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 *ADVANCED ENCRYPTION STANDARD* 128 UNTUK MENGAMANKAN FILE DOKUMEN PT. ANTARA PERSADA SUKSES

Arfian Nur Ikhsan[1*], Dewi Kusumaningsih[2]

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

Email: [1*]arfian718@gmail.com, [2]dewi.kusumaningsih@budiluhur.ac.id,
(* : correspondingauthor)

Abstrak- Pada perkembangan teknologi yang berkembang saat ini, sering terjadinya pencurian atau peretasan data. Maka faktor utama masalah pada penelitian ini untuk mencegah adanya pencurian atau peretasan data dan masalah pada saat pengiriman data itu sendiri. Pengamanan file menggunakan metode algoritme *Advanced Encryption Standard* 128. hasil pengujian program waktu yang dibutuhkan saat mengenkripsi file dengan ukuran 246kb dengan type data xlsx membutuhkan waktu 0,67 detik, Proses dekripsi dengan file dan ukuran yang sama membutuhkan waktu 0,32detik.jika data yang akan di enkripsi melebihi dari 5mb maka akan terjadinya kegagalan pada proses enkripsi, besarnya suatu ukuran file makan akan lebih membutuhkan waktu yang lama. Proses enkripsi Pada *subytes* mentransformasikan byte dimana setiap elemen pada state akan dipetakan menggunakan table dengan tahapan mensubsitusikan, kemudian ada tahpan *shifrows* memindahkan byte dari kiri kekanan, lalu mengalikan setiap blok *cipher* dengan matrix akan menjadi *mix columns* yang digabungan pada colomn selanjutnya akan diproses dalam *addroundkey* pada round akhir dlm proses 3 tahapan tanpa melalui *mixcolum* yang akan menghasilkan *chipertext* terjadi kembali array 4x4 pada colum *addroundkey*. Proses dekripsi *Chipertext* hasil dari enkripsi yang masuk kedalam proses initial round menggunakan round key ke 10 pada tahapan *invshiftrows* / mengembalikan baris kedalam bentuk semula, yang dilanjutkan dengan *Invsubbyte* / memindahkan byte paling kiri ke kanan, setiap state dikalikan dengan matrix perkalian dengan pengembalian semua tahapan ke bentuk semula dengan menggabungkan kolom didalam round akhir akan menghasilkan plaint text, dan data dapat kembali dibaca.

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

IMPLEMENTATION OF ADVANCED ENCRYPTION STANDARD 128 ALGORITHM TO SECURE PT. ANTARA PERSADA SUKSES

Abstract- *In the development of technology that is developing at this time, it often happens data theft or hacking. Then the main factor is the problem in this study to prevent any data theft or hacking and problems at this point sending the data itself. File security uses an algorithmic method Advanced Encryption Standard 128. With the results of testing the program if the data which will be encrypted exceeds 5mb then there will be a failure on encryption process. Time taken when encrypting files with size 246kb with data type xlsx takes 0.67 seconds, equal to one file size will take longer. Process description with file and the same size takes 0.32sec. The encryption process is a process of changing files that previously could be read by doing encryption, the file will not be read. Process description performs returns previously unread files will be read. Encryption process In subbytes transforming bytes where each element in the state will be mapped using a table with stages of substituting, then there are stages of shifts moving bytes from left to right, then multiplying each cipher block with the matrix will become mix columns which are combined in the next column will be processed in the addroundkey on the final round in the 3-stage process without going through the mixcolum which will produce the ciphertext recurs the 4x4 array on the addroundkey column. The chipertext decryption process results from encryption that goes into the initial round process using the 10th round key at the invshiftrows stage / returns the row to its original form, followed by Invsubbyte / moves the leftmost byte to the right, each state is multiplied by the multiplication matrix by returning all stages to the original form by combining the columns in the final round will produce plain text, and the data can be read again*

Keywords*: cryptographic, encryption, decryption, Advanced Encryption Standard (AES-128).*

1. PENDAHULUAN

Pada perkembangan teknologi yang sangat pesat saat ini, sangatlah berpengaruh pada setiap permasahalan teknologi informasi[1]. Sehingga keamanan data menjadi salah satu yang paling penting dalam teknologi informasi agar penyimpanan file atau data yang bersifat rahasia tersebut menjadi aman dan tersimpan dengan baik.

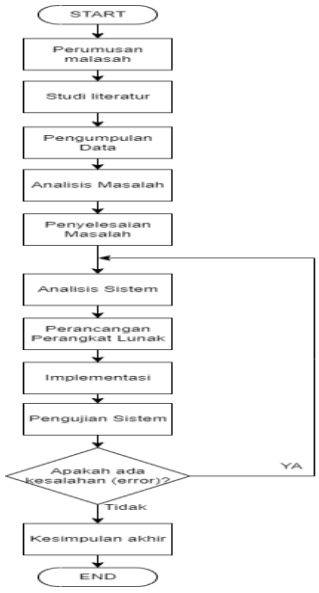
Dalam penelitian ini akan mengamankan data laporan keungan perusahaan, di dalam data laporan keungan perusahaan ada beberapa data yang akan di amankan. Jika data laporan keungan perusahaan mengalami pencurian atau kebocoran maka nantinya data tersebut akan menjadi perhitungan tersendiri bagi perusahaan yang bergerak di bidang yang sama. Kemanan di lakukan dengan cara mengenkripsi dan deskripsi file yang akan di amankan. Permasalahan yang ada pada saat ini masih menjadi perhatian pada rendahnya system keamanan file penting yang dimiliki oleh suatu instansi perusahaan.

Dengan seiring terjadinya kasus pencurian data dan rendahnya sistem keamanan file perusahaan maka pentingnya penyimpanan dan pengiriman file atau data dengan baik dan aman, untuk mencegah terjadinya suatu pencurian data yang terjadi di suatu perusahaan. untuk mengatasi permasalahan yang ada yaitu melakukan suatu perancangan sistem keamanan data untuk melindungi dan menjaga data infomasi tersebut berupa file dengan menggunakan teknik kriptografi. suatu proses yang akan di lakukan dalam kriptografi melakukan enkripsi dan dekripsi.proses enkripsi adalah proses dimana plaintext digabungkan dengan *chiperkey* dan ada tahapan selanjutnya seperti *Addroundkey*, *Subbyte*, *Shiftrows* dan *MixColumns* lalu file akan berubah menjadi *chipper text*[2]. Proses dekripsi adalah kebalikan daripada enkripsi itu sendiri tahapan saat melakukan proses enkripsi *Addroundkey*, *InvSubbyte, InvShiftrows* dan *InvMixColumns* setelah melalui tahapan proses dekripsi file akan kembali awal.

Penggunaan algoritme AES -128 didasarkan pada studi literature penelitan terdahulu yang berjudul "Implementasi Keamanan Data Gaji Karyawan Pada PT. Capella Medan Menggunakan Metode Advanced Encryption Standard (AES)"[3]. Yang berkaitan dengan penilitan yang pertama adalah bagaimana mengamankan suatu data atau file yang bersifat rahasia. Penelitian yang kedua berjudul "Implementasi Kriptografi Metode Advanced Encryption Standard(AES-128) Untuk Pengamanan File Pada Toko Sepatu Dessler.Id"[4]. Yang berkaitan dengan jurnal terdahulu kedua adalah dengan menggunakan metode Advanced Encryption Standard (AES-128). Penelitian yang ketiga berjudul "Analisa Metode Kriptografi Modern Advance Encryption Standard (AES) 128 Bit dalam Mengenkripsi dan Mendekripsi File Dokumen Digital"[5]. Yang berkaitan dengan jurnal terdahulu yang ketiga saat melakukan proses enkripsi file akan tidak dapat terbaca, lalu saat melakukan proses dekripsi file akan kembali ke semula.

2. METODE PENELITIAN

Metode penelitian ini menggunakan metode *waterfall*, yang dilakukan pertama kali adalah merumuskan masalah penelitian, sumber data yang lengkap dan terpercaya untuk memperoleh informasi yang diperlukan dalam memecahkan masalah yang ingin diselesaikan[6]. lalu selanjutnya melakukan studi literatur dengan membaca referensi penelitian yang terdahulu untuk menunjang hasil yang tidak menyimpang dari tujuan penelitian. Gambar 1. Menggambarkan Langkah – Langkah yang di ambil untuk menerapkan metode penelitian yang dilakukan pada penelitan ini.



Gambar 1. Tahapan Penelitian

a. Studi Literatur

Tahapan studi litreatur ini mengumpulkan sebuah jurnal atau penelitian yang terdahulu agar menjadi suatu acuan untuk melakukan suatu penelitian. Dengan mengutip kalimat penelitian penelitian terdahulu itu yang di sebut studi literatur. Jurnal harus sesuai topik dengan penelitian yang akan dibuat seperti jurnal *Advanced Encryption Standard*(AES-128).

b. Pengumpulan Data

1) Wawancara (*Interview*)

Wawancara ini dapat dilakukan dengan melakukan tanya jawab langsung antara pihak perusahaan dan pembuat program, agar nantinya mendapatkan informasi yang lebih lanjut tentang tentang aplikasi dan keamanan yang ada di perushaan tersebut.

2) Observasi (*Observation*)

Observasi ini dilaksanakan di perusahaan yang akan diteliti,yang bertujuan untuk mengetahui objek penelitian yang ada di perusahaan tersebut. Agar dapat mengetahui data – data apa saja yang akan di amankan di perusahaan tersebut..

c. Analisis sistem

1) Analisis Data

Analisis data salah satu tahapan dari analisis system untuk menyelesaikan permasalahan kemanan data,yang dilakukan pada analisis data ialah :

a) Mengumpulkan sebuah file untuk memperoleh data yang datanya akan dipergunakan untuk perancangan sebuah program.
b) Memisahkan sebuah file sesuai kebutuhan dan tipenya.
c) Mendeskripsikan file yang yang di gunakan untuk membangun sebuah aplikasi.

2) Analisis Penerapan Algoritme

Langakah selanjutnya ialah Analisis Penerapan Algoritme mendeskripsikan tahapan untuk melengkapi metode kriptografi *Advanced Encryption Standard* (AES).Tahapan ini dilakukan :
Menentukan kunci yang akan digunakan dalam proses enkripsi dan dekripsi *file*.

a) Proses enkripsi file menggabungkan antara kunci enkripsi dan *plaintext*, yaitu proses mengubah file yang akan dienkripsi menjadi ciphertext dengan menggunakan kunci enkripsi tersebut.
b) Proses dekripsi ciphertext menggunakan kunci dekripsi yang sebelumnya telah di buat saat melakukan proses enkripsi, yaitu proses mengubah ciphertext menjadi file ke awal semula yang dapat terbaca kembali (*plaintext*).

3) Analisis Sistem

Analisis system ini melakukan pengimplementasian pengamanan yang ada pada proses enkripsi yang nantinya file akan disimapan pada basis data.proses enkripsi ini dilakukan agar data yang penting terjaga dari pihak-pihak yang tidak bertanggung jawab data tersimpan dalam database.

d. Perancangan Perangkat Lunak

Tahapan ini dilakuakan pada sebuah perancangan yang sesuai dengan analisis system yang ada pada perancangan enkripsi dan dekripsi, yang di dukung dengan aplikasi dan user interface.

Proses pengembangan sistem ini menggunkan metode *waterfall*,dengan menggunakannya metode waterfall ini cara penyelesaiannya ialah menyelesaikan secara satu persatu dengan tuntas.Agar hasil dari masing- masing tahap di dokumentasikan dengan baik.

e. Implementasi

Pada tahapan implementasi ini menjelaskan software dan hardware yang digunakn pada saat melakukan perancangan program . Dibawah ini software dan hardware yang di gunakan :

a) Pengunaan software pada proses mengamankan data ini menggunkan bahasa pemograman php lalu DBMS yang digunkan PHP myAdmin.
b) Hardware yang digunakan Procesor Intel Core i5 RAM 4GB DDR3 SSD 512GB.

f. Pengujian Sistem

Pengujian sistem ini sangat penting dilakukan agar menjamin sistem untuk mengamankan sebuah data berjalan dengan sesuai harapan hasil yang sudah di analisis sebelumnya agar dapat menghasilkan suatu sistem yang diharapkan dan jika file melebihi batas 5mb maka akan gagal melakukan proses enkripsi.

g. Kesimpulan

Kesimpulan penerapan metode kriptografi *Advanced Encyption Standard* (AES) 128 ini agar dapat berfungsi dengan baik, dan aplikasi dapat menjaga ,mengamankan dan mencegah adanya peretasan dan kebocoran data pada perusahaan PT . ANTARA PERSADA SUKSES.

2.1 Kriptografi

Sejarah enkripsi sebagian besar adalah sejarah enkripsi klasik, yaitu metode enkripsi dengan kertas dan pena atau mungkin dengan perangkat mekanis sederhana. Secara umum, algoritma enkripsi klasik dibagi menjadi dua kategori, yaitu cipher transposisi dan cipher substitusi. Sandi transposisi mengubah urutan huruf dalam pesan, sedangkan sandi substitusi menggantikan setiap huruf atau kelompok huruf dengan huruf atau kelompok huruf yang berbeda[7]. Enkripsi terbaru diterbitkan oleh NIST (*National Institute of Standards and Technology*), yang menggantikan algoritma DES (*Data Encryption Standard*) yang sudah ketinggalan zaman. Algoritma AES merupakan algoritma enkripsi yang dapat mengenkripsi dan mendekripsi data dengan kunci yang berbeda panjang yaitu 128-bit, 192-bit dan 256-bit[8]. .

2.2 *Advanced Encryption Standard*(AES-128)

AES-128 (*Advanced Encryption Standard*) merupakan pengembangan lebih lanjut dari algoritma sebelumnya yaitu Data *Encryption Standard* (DES) yang dianggap kadaluarsa karena alasan keamanan. Kriteria evaluasi yang ditentukan oleh NIST didasarkan pada tiga kriteria utama yaitu aspek keamanan, aspek biaya, dan aspek implementasi serta karakteristik algoritma. Oleh karena itu, diperlukan suatu aplikasi yang dapat mendukung kita dalam melakukan pemesanan. Karena perlindungan dokumen yang dikirim menjadi prioritas, diperlukan metode perlindungan yang dilengkapi dengan sistem enkripsi[9].

2.2.1 Proses Enkripsi AES – 128

Berikut adalah ringkasan dari algoritma AES yang bekerja di blok 128bit menggunakan kunci 128bit (selain proses pembuatan round kunci).

1. *AddRoundKey* : XOR state awal (*plainteks*) dengan *cipherkey*. Langkah ini disebut *initial round*.
2. Putaran sebanyak Nr – 1 kali. Langkah yang dilakukan dalam setiap putaran adalah :

a. *SubBytes* : Substitusi byte dengan S- box (tabel substitusi).
b. *ShiftRows* : Memindahkan baris array state dengan wrapping.
c. *MixColumns* : Acak data pada setiap kolom *state array*.
d. *AddRoundKey* : Melakukan XOR antara state saat ini dengan round key.

2.2.2 Proses Dekripsi AES – 128

Langkah dekripsi AES, juga dikenal sebagai Invers Cipher dari algoritma Rijndael, yang beroperasi blok 128bit dengan kunci 128bit, adalah :

1. InitialRound : Tahap AddRoundKey yang melakukan XOR antara state awal (ciphertext) dan kunci enkripsi. Langkah ini juga disebut InitialRound.
2. Putaran sebanyak Nr – 1 kali. Proses yang terjadi pada setiap putaran yaitu :

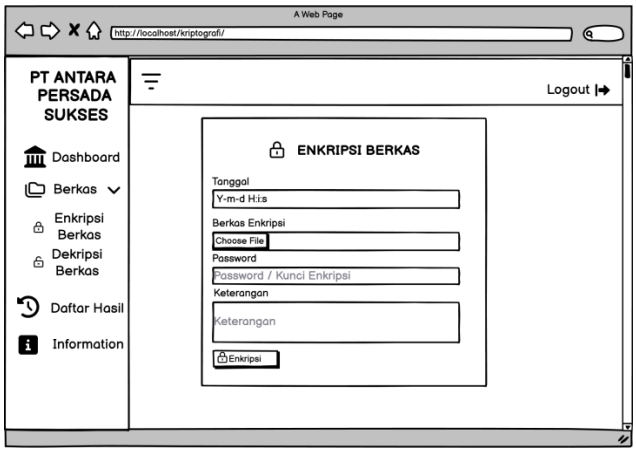
a. InvShiftRow : Memindahkan baris state array dengan wrapping.
b. InvByteSub : Substitusi byte dengan tabel substitusi kebalikan (inverse S-box).
c. AddRoundKey : Yaitu XOR antara state saat ini dengan round key.
d. InvMixColumn: Acak data di setiap kolom state array[10].

2.3 Rancangan Layar

Rancangan ini sangat di butuhkan saat perancangan suatu aplikasi, rancangan layar langkah yang pertam saat pembuatan tampilan aplikasi yang diinginkan. Tujuan rancangan layar agar mempermudah saaat membuat tampilan.

2.3.1 Rancangan Layar Enkripsi Berkas

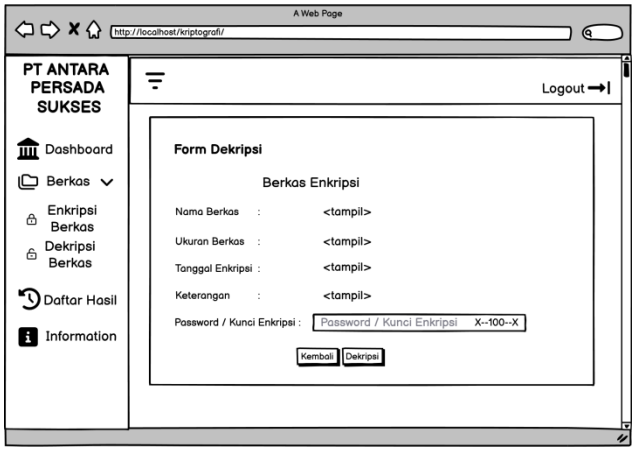
Tampilan rancangan layar yang terdapat pada enkripsi berkas seperti tanggal pada saat melakukan proses enkripsi, pemilihan file untuk melakukan proses enkripsi, keterangan file dan memasukan *password*.Berikut Gambar 2. rancangan layar Enkripsi Berkas.



Gambar 2. Rancangan Layar Enkripsi Berkas

2.3.2 Rancangan Layar *Form* Dekripsi Berkas

Rancangan layar halaman *form* deskripsi ini menampilkan halaman proses deskripsi. Halaman ini terdapat password yang harus di isi oleh pengguna agar bisa melakukan proses deskirpsi pada file. Berikut gambar 3. Rancangan Layar Halaman Deskripsi.



Gambar 3. Rancangan Layar *Form* Dekripsi

3. HASIL DAN PEMBAHASAN

Pada hasil dan pembahasan memaparkan suatu flowchart enkripsi dan dekripsi, tampilan layar dan hasil pengujian dari suatu program yang di buat peneliti.

3.1 Proses Perhitungan Enkripsi Dan Dekripsi

proses enkripsi dimulai dengan *plaintext* dan *chipper key* melalui addround key ditambahkan kedalam operasi XOR. Tahap *subBytes* yaitu dengan memindahkan baris *plaintext* kiri ke dalam *chipper key*, dengan *shiftRows* memindahkan kolom plaintext kiri ke *chipper key*

Plain Text : ARFIANNURIKHSANS

Chiper Key : KRIPTOGRAFIAESKU

Yang terdapat pada tabel 1. adalah *Plain Text* yang di konversi ke hexadecimal

Tabel 1. *Plain Text*

41	52	46	49
41	4E	4E	55
52	49	4B	48
53	41	4E	53

Yang terdapat pada tabel 2. adalah *chiper key* yang di konversi ke hexadecimal

Tabel 2. *Chiper key*

4B	54	41	45
52	4F	46	53
49	47	49	4B
50	52	41	55

Tahap mixcoloumns ini menggabungkan *plaintext* dengan chiperkey terjadi sebanyak 9 kali round, dengan *addroundkey* pada proses ini.

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \mathbf{X} \begin{bmatrix} 8F \\ 43 \\ A3 \\ 63 \end{bmatrix}$$

$= 2 \times 8F = 10 \text{ xor } 1000111$

$= X \text{ xor } X^7 + X^3 + X^2 + X + 1$

$= X^8 + X^4 + X^3 + X^2 + X \text{ Modulo } X^8 + X^4 + X^3 + X + 1$

$= X^2 + 1 = 00000101$

$3 \times 43 = 11 \text{ xor } 01000011$

$= (X + 1) \text{ xor } (X^6 + X + 1)$

$= (X^7 + X^2 + X) + (X^6 + X + 1)$

$= X^7 + X^6 + X^2 + 1 = 111000101$

$1 \times A3 = 1 \text{ xor } 10100011 = 10100011$

$1 \times 63 = 1 \text{ xor } 01100011 = 01100011$

HASIL AKHIR

00000101

11000101

10100011

01100011

Tahapan pada proses dekripsi 00000000 = 00(hex) untuk baris 1 kolom dan seterusnya untuk masing- masing baris dan kolom sampai semua dihitung untuk hasil *invsmixcolumns* round 1 pada tabel 3. yang terdapat dibawah ini.

Tabel 3. *InvsMixcolumns*

00	36	05	C0
B4	BC	7E	92
34	60	65	E9
AC	65	AF	B9

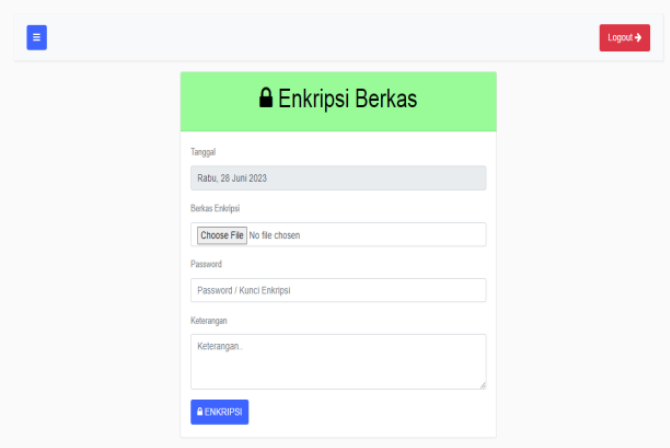
Setelah melalu invsubbytes lagi setelah round key 9 ke round key 1 sebannyak 9 kali, akan di round dengan key 0 dan menjadi tahap akhir atau round 0, dan sebagai hasil akhirnya adalah data dalam bentuk *plaintext* yang kembali ke dalam bentuk semula, sama seperti pada proses enkripsi

3.2 Tampilan Layar

Pada tampilan layar ini form – form yang terdapat pada program

3.2.1 Tampilan Layar Enkripsi Berkas

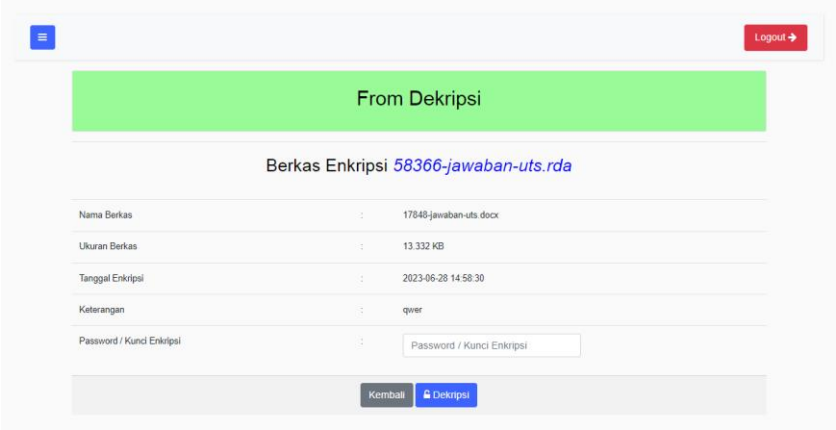
Berikut hasil dari rancangan layar enkripsi berkas terdapat pada gambar 6. Tampilan layar enkripsi berkas.



Gambar 6. Tampilan Layar Enkripsi Berkas

3.2.2 Tampilan Layar Form Dekripsi Berkas

Berikut hasil dari rancangan layar *form* dekripsi terdapat pada gambar 7. Tampilan layar *form* dekripsi.



Gambar 7. Tampilan Layar *Form* Dekripsi

3.3 Pengujian

Berikut adalah hasil dari pengujian *file* yang asli dengan *file* yang telah terenkripsi menggunakan aplikasi ini dengan kebutuhan yang telah terpenuhi baik spesifikasi software maupun spesifikasi hardware.

Tabel 1. Hasil Pengujian Dekripsi

NO	Nama File Awal	Ukuran File	Nama File Hasil Enkripsi	Ukuran File Setalah Enkripsi	Status	
					Durasi Enkripsi	Keterangan
1	ContohBerkas 1.xlsx	246 KB	24691-contoh-berkas-1.rda	13 KB	0.67 detik	BERHASIL
2	ContohBerkas 2.mp3	456 KB	98838-2Contoh-Berkas-2.rda	456 KB	11.41 detik	BERHASIL
3	Contohberkas 3.jpg	43 KB	54221-Contoh Berkas-3.rda	43 KB	1.43 detik	BERHASIL
4	ContohBerkas 4.docx	43 KB	5250-ContoH-Berkas-4.rda	43 KB	0.31 detik	BERHASIL
5	ContohBerkas 5.pdf	151 KB	34974-Contoh-Berkas-5.rda	151 KB	4.62 detik	BERHASIL
6	ContohBerkas 6.pptx	1.853 KB	99317-Contoh-berkas-6.rda	1.853 KB	43.48 detik	BERHASIL

Tabel 2. Hasil Pengujian Dekripsi

NO	Nama File Enkripsi	Ukuran File Enkripsi	Nama File Hasil Dekripsi	Ukuran File Dekripsi	Status	
					Durasi Enkripsi	Keterangan
1	24691-contoh-berkas-1.rda	246 KB	78428-contoh-berkas-1.xlx	13 KB	0.32 detik	BERHASIL
2	98838-2Contoh-Berkas-2.rda	456 KB	95324-Contoh-Berkas-2.mp3	456 KB	11.17 detik	BERHASIL
3	54221-ContohBerkas-3.rda	43 KB	35612-Contoh Berkas-3.jpeg	43 KB	1.38 detik	BERHASIL
4	5250-Contoh-Berkas-4.rda	14 KB	60499-Contoh Berkas-4.docx	14 KB	0.62 detik	BERHASIL
5	34974-Contoh-Berkas-5.rda	14 KB	26249-Contoh-Berkas-5.pdf	151 KB	3.69 detik	BERHASIL
6	99317-Contoh-berkas-6.rda	151 KB	93410-Contoh-berkas-6.ppt	1.853 KB	44.89 detik	BERHASIL

4. KESIMPULAN

Bedasarkan analisis dan uraian terhadap aplikasi yang dikembangkan, dapat disimpulkan bahwa program aplikasi pengamanan berkas berbasis web dengan menggunakan algoritme Advanced Encryption Standard (AES-128) pada PT. Antara Persada Sukses dapat disimpulkan sebagai berikut:

1. Berhasil mengenkripsi berkas dengan format excel, ppt, doc, jpeg, pdf, dan mp3.
2. Berkas yang telah dienkripsi tidak bisa dibaca oleh pihak lain, dikarenakan hanya pemilik password yang dapat mendekripsi dengan kunci (*key*) yang telah diberikan saat melakukan enkripsi.
3. Algoritme *Advanced Encryption Standard* (AES-128) dapat diterapkan pada aplikasi pengamanan berkas pada PT.Antara Persada Sukses.
4. Ukuran berkas tidak berubah sesudah dienkripsi dan setelah didekripsi.

DAFTAR PUSTAKA

[1] B. I. T. Dalam *et al.*, "IMPLEMENTASI KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD 128 BIT DALAM PENGAMANAN DATA KEUANGAN KAS (Studi Kasus: Masjid Al-Ikhlas Trini Sleman D.I.Yogyakarta) Hilda Dwi Novianti 1 , Ahmad Tri Hidayat 2," 2023.

[2] D. D. Rusnadi and N. Juliasari, "Implementasi Algoritme Aes 128 Untuk Aplikasi Serah Terima Dokumen Project Pada Pt Telkomsigma," *Skanika*, vol. 4, no. 2, pp. 23–28, 2021, doi: 10.36080/skanika.v4i2.2205.

[3] J. Prayudha, _ S., and _ I., "Implementasi Keamanan Data Gaji Karyawan Pada PT. Capella Medan Menggunakan Metode Advanced Encryption Standard (AES)," *J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer)*, vol. 18, no. 2, p. 119, 2019, doi: 10.53513/jis.v18i2.150.

[4] G. P. Utama *et al.*, "IMPLEMENTASI KRIPTOGRAFI METODE ADVANCED ENCRYPTION STANDART (AES-128) UNTUK PENGAMANAN FILE PADA TOKO SEPATU DESSLER . ID IMPLEMENTATION OF ADVANCED ENCRYPTION STANDARD (AES- 128) CRYPTOGRAPHY METHOD FOR SECURING FILES AT DESSLER . ID SHOE STORE," vol. 2, no. April, pp. 74–81, 2023.

[5] S. P. Ananda and S. Lukman, "Analisa Metode Kriptografi Modern Advance Encryption Standard (AES) 128 Bit dalam Mengenkripsi dan Mendekripsi File Dokumen Digital," *J. Ilm. Komputasi*, vol. 21, no. 3, pp. 333–344, 2022, doi: 10.32409/jikstik.21.3.2973.

[6] 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.

[7] A. Eka Putri, A. Kartikadewi, and L. A. Abdul Rosyid, "Implementasi Kriptografi dengan Algoritma Advanced Encryption Standard (AES) 128 Bit dan Steganografi menggunakan Metode End of File (EOF) Berbasis Java Desktop pada Dinas Pendidikan Kabupaten Tangerang," *Appl. Inf. Syst. Manag.*, vol. 3, no. 2, pp. 69–78, 2021, doi: 10.15408/aism.v3i2.14722.

[8] R. Saepul Rohman, D. A. Firmansah, and E. Ermawati, "Sistem Informasi Decrypt Respon Bridging Bpjs Kesehatan Dengan Algoritma Aes 256," *J. Responsif Ris. Sains dan Inform.*, vol. 4, no. 2, pp. 142–151, 2022, doi: 10.51977/jti.v4i2.761.

[9] M. Azhari, D. I. Mulyana, F. 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. 01, pp. 163–171, 2022, doi: 10.47709/jpsk.v2i01.1390.

[10] A. Teguh Utomo and R. Pradana, "Implementasi Algoritma Advanced Encryption Standard (AES-128) Untuk Enkripsi dan Dekripsi File," *Semin. Nas. Mhs. Fak. Teknol. Inf. Jakarta-Indonesia*, no. September, pp. 21–23, 2022.