr (putaran) cocok dengan Nr1 untuk AES. Ketika jumlah putaran berkurang satu atau mencapai 0 putaran, sistem melanjutkan proses putaran terakhir yang terdiri dari InvShiftRows, InvSubByte, dan AddRoundKey.*
d. *Flowchart halaman enkripsi file, yang menjelaskan cara mengengkripsi file dengan flowchart.*
e. *Flowchart Halaman Dekripsi File, flowchart halaman dekripsi file. Flowchart ini menjelaskan cara dekripsi file. Saat mendekripsi file, pengguna harus memasukkan sandi yang cocok dengan kata sandienkripsi file*. Kemudian program akan melakukan dekripsi

3.4 Pengujian

Pengujian aplikasi ini adalah proses penelitian untuk mengetahui hasil dari sistem aplikasi pengamanan. Pengujian ini dilakukan melalui dua proses pemrosesan: proses enkripsi dan dekripsi *file*.

a. Proses Pengujian Enkripsi, berikut adalah proses pengujian enkripsi yang dijabarkan dalam tabel 4.

Tabel 4 Uji Enkripsi

No.	Nama Asli *File*	Ukuran*File* Asli (kb)	Nama *File*Setelah Enkripsi	Ukuran *File* Cipher (kb)	Waktu (detik)
1.	REKAP RAB ANGGANA VILAGE T95_R1 (NEGO HARGA)_Kirim.xlsx	227 kb	23126-rekap-rab-anggana-vilage-t95_r1-(nego-harga)_kirim.rda	226.654 KB	2.9497 Detik
2.	PENAWARAN CIBINONG, 72 R1.pdf	181 kb	84335-penawaran-cibinong,72-r1.rda	180.54 KB	2.3512 Detik

b. Proses Pengujian Dekripsi, berikut ini adalah proses pengujian dekripsi yang dijabarkan dalam tabel 5.

Tabel 5 Uji Dekripsi

No.	Nama Asli *File*	Ukuran *File* Asli (kb)	Nama *File*Setelah Dekripsi	Ukuran *File* Plain (kb)	Waktu (detik)
1.	23126-rekap-rab-anggana-vilage-t95_r1-(nego-harga)_kirim.rda	226.654 KB	63020-rekap-rab-anggana-vilage-t95_r1-(nego-harga)_kirim.xlsx	226.654 KB	2.9497 Detik
2.	84335-penawaran-cibinong,72-r1.rda	180.54 KB	31855-penawaran-cibinong,72-r1.pdf	180.54 KB	2.4105 Detik

c. Hasil Rancangan Pengujian Program, berikut ini adalah hasil rancangan pengujian program yang ditunjukkan pada tabel 6.

Tabel 6 Uji Program

No	Skenario Tes	Hasil Yang Diinginkan	Hasil Tes
1.	*User* memasukkan form *login.*	Menampilkan halaman menu *dashboard*	Memenuhi harapan
2.	*User* menekan submenu *file* enkripsi	Menampilkan halaman sub menu enkripsi	Memenuhi harapan
3.	*User* menekan sub Menu *file* dekripsi	Menampilkan halaman sub menu dekripsi	Memenuhi harapan
4.	Memasukkan *file* dan menekan tombol untuk dienkripsi atau didekripsi	Menampilkan halaman hasil proses enkripsi atau dekripsi *file*	Memenuhi harapan
5.	Men*download file* yang sudah terenkripsi dan terdekripsi	Berhasil men*download file*	Memenuhi harapan
6.	*User* memilih submenu daftar *file*	Menampilkan halaman daftar berkas yang sudah terenkripsi dan yang belum terenkripsi atau tampil halaman hapus *file*	Memenuhi harapan
7.	*User* meng-klik Hapus *file*	Menampilkan halaman *file* terhapus	Memenuhi harapan
8.	*User* meng-klik tombol *logout*	Menamoilkan kembali ke halaman *login*	Memenuhi harapan

3.5 Analisis Hasil Uji Coba Program

Berdasarkan tes program yang telah dilakukan terhadap program aplikasi tersebut terdapat kelebihan dan kekurangan. Kelebihan aplikasi berdasarkan uji coba program adalah sebagai berikut:

a. Karena berbasis web, program aplikasi ini dapat diakses dengan mudah.
b. Tampilan program aplikasi ini ramah pengguna, sehingga sangat mudah dan nyaman digunakan.
c. Ukuran berkas yang dienkripsi tidak mengubah ukuran dengan berkas aslinya.
d. Berkas yang telah dienkripsi tidak bisa dibaca dan dibuka sebelum berkas tersebut didekripsi seperti awal.
e. Isi berkas dari dekripsi tidak mengalami perubahan sedikit pun hasilnya sama seperti dengan *file* asli
f. Untuk melakukan enkripsi dan dekripsi *file* tidak menggunakan internet.

Berdasarkan uji coba program, didapatkan kekurangan aplikasi sebagai berikut:

a. Program aplikasi ini tidak bisa melampirkan berkas lebih dari 3 MB.
b. Semakin besar ukuran berkas yang akan dienkripsi, maka makin lama pula proses untuk melakukan enkripsi.
c. Program aplikasi masih menggunakan tampilan yang sederhana.

3.6 Tampilan Layar

Bagian ini menjelaskan tampilan layer aplikasi pengamanan *file* PT.Adhi Karya (Persero) Tbk berdasarkan rancangan layar yang sudah dibuat sebelumnya.

a. Login, saat Anda pertama kali mengakses *website*, ini adalah tampilan yang akan Anda lihat pada halaman informasi login. dimana orang harus memasukkan *username* dan *password* mereka untuk mengakses *website*.
b. Beranda, Berikut ini adalah tampilan halaman Beranda, yang menampilkan jumlah pengguna, jumlah data yang dienkripsi, dan data yang didekripsi.
c. Menu, Tampilan menu berada di sebelah kiri, menampilkan menu yang ada di *website* ini, yang bisa diakses pengguna jika sudah login ke dalam *website*.
d. Halaman Enkripsi, Di halaman ini menampilkan halaman enkripsi dimana jika pengguna ingin mengenkripsi *file*. Mereka harus memasukan *file*nya dan juga kata kunci dan keterangan yang nantinya kata kunci tersebut dipakai untuk meng dekripsikan *file*-nya kembali.
e. Halaman Dekripsi, Di halaman ini menampilkan halaman dekripsi dimana jika pengguna ingin mengdekripsi *file*. Mereka tinggal memilih *file* apa yang ingin mereka dekripsi dan memasukan kata kunci enkripsinya.

4. KESIMPULAN

Berdasarkan analisis yang telah dilakukan terhadap masalah yang ada dalam program aplikasi yang telah dibuat, dapat diambil kesimpulan dan saran yang berpotensi untuk memperbaiki dan mengembangakan aplikasi ke tahap yang lebih baik di masa depan. Dari analisis perancangan, pembuatan, dan pengujian program aplikasi kriptografi dapat disimpulkan bahwa dengan menggunakan Kriptografi AES 128 dalam aplikasi ini penulis berhasil mengamankan dokumen pada proyek pembangunan perumahan Anggana Sentul PT. Adhi Karya (Persero) tbk. Selanjutnya adalah aplikasi harus memiliki kemampuan untuk mengenkripsi dokumen proyek menggunakan algoritma AES 128, yang akan mengubah dokumen menjadi bentuk yang tidak dapat dibaca tanpa kunci rahasia yang tepat. Aplikasi juga harus memiliki kemampuan dekripsi, yang memungkinkan pengguna mendekripsi dokumen kembali ke bentuk aslinya menggunakan kunci yang tepat.

Adapun beberapa saran untuk meningkatkan pengembangan program aplikasi enkripsi dan dekripsi berbasis web yaitu: (1) perlu dilakukan pengembangan sistem agar dapat memproses tidak hanya dokumen teks, tetapi juga dokumen video dan audio; (2) perlu dilakukan pengembangan sistem yang menggunakan AES192 atau AES258, yang akan meningkatkan tingkat keamanan dan membuat sulit bagi pihak yang tidak bertanggung jawab untuk mencuri data; dan (3) perlu dilakukan pengembangan sistem yang lebih lanjut untuk menguji algoritma AES dalam pengembangan aplikasi dari perspektif Android *native*, iOS, dan *hybrid*.

DAFTAR PUSTAKA

[1] Firdaus R, Santika R., "Penerapan Algoritma AES-128 Untuk Enkripsi Dokumen Di PT Caveo Biometric Security", Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI), 2022.

[2] Hermawan A, Ujianto H., "Implementasi Enkripsi Data Menggunakan Kombinasi AES dan RSA", *Jurnal Nasional Informatika dan Teknologi*, Vol. 5(2), Hal. 325-330, 2021

[3] Noprianto N, Wijayaningrum V, & Ariyanto R., Pemanfaatan AES dengan Key Dinamis sebagai Metode Pengamanan Data pada Smart Card", *Sistemasi: Jurnal Sistem Informasi*, Vol. 10(3), Hal. 575-585, 2021.

[4] Nuari, Rivian & Ratama, Niki., "Implementasi Algoritma Kriptografi AES (Advanced Encryption Standard) 128 Bit Untuk Pengamanan Dokumen Shipping", *Journal of Artificial Intelligence and Innovative Applications*. Vol. 1, No. 2, 2020.

[5] Pratomo, D., Nugroho, N. B., & Ginting, R. I., "Implementasi Kriptografi Untuk Mengamankan Data Penjualanan Di PT. Papparich Medan Menggunakan Metode AES 128", *Jurnal Cyber Tech*, 2021, https://ojs.trigunadharma.ac.id/index.php/jct/article/view/4371

[6] Rismaya M, Sakti D., "Penerapan Algoritma Aes128 Dan Rc4 Untuk Pengamanan Database Dan File Pada PT. Mayaksa Mugi Mulia", Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI), 220-229, 2022.

[7] Saputra Djong H, Siswanto S., "Implementasi Kriptografi Dengan Menggunakan Metode RC4 Dan AES-256 Untuk Mengamankan File Dokumen Pada PT Varnion Technology Semesta", Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI), 2022.

[8] Silalahi, L., & Sindar, A., "Penerapan Kriptografi Keamanan Data Administrasi Kependudukan Desa Pagar Jati Menggunakan SHA-1", *Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)*, 3(2), 2020, https://doi.org/10.32672/jnkti.v3i2.2413

[9] Ungkawa U, Rosmala D, & Fauzi H., "Penerapan Advance Encryption Standart dalam Pengamanan Elektronik Voting", *Journal of Information Technology*, Vol. 3(1), 2021

[10] Wijaya, H., "Implementasi Kriptografi AES-128 Untuk Mengamankan URL (Uniform Resource Locator) dari SQL Injection", *Akademika Jurnal*, 17(1), 8–13, 2020.