2nd Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
21 Maret 2023 – Jakarta, Indonesia
Volume 2, Nomor 1, April 2023 - ISSN 2962-8628 (*online*)

IMPLEMENTASI ALGORITMA *ADVANCED ENCRYPTION STANDARD* UNTUK PENGAMANAN *FILE* PADA SMP NEGERI 189 JAKARTA BARAT

Nur Ubay Baidoi[1*], Mardi Hardjianto[2], Arief Wibowo[3]

[1,2,3] Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, DKI Jakarta, Indonesia

Email: [1*]nurubaybaidoi@gmail.com, [2]mardi.hardjianto@budiluhur.ac.id, [3]arief.wibowo@budiluhur.ac.id
(* : *corresponding author*)

Abstrak-Sebuah data dan informasi menjadi suatu aspek yang harus terjaga keamanan dan kerahasiaannya pada saat ini di dunia teknologi informasi. Data dan informasi menjadi suatu aset pada instansi maupun individu, khususnya di lembaga pendidikan SMP Negeri 189 Jakarta. Sebuah lembaga pendidikan memiliki banyak file yang sangat penting untuk dijaga kerahasiaannya seperti data diri siswa dan siswi serta nilai UAS masing-masing. File data diri dan nilai UAS dari siswa dan siswi bersifat internal yang hanya dapat dilihat oleh pihak sekolah saja, dan untuk mengantisipasi kebocoran dari file dan data tersebut maka harus ada pengamanan dalam sebuah file. Penelitian ini akan merancang sebuah sistem pengamanan file yang mengimplementasikan kriptografi sebagai metode yang dipakai, kriptografi merupakan suatu jalan keluar atau metode dalam pengamanan sebuah file yang tepat untuk menjaga kerahasiaan dan keamanan dari data dan informasi yang penting. Dalam merancang sebuah sistem diperlukan sebuah algoritma yang dipakai, dan algoritma dari kriptografi yang akan dipakai adalah algoritma *Advanced Encryption Standard* (*AES*) untuk melakukan proses dari enkripsi file dan dekripsi file. Ditentukannya algoritma *AES* karena memiliki suatu tingkat keamanan pertukaran informasi yang cukup bagus. Hasil dari uji coba data yang berbeda saat dilakukannya enkripsi dan dekripsi dengan ukuran file yang beda akan mempengaruhi waktu dalam proses enkripsi dan dekripsi. File yang berukuran 57.8389 *bytes* memiliki waktu enkripsi 05,57 *milisecond* dan file yang berukuran 156.438 *bytes* memiliki waktu enkripsi 15,40 *milisecond*. Kesimpulan dari hasil implementasi, bahwa algoritma kriptografi *Advanced Encryption Standard* (*AES*) dapat menjaga keamanan dan kerahasiaan dari file dan data yang ada pada lembaga pendidikan SMP Negeri 189 Jakarta Barat.

Kata Kunci: Kriptografi, *Advanced Encryption Standard* (AES), Pengamanan File.

IMPLEMENTATION OF THE ADVANCED ENCRYPTION STANDARD ALGORITHM FOR SECURING FILES AT SMP NEGERI 189 WEST JAKARTA

Abstract- *Data and information become an aspect that must be kept secure and confidential at this time in the world of information technology. Data and information become an asset for both institutions and individuals, especially at SMP Negeri 189 Jakarta educational institutions. An educational institution has many files that are very important to keep confidential, such as students' personal data and their respective UAS scores. Personal data files and UAS scores from students are internal and can only be seen by the school, and to anticipate leaks from these files and data, there must be security in a file. This research will design a file security system that implements cryptography as the method used, cryptography is a solution or method for securing a file that is appropriate for maintaining the confidentiality and security of important data and information. In designing a system, an algorithm is needed, and the cryptographic algorithm that will be used is the Advanced Encryption Standard (AES) algorithm to carry out the process of file encryption and file decryption. The AES algorithm was chosen because it has a fairly good level of information exchange security. The results of testing different data when encrypting and decrypting with different file sizes will affect the time in the encryption and decryption process. Files measuring 57,8389 bytes have an encryption time of 05.57 milliseconds and files measuring 156,438 bytes have an encryption time of 15.40 milliseconds. The conclusion from the results of the implementation is that the Advanced Encryption Standard (AES) cryptographic algorithm can maintain the security and confidentiality of files and data that exist in 189 Junior High School West Jakarta educational institutions.*

Keywords*: Cryptography, Advanced Encryption Standard (AES), File Security.*

1. PENDAHULUAN

Teknologi Informasi yang memberikan pengaruh positif tetapi juga memberikan pengaruh negatif, dan pengaruh negatif dalam berkembangnya teknologi informasi terdapatnya penyadapan data. Masalah keamanan dan kerahasiaan dari sebuah data, informasi dan pesan merupakan salah satu aspek penting, data yang dapat berbentuk format dokumen digital seperti .docx, .pdf, .xlsx, dan lain-lain [1]. Informasi dan data adalah sebuah aset yang penting untuk sebuah instansi maupun individu. Dari semua yang menggunakan komputer banyak yang melakukan

penyimpanan data yang telah dipakai untuk meningkatkan keamanan dari data yang disimpan agar setiap informasi yang telah dikerjakan dapat terjamin kerahasiaan dan keasliannya [2].

Pada pengelolaan data di Sekolah SMP Negeri 189 Jakarta Barat sudah tersimpan secara sistematis, tetapi data-data yang sudah ada dalam sekolah masih berupa teks asli, yang dapat dengan mudahnya dilihat dan dibaca. File dari nilai UAS dan data diri siswa memiliki sifat internal yang hanya dapat diakses oleh pihak sekolah seperti guru-guru dan staf sekolah dikarenakan file-file tersebut bersifat sangat penting. Permasalahan dalam data-data yang bisa untuk dilihat dan diakses pihak yang tidak seharusnya dapat melihat dan mengakses, itu disebabkan karena instansi yang tidak memiliki sistem pengamanan pada file. Solusi dari permasalahan ini adalah dengan mengimplementasikan pengamanan file menggunakan metode kriptografi yang dapat mengunci isi data-data sehingga data-data menjadi lebih aman [3].

Kriptografi, yang pada zaman dahulu digambarkan sebagai ilmu yang mempelajari cara menyembunyikan pesan. secara modern kriptografi digambarkan sebagai ilmu yang didasarkan pada teknik matematika. Ilmu ini menjamin keamanan data dan informasi seperti kerahasiaan dan keakuratan. Dalam kriptografi modern, tidak hanya menangani pesan tersembunyi namun lebih pada teknik yang menjamin sebuah keamanan data dan informasi [4]. Terdapat beberapa metode kriptografi yang tersedia untuk digunakan dalam kasus pengamanan file. File yang dilindungi selalu mendapat kata sandi atau kode enkripsi. File yang dilindungi tidak dapat dibaca atau ditampilkan karena kata sandi telah ditetapkan padanya. Jika Anda ingin melihat atau membaca file yang dilindungi kata sandi, anda harus mengembalikan data yang dilindungi kata sandi ke data asli.

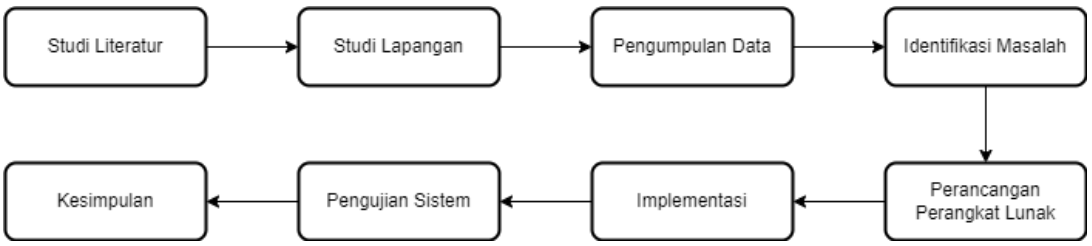
Berhubungan dengan solusi yang dipaparkan, Kriptografi pengamanan file menggunakan algoritme *Advanced Encryption Standard*, algoritme ini menjadi standar dari algoritme Kriptografi dan pada sampai saat ini masih belum ada yang dapat memecahkan algoritme dari *Advanced Encryption Standard*. Berdasarkan kondisi tersebut, akan diimplementasikan Kriptografi menggunakan algoritme *Advanced Encryption Standard* (*AES*-128) pada pemrosesan enkripsi dan dekripsi file dokumen yang berformat .doc, .xlsx dan .pdf dan diharapkan informasi dan data bersifat penting yang ada di dalam file tersebut tidak disalah gunakan oleh pihak yang tidak berkepentingan. Jenis dokumen yang diujikan adalah biodata dan nilai ujian dari siswa dan siswi dengan periode data terbaru dan jumlah data lebih dari 5 data yang diujikan.

Penelitian Azhari dkk., yang berjudul Implementasi Pengamanan Data Pada Dokumen Menggunakan *Algoritma Kriptografi Advanced Encryption Standard (AES)* [5]. Penelitian Hulu dkk., yang berjudul Implementasi algoritma *AES (Advanced Encryption Standard)* untuk keamanan file hasil radiologi di RSU Imelda Medan [6]. Penelitian Indrayani & Suartana yang berjudul Implementasi Kriptografi Dengan Modifikasi *Algoritma Advanced Encryption Standard (AES)* Untuk Pengamanan File Document [7]. Penelitian Prameshwari & Sastra yang berjudul Implementasi Algoritma *Advanced Encryption Standard (AES)* 128 Untuk Enkripsi Dan Dekripsi File Dokumen [8].

2. METODE PENELITIAN

2.1. *Flowchart* Penelitian

Metode Waterfall adalah metode yang dipakai pada penelitian ini dan menjadi prinsip dalam melakukan penelitian maka tidak ada penyimpangan dan kesalahan dari hasil dan tujuan yang sudah dilakukan sehingga penelitian dapat lebih baik. Pada Gambar 1 adalah flowchart penelitian.



Gambar 1. *Flowchart* Penelitian

2.2. Pengumpulan Data

Langkah pengumpulan data ini dilakukan untuk mengumpulkan data yang dibutuhkan untuk perancangan sistem, berikut merupakan tahap-tahap yang dilakukan adalah:

a. Wawancara Dilakukan tanya jawab kepada pihak-pihak yang tersangkut. Untuk memperoleh informasi tentang kebutuhan untuk menjalankan sistem pengamanan file pada nilai UAS dan data diri siswa/i.
b. Observasi Mengumpulkan data dan mengamati tahapan yang terjadi secara langsung di SMP Negeri 189

Jakarta Barat yang nantinya digunakan sebagai masukan untuk laporan penelitian.

c. Studi Pustaka dilakukan dengan cara membaca buku digital dan jurnal serta referensi lainnya yang berhubungan dengan teori kriptografi, teori pengamanan file, teori dari metode AES dan teori-teori pendukung lainnya.

2.3. Kriptografi

Berdasarkan pendapat Saragi dkk., Kriptografi memegang peranan penting dalam dunia teknologi informasi saat ini, terlebih lagi dalam ilmu komputer, yang mempelajari konsep matematika yang berkaitan dengan keamanan informasi. Enkripsi juga merupakan persyaratan keamanan TI yang penting untuk mengirim pesan sensitif dan rahasia [9].

a. *Plaintext (message)* adalah pesan asli yang akan dikirimkan dan dijaga keamanannya.
b. *Ciphertext* adalah pesan yang sudah dilakukan pengkodean dan sudah siap untuk dikirimkan.
c. *Cipher* merupakan algoritme matematis yang dipakai sebagai proses penyandian plaintext menjadi *ciphertext*.
d. Enkripsi (*encryption*) yakni tahap yang bertujuan untuk memberikan sandi *plaintext* sehingga menjadi *ciphertext*.
e. Dekripsi (*decryption*) yakni tahap yang bertujuan untuk mendapatkan kembali *plaintext* dari *ciphertext*.
f. *Kriptosystem* adalah sebuah sistem yang dibuat untuk mengamankan sebuah informasi dan data dengan menggunakan kriptografi.

2.4. *Advanced Encryption Standard* (*AES*)

a. Algoritme Enkripsi *AES*-128.

Berdasarkan pendapat Muharram dkk., Proses enkripsi pada algoritme AES memiliki 4 macam perubahan bytes, yaitu adalah *SubBytes, ShiftRows, Mixcolumns, dan AddRoundKey.* Semua kegunaan operasi yang ada pada algoritme AES adalah sebuah operasi yang diartikan dalam ruang lingkup finite field GF(28) dengan polinominal irreducible pembangkit m(x) = x8 + x4 + x3 + x + 1 [10].

1) Didalam tahapan algoritme AES *AddRoundKey*, merupakan round key yang dijumlahkan pada *state* dengan penerapan XOR. Masing-masing key mamiliki kata Nb dimana tiap kata tersebut akan dijumlahkan dengan kata atau kolom yang sesuai dari state sehingga menjadi persamaan.
2) *SubBytes* adalah perubahan *bytes* dimana setiap elemen pada *state* akan dipetakan dengan memakai sebuah tabel substitusi (*S-Box*). Setiap Bytes yang ada pada array state, misalnya S[r, c] = xy yang dalam kasus ini xy adalah digit heksadesimal dari nilai S[r, c], maka nilai substitusinya, dinyatakan dengan S'[r, c], adalah elemen didalam tabel substitusi yang merupakan perpotongan baris x dengan kolom y.
3) Transformasi *Shiftrows* merupakan proses bergesernya bit dimana bit yang posisinya paling kiri akan dipindahkan ke posisi bit yang paling kanan (rotasi bit).
4) *Mixcolumns* melakukan operasi pada setiap elemen yang ada di dalam satu kolom pada *state*.

Algoritme 1. Enkripsi *AES*

1	*Start*
2	*Input plaintext*
3	*i=1*
4	*Add round key (0)*
5	*Sub bytes*
6	*Shift rows*
7	*Mix column*
8	*Add round key (1)*
9	*if <= 9*
10	*i++*
11	Kembali ke baris 5
12	*End if*
13	*Sub bytes*
14	*Shift rows*
15	*Add round key (Nr)*
16	*Output ciphertext*
17	*end*

b. Algoritme Dekripsi AES-128.

Berdasarkan pendapat Muharram dkk., Transformasi chipper dapat dilakukan terbalik dan diterapkan dengan arah yang berlawanan untuk menghasilkan *inverse chiper* yang mudah dimengerti untuk algoritma *AES*. Perubahan *byte* yang dipakai pada *inverse cipher* adalah *InvShiftRows, InvSubBytes, InvMixColumns* dan *AddRoundKey* [10].

1. *InvShiftRows* merupakan perubahan byte yang terbalik dengan perubahan *ShiftRows*. Pada perubahan InvShiftRows, dilakukan pertukaran bit ke kanan sedangkan pada ShiftRows dilakukan pertukaran bit ke kiri.
2. *InvSubBytes* juga merupakan perubahan *bytes* yang terbalik dengan perubahan *SubBytes*. Pada *InvSubBytes*, setiap elemen yang ada pada *state* dipetakan dengan menggunakan *Inverse S-Box.*
3. Pada *Inverse Mixcolumns* kolom yang ada pada tiap *state (word)* akan dilihat sebagai polinomial atas GF(2^8) dan mengalikan *modulo* $x^4 + 1$ dengan polinomial tetap $a^{-1}(x)$ yang didapat dari : $a^{-1}(x) = \{0b\}x^3 + \{0d\}x^2 + \{0d\}x + \{0e\}$.

Algoritme 2. Dekripsi AES

1	*Start*
2	*Input ciphertext*
3	*Add round key (9)*
4	*Inverse shiftrows*
5	*Inverse subbytes*
6	*i=1*
7	*Add round key (8)*
8	*Inverse mixcolumn*
9	*Inverse shiftrows*
10	*Inverse subbytes*
11	*if <= 9 Then*
12	*i++*
13	Kembali ke baris 7
14	*End if*
15	*Add round key (0)*
16	*Output plaintext*
17	*end*

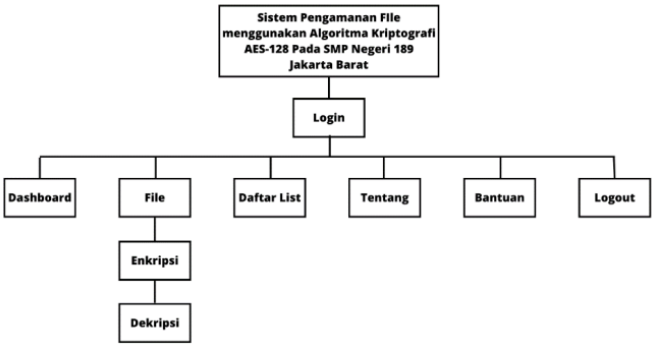
3. HASIL DAN PEMBAHASAN

3.1. Rancangan Pengujian

Rancangan pengujian yang diterapkan akan menggunakan algoritme kriptografi *Advanced Encryption Standard* (AES) untuk setiap format yang terdapat pada aplikasi berbasis web yang akan dirancang. Pengujian ini bermaksud untuk mengetahui apabila data yang sudah diuji, akan terenkripsi dengan baik di dalam database. Untuk mengetahui sebuah file yang sudah terenkripsi dengan baik, bisa dengan membuka file yang dienkripsi, apabila file yang sudah di enkripsi tidak dapat dibuka artinya pengenkripsian file berhasil.

3.2. Rancangan Menu

Struktur Rancangan menu web pengamanan *file* pada SMP Negeri 189 Jakarta Barat yang akan dirancang memiliki beberapa menu tampilan yang dilihat pada Gambar 2.

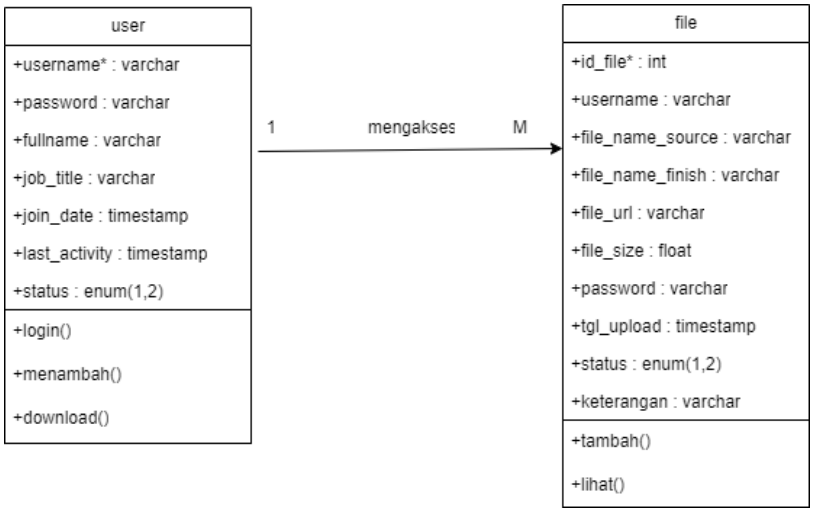


Gambar 2. Rancangan Menu

3.3. Rancangan Basis Data

a. *Class Diagram*

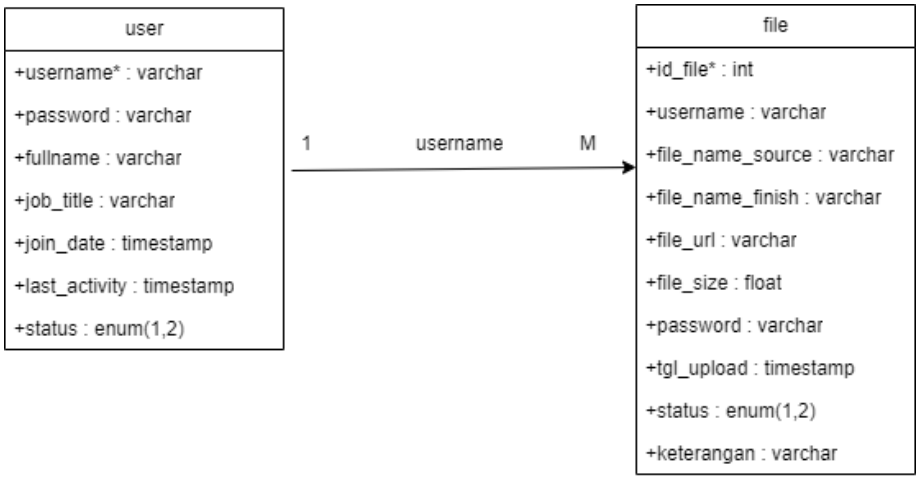
Pada Class Diagram ini menunjukan struktur-struktur dari aplikasi ini. Struktur yang ada ialah atribut dan metode yang apa pada masing-masing *Class*. Berikut *Class Diagram* yang ditunjukkan seperti pada gambar 2.



Gambar 3. *Class Diagram*

b. *Logical Record Structure* (LRS)

Bentuk dari *Logical Record Structure* (LRS) pada aplikasi yang dibuat ditunjukan pada gambar 3.



Gambar 4. *LRS*

c. Spesifikasi Basis Data

Pada Spesifikasi Basis Data terdapat struktur-struktur tabel yang ada pada basis data yang digunakan dalam perancangan aplikasi ini yang ditunjukan pada Tabel 1 dan Tabel 2.

Tabel 1. Spesifikasi Basis Data User

Nama	Tipe Data	Keterangan
Username	VarChar (15)	*Username*
Password	VarChar (100)	*Password*
Fullname	VarChar (50)	Nama *User*
Job_title	VarChar (50)	Nama Jabatan
Job_activity	TimeStamp (-)	Tanggal Gabung
Last_activity	TimeStamp (-)	Aktivitas Terakhir
Status	Enum (1,2)	Admin

Tabel 2. Spesifikasi Basis Data Tabel *File*

Nama	Tipe Data	Keterangan
Id_file	Int (11)	Id_file
Username	VarChar (15)	Username
File_nama_source	VarChar (225)	Nama File Asli
File_nama_finish	VarChar (225)	Nama Hasil File
File_url	VarChar (225)	url File
File_size	Float (-)	Ukuran
Password	VarChar (16)	Password
Tgl_upload	TimeStamp (-)	Tanggal Upload
Status	Enum (1,2)	Enkripsi dan Dekripsi
Keterangan	VarChar (225)	Keterangan

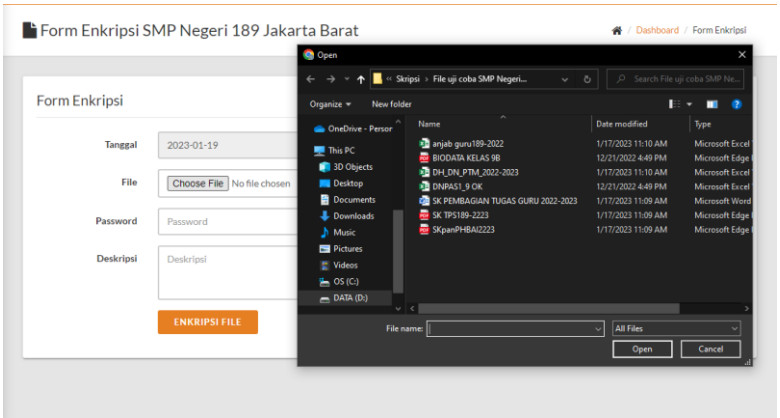
Pada tahap ini terdapat penjelasan yang berupa gambar, tabel dan keterangan dari hasil implementasi dari topik penelitian yang dibahas.

3.4. Implementasi *Advanced Encryption Standard* (AES-128)

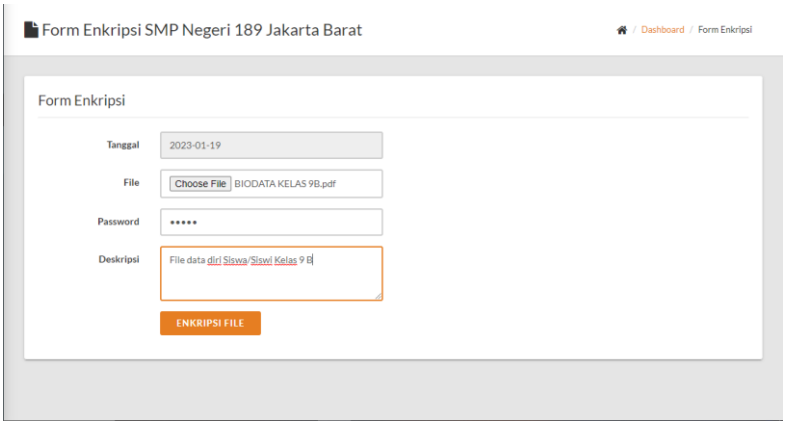
Pada proses implementasi metode terdapat sejumlah langkah-langkah yang akan dilakukan diantaranya sebagai berikut.

a. Implementasi Enkripsi.

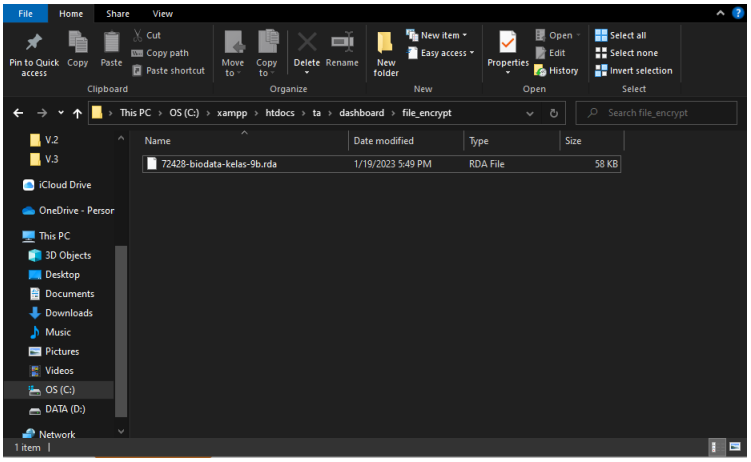
Pada proses enkripsi ini tahap pertama yang dapat dilakukan oleh user memilih menu file dan akan muncul *sub menu* enkripsi dan pilih *sub menu* enkripsi, setelah submenu enkripsi dipilih user harus memasukan file yang akan dienkripsi dan memberikan *password* untuk penguncian file, lalu tekan tombol enkripsi dan aplikasi akan memproses file yang dienkripsi. Proses dari pemilihan file, input password dan hasil dari enkripsi dapat dilihat pada gambar 4, 5 dan 6.



Gambar 5. Implementasi Enkripsi



Gambar 6. Implementasi Enkripsi (2)

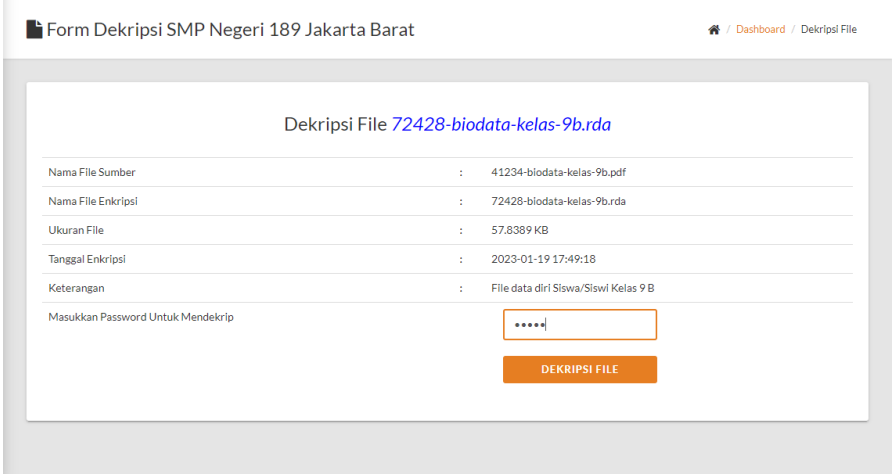


Gambar 7. Implementasi Enkripsi (3)

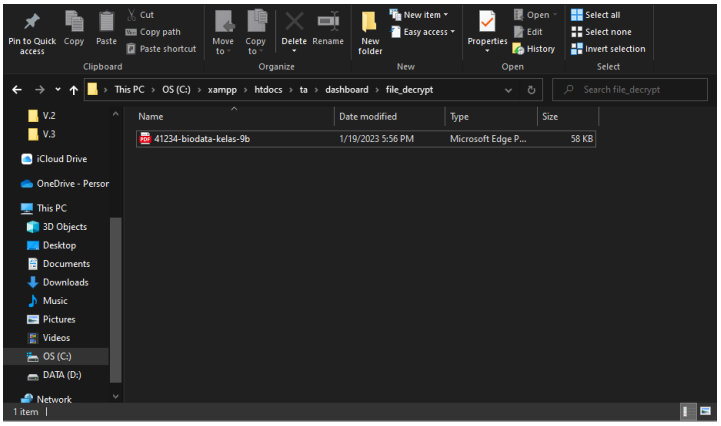
b. Implementasi Dekripsi.

Pada proses dekripsi *user* akan melakukan pendekripsian pada file yang sudah dienkripsi dengan menekan tombol dekripsi pada tabel form dekripsi dan memasukan *password* yang sudah diinput pada proses enkripsi. Proses dari dekripsi file, *input password* dan hasil dekripsi dapat dilihat pada gambar 7, 8 dan 9.

Gambar 8. Implementasi Dekripsi



Gambar 9. Implementasi Dekripsi (2)



Gambar 10. Implementasi Dekripsi (3)

3.5. Pengujian

Pada tahap ini akan dilakukannya pengujian terhadap aplikasi kriptografi pengamanan file dan yang akan diuji dari proses enkripsi dan dekripsi adalah file dari biodata dan nilai ujian dari siswa dan siswi agar aplikasi ini berjalan sesuai dengan yang direncanakan. Jumlah pengujian file yang menjadi contoh berjumlah 5 file dengan periode data yang terbaru.

a. Tabel Hasil Pada Pengujian Enkripsi File.
Pada tabel 3 dibawah merupakan hasil dari pengujian enkripsi file.

Tabel 3. Hasil Pengujian Enkripsi File

No.	Nama File Awal	Ukuran File	Nama File Hasil Enkripsi	Ukuran File Setelah Enkripsi	Keterangan & Durasi Enkripsi
1	biodata kelas 9b.pdf	58 KB	72428-biodata-kelas-9b.rda	57.8389 KB	Biodata Kelas 9 B & 00.05,57 Detik
2	DNPAS1_9 OK .xlsx	157 KB	22197- dnpas1_9-ok.rda	156.438 KB	Nilai Akhir Semester 9 & 00.15,40 Detik
3	biodata kelas 9a.pdf	60 KB	12344-biodata-kelas-9a.rda	59.8295 KB	Biodata Kelas 9 A & 00.05,59 Detik
4	DNPTS1_8 OK.xlsx	167 KB	63108-dnpts1_8-ok.rda	166.440 KB	Nilai Tengah Semester 8 & 00.16,58 Detik
5	biodata kelas 8a.pdf	57 KB	94299- biodata-kelas-8a.rda	56.8480 KB	Biodata Kelas 8 A & 00.05,24 Detik

b. Tabel Hasil Pada Pengujian Dekripsi File
Pada Tabel 4 merupakan hasil dari pengujian dekripsi file.

Table 4. Hasil Pengujian Dekripsi File

No.	Nama File Enkripsi	Ukuran File Enkripsi	Nama File Hasil Dekripsi	Ukuran File Dekripsi	Keterangan & Durasi Enkripsi
1	72428-biodata-kelas-9b.rda	57.8389 KB	41234- biodata-kelas-9b.pdf	58 KB	Biodata Kelas 9 B & 00.05,57 Detik
2	22197- dnpas1_9-ok.rda	156.438 KB	86498- dnpas1_9-ok.xlsx	157 KB	Nilai Akhir Semester 9 & 00.15,40 Detik
3	12344-biodata-kelas-9a.rda	59.8295 KB	82193- biodata-kelas-9a.doc	60 KB	Biodata Kelas 9 A & 00.05,59 Detik
4	63108-dnpts1_8-ok.rda	166.440 KB	4009- dnpts1_8-ok.xlsx	167 KB	Nilai Tengah Semester 8 & 00.16,58 Detik
5	94299- biodata-kelas-8a.rda	56.8480 KB	7985- biodata-kelas-8a.xlsx	57 KB	Biodata Kelas 8 A & 00.05,24 Detik

4. KESIMPULAN

Berdasarkan penjelasan dan uraian yang telah dibahas, maka dapat disimpulkan pada SMP Negeri 189 Jakarta Barat dapat diimplementasikan aplikasi berbasis *web* kriptografi pengamanan file dengan format .doc, .xlsx dan pdf menggunakan algoritma *Advanced Encryption Standard* (*AES*-128). Oleh karena itu dengan adanya aplikasi berbasis *website* pengamanan file ini mampu membantu SMP Negeri 189 Jakarta Barat dalam mengamankan file biodata dan nilai dari siswa dan siswi. *Website* pengamanan file ini dapat berhasil melakukan proses enkripsi dan dekripsi dan tidak mengubah ukuran pada file data asli. Sistem kriptografi yang berbasis *website* ini diharapkan dapat melakukan pengamanan selain file yang berformat .doc, .xlsx dan .pdf sehingga file yang berformat lain dapat dilakukan pengamanan dan terhindar dari penyalahgunaan data. Penelitian selanjutnya diharapkan dapat mengkombinasikan lebih banyak metode kriptografi lain dalam pengamanan file agar keamanan data yang dilakukan penguncian lebih aman dan tidak mudah untuk dibuka oleh pihak lain yang tidak bertanggung jawab.

DAFTAR PUSTAKA

[1] W. Pramusinto, N. Wizaksono and A. Saputro, "Aplikasi Pengamanan File Dengan Metode Kriptografi AES 192, RC4 Dan Metode Kompresi Huffman," *JURNAL BIT,* vol. 16, no. 2, pp. 47-53, 2019.
[2] I. Gunawan, "Peningkatan Pengamanan Data File Menggunakan Algoritma Kriptografi AES Dari Serangan Brute Force," *TECHSI,* vol. 13, no. 1, pp. 14-25, 2021.
[3] H. S. Djong and S. Siswanto, "Implementasi Kriptografi Dengan Menggunakan Metode RC4 dan AES-256 Untuk Mengamankan File Dokumen pada PT Varnion Technology Semesta," *SENAFTI,* vol. 1, no. 1, pp. 149-158, 2022.
[4] M. Syahril and H. Jaya, "Aplikasi Steganografi Pengamanan Data Nasabah di Standard Chartered Bank Menggunakan Metode Least Significant Bit dan RC4," *SENSASI,* vol. 1, no. 1, pp. 505-509, 2019.
[5] M. Azhari, D. I. Mulyana, F. J. Perwitosari and F. Ali, "Implementasi Pengamanan Data Pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," *Pendidikan Sains dan Komputer,* pp. 163-171, 2022.
[6] D. Hulu, B. Nadaek and S. Aripin, "Implementasi Algoritme AES (Advanced Encryption Standard) Untuk Keaman file Hasil Radiologi di RSU Imelda Medan," *KOMIK,* vol. 4, no. 1, pp. 78-86, 2020.
[7] L. A. Indrayani and I. M. Suartana, "Implementasi Kriptografi dengan Modifikasi Algoritma Advanced Encryption Standard (AES) untuk Pengamanan File Document," *JINACS,* vol. 1, no. 01, pp. 42-47, 2019.
[8] A. Prameshwari and P. N. Sastra, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen," *Eksplora Informatika,* p. 52, 2018.
[9] D. R. Saragi, J. M. Gultom, J. A. Tampubolon and I. Gunawan, "Pengamanan Data File Teks (Word) Menggunakan Algoritma RC4," *JSON,* vol. 1, no. 2, p. 114, 2020.
[10] F. Muharram, H. Aziz and A. R. Manga, "Analisis Algoritma Pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES)," *Prosiding Seminar Nasional Ilmu Komputer dan Teknologi Informasi,* pp. 1-4, 2018.