**IMPLEMENTASI KRIPTOGRAFI MENGGUNAKAN ALGORITMA *ADVANCED ENCRYPTION STANDARD* (AES-256) UNTUK MENGAMANKAN *FILE* DOKUMEN BERBASIS WEB PADA   
PT. DAMAI ELOK**

**Achmad Choirul Imamudin**

Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, Jakarta, Indonesia

Email: 11811502622@student.budiluhur.ac.id

(\* : corresponding author)

**Abstrak-**Banyak ahli membuat algoritma, terutama pengembangan algoritma kriptografi yang semakin pesat, sehingga teknologi komputer kontemporer dapat mempertahankan keamanan data. Bagian akuntansi PT Damai Elok sering membuat *file* atau data seperti kontrak kerja, data pelanggan, dan gaji karyawan. Oleh karena itu, data atau *file* ini tidak aman; orang yang tidak bertanggung jawab dapat melihatnya jika disimpan di folder komputer atau flash disk.

Penulis membuat aplikasi yang dapat digunakan untuk enkripsi dan dekripsi file ini untuk memastikan bahwa informasi dan file perusahaan tetap aman. Algoritma AES-256 digunakan untuk kriptografi dalam penelitian ini. Algoritma ini menjamin bahwa keamanan file tetap aman dan tidak dapat diketahui oleh pihak yang tidak dapat mengaksesnya. Program yang dapat melihat database aplikasi yang dienkripsi dan kemudian mendekripsi file akan memastikan bahwa file tersebut aman karena kata sandi atau tombol juga dienkripsi. Proses enkripsi dan dekripsi sistem menggunakan algoritma enkripsi standar lanjutan AES-256 telah diubah dengan menambahkan Randomize karakter. Jumlah waktu yang diperlukan untuk enkripsi dan dekripsi file akan meningkat karena data asli file tidak dapat dibaca setelah dienkripsi. Hasil implementasi menunjukkan bahwa ukuran file tidak berubah, sehingga algoritma kriptografi AES-256 dapat digunakan untuk melindungi isi file.

**Kata Kunci:** Kriptografi, AES-256, Enkripsi Berkas, Dekripsi Berkas, Modifikasi.

***IMPLEMENTATION OF CRYPTOGRAPHY USING ADVANCED ENCRYPTION STANDARD (AES-256) ALGORITHM TO SECURE***

***WEB-BASED DOCUMENT FILES AT***

***PT. DAMAI ELOK***

**Abstract-** *Many experts create algorithms, especially the rapid development of cryptographic algorithms, so that contemporary computer technology can maintain data security. The accounting department of PT Damai Elok often creates files or data such as work contracts, customer data, and employee salaries. Therefore, these data or files are not secure; irresponsible people can see them if they are stored in computer folders or flash disks.*

*The author created an application that can be used for encryption and decryption of these files to ensure that company information and files remain secure. The AES-256 algorithm is used for cryptography in this study. This algorithm ensures that the security of the files remains safe and cannot be known by those who cannot access them. A program that can view the encrypted application database and then decrypt the file will ensure that the file is secure because the password or key is also encrypted. The system encryption and decryption process using the advanced standard encryption algorithm AES-256 has been changed by adding Randomize characters. The amount of time required for file encryption and decryption will increase as the original data of the file cannot be read after being encrypted. The implementation results show that the file size does not change, so the AES-256 cryptographic algorithm can be used to protect the contents of the file.*

***Keywords****: Cryptography, AES-256, File Encryption, File Decryption, Modification.*

# PENDAHULUAN

Banyak ahli telah membuat algoritma, terutama algoritma kriptografi, yang semakin berkembang untuk menjaga keamanan data, sehingga teknologi komputer di era modern telah berkembang. Dekripsi adalah proses mengubah teks tersandi menjadi bentuk awalnya, sedangkan enkripsi adalah proses mengubah teks biasa menjadi teks terlindung, juga dikenal sebagai teks *chiper*. Masalah keamanan dan media penyimpanan *file* sangat penting, tetapi masalah keamanan kurang diperhatikan dalam Desain dan pengelolaan dokumen. Media penyimpanan seperti *Flash Disk*, HDD (*Hard Disk Drive*), SSD (*Solid State Drive*), dalam mentransfer *file* dibutuhkan koneksi yang stabil, tetapi koneksi yang cepat dan stabil tidak menjamin kerahasian dari data tersebut.

*Advanced Encryption Standard* (AES) adalah salah satu algoritma kriptografi simetris yang paling banyak digunakan untuk mengenkripsi data. Dengan menggunakan kunci enkripsi yang panjang, seperti 256-bit (AES-256), AES menawarkan tingkat keamanan yang sangat tinggi dan telah diakui secara global untuk melindungi data sensitif. AES-256 menjadi pilihan utama dalam banyak aplikasi keamanan informasi karena kemampuannya untuk melindungi data dari akses yang tidak sah dengan tingkat perlindungan yang sangat baik.

PT. Damai Elok merupakan perusahaan yang mengelola berbagai dokumen penting dan data sensitif yang memerlukan perlindungan khusus. Dalam upaya untuk menjaga integritas dan kerahasiaan dokumen yang dikelola, perusahaan ini membutuhkan solusi keamanan yang handal.

Implementasi kriptografi menggunakan algoritma AES-256 dalam aplikasi berbasis web dapat memberikan perlindungan tambahan untuk data mereka. PT Damai Elok adalah sebuah perusahaan yang bergerak di bidang makanan. Berkantor di Jl. Kedoya Raya No 5, Kota Jakarta Barat, Daerah Khusus Ibu Kota Jakarta 11520. PT Damai Elok menyimpan data penting seperti kontrak kerja, gaji karyawan, dan data pelanggan. PT Damai Elok sangat berhati-hati untuk mencegah pencurian atau manipulasi data yang merugikan bagi klien dan perusahaan yang bekerja dengannya. Oleh karena itu, sangat penting untuk memastikan bahwa data yang disimpan di PT Damai Elok, yang berupa *file* seperti.docx, doc,.xlsx, dan sebagainya, tidak disalahgunakan.

Pada penelitian ini penulis juga mencari sumber referensi dari keamanan *file* yang dilakukan oleh Aji Teguh Utomo, Rizky Pradana yang berjudul “Implementasi algoritma *Advanced Encryption Standard* (AES-128) untuk enkripsi dan dekripsi” hubungan penelitian ini dengan penelitian yang sudah ada, yaitu untuk melakukan pengamanan *file* dokumen dengan cara enkripsi dan dekripsi. Pada Perusahaan PT Damai Elok di mana penelitian ini menggunakan metode yaitu metode AES-256, Pada proses penelitian terdahulu *file* yang di enkripsi *file*. Untuk penelitian ini *file* yang di enkripsi data customer, gaji karyawan dan perjanjian kontrak kerja semua ini dilakukan oleh bagian Accounting dengan format yaitu:docx, doc, .xlsx, .xls, .pdf.

Penelitian sebelumnya banyak berfokus pada keamanan teoretis, tetapi belum banyak yang mengevaluasi kinerja algoritma ini dalam aplikasi web yang spesifik seperti yang digunakan oleh PT. Damai Elok. Gap ini mencakup analisis tentang bagaimana implementasi AES-256 mempengaruhi kecepatan pemrosesan dokumen dan penggunaan sumber daya sistem di lingkungan web.

# METODE PENELITIAN

# Data Penelitian

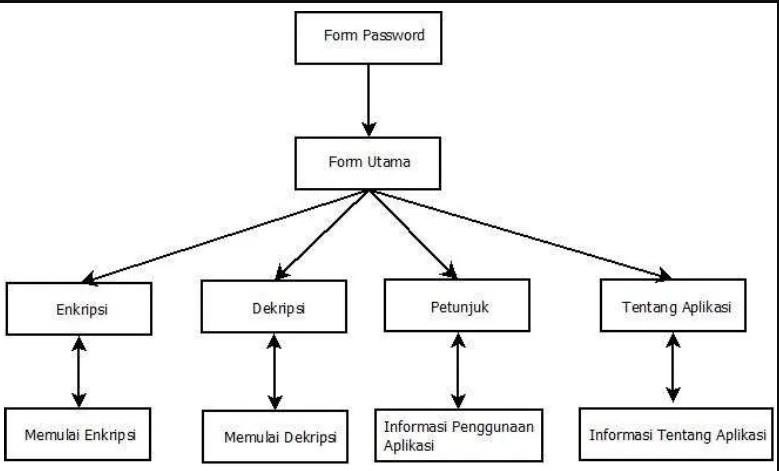
Data Penelitian ini menggunakan data dari bagian Accounting PT Damai Elok, yang terdiri dari tiga jenis file: data pelanggan, gaji karyawan, dan perjanjian kontrak kerja. Format file yang digunakan adalah .docx, .xlsx, dan .pdf, dengan ukuran file berkisar antara 1 hingga 3 MB. Semua data tersebut dikumpulkan pada bulan Juli 2024.

# Penerapan Metode

Untuk memastikan bahwa penelitian ini tidak menyimpang dari jalan yang benar dan mencapai tujuan awalnya,ini merupakan tahapan metode penelitian ini.

1. Pengumpulan Data, informasi tentang konfigurasi sistem dan detail implementasi AES-256.
2. Identifikasi Masalah, bagaimana AES-256 dapat diterapkan secara efektif dalam mengamankan file dokumen berbasis web di PT. Damai Elok.
3. Analisis Masalah, Analisis dampak AES-256 terhadap waktu akses dan penggunaan sumber daya sistem.
4. Strategi Penyelesaian Masalah, Mengimplementasikan solusi untuk mengurangi dampak negatif pada aksesibilitas dokumen.
5. Implementasi, melakukan pengujian untuk memastikan implementasi berjalan sesuai rencana dan melakukan penyesuaian jika diperlukan.
6. Kesimpulan, implementasi AES-256 dapat mempengaruhi performa sistem dan pengalaman pengguna, tetapi langkah-langkah perbaikan dapat mengurangi dampak negatif.

# State Diagram Aplikasi EnDe *File* (*Enkripsi* dan *Dekripsi File*)



# Gambar 1. *State Diagram Aplikasi EnDe*

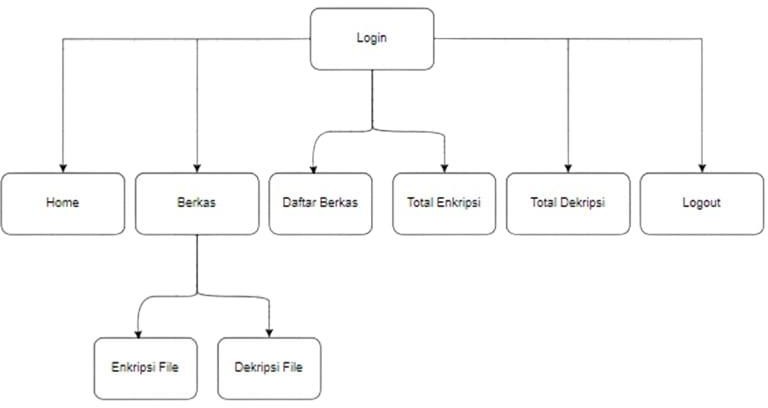
# *File* (*Enkripsi* dan *Dekripsi File*)

Berikut adalah penjelasan dari setiap *menu* yang ada distate *diagram* di aplikasi EnDe *File* (Enkripsi dan Dekripsi *File*):

1. *State: Form Login*
2. *State: Form Menu Utama*
3. *State: Form Enkripsi File*
4. *State: Form Dekripsi File*
5. *State: Form Isi Dekripsi File*

# Desain *Menu*

Pada Desain Menu ini saling berhubungan dan ada beberapa pilihan menu utama dan sub menu, untuk user dalam berinteraksi pada menu layar ini dengan menggunakan mouse. Berikut Desain Menu:



**Gambar 2.** Desain *Menu*

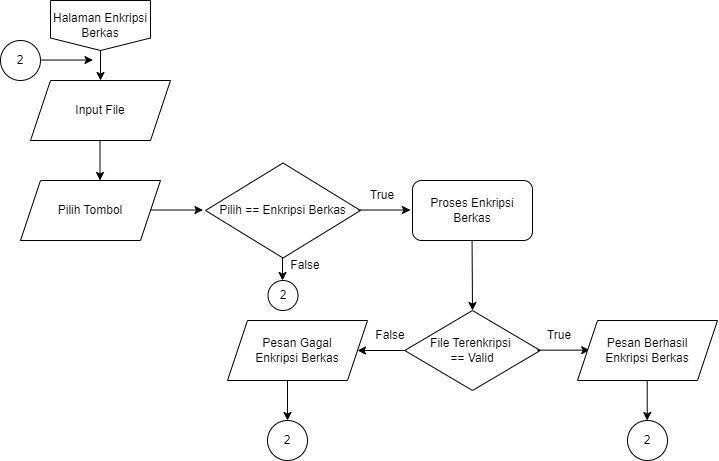
# Desain Layar *Website* untuk *Enkripsi* dan *Dekripsi File*

Desain layar adalah bagian penting dari pembuatan program, jadi tujuan dari desain layar ini adalah agar pengguna dapat menggunakannya dengan mudah, cepat memahaminya, dan tidak mengalami kesulitan.

# HASIL DAN PEMBAHASAN

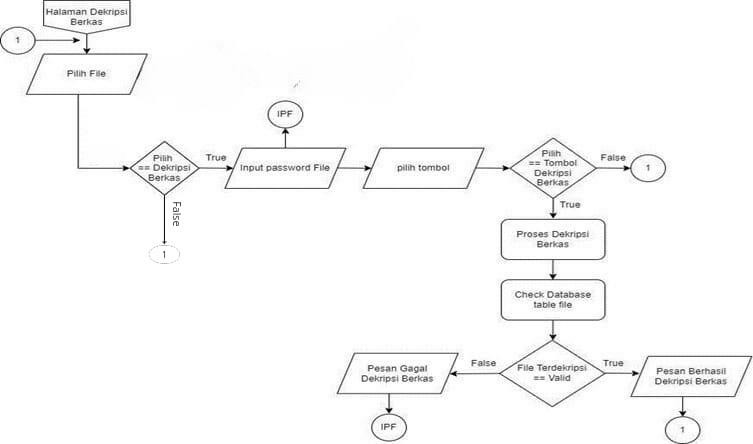
# *Flowchart*

Masukkan file yang ingin dienkripsi dengan password dan deskripsi, tombol untuk mengenkripsi isi file matriks dan lain-lain. matriks, Perubahan fungsi ini mengubah setiap baris tabel status, MixColumns melakukan proses mengalikan setiap elemen blok chip. dan matriks serta fungsi selanjutnya yaitu AddRoundKey melakukan fungsi menggabungkan ciphertext dengan clear key terkait dengan gambar di bawah ini yang merupakan gambar diagram alir proses enkripsi file.



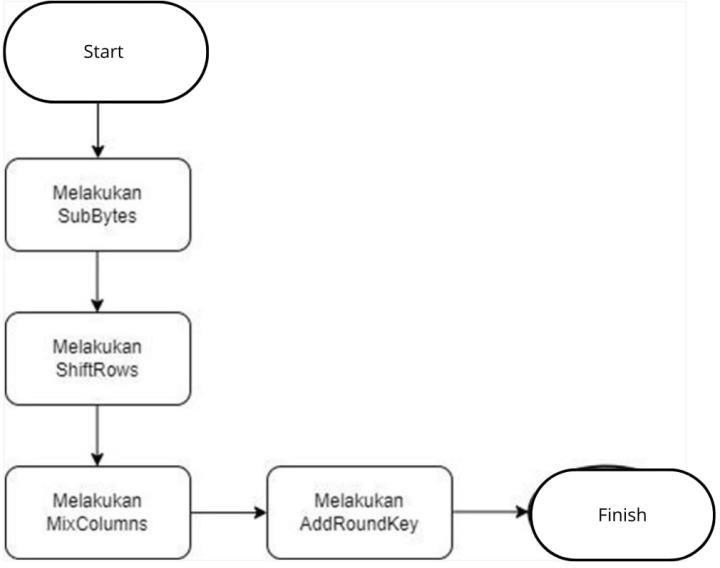
**Gambar 3.** Proses Halaman *Enkripsi* Berkas

Alur proses dari halaman dekripsi berkas dengan algoritma AES-256. Gambar di bawah adalah contoh diagram alur proses untuk proyek dekripsi file.



**Gambar 4.** Proses Halaman Dekripsi Berkas

Alur proses dari enkripsi dengan algoritma AES-256. Berikut gambar Flowchart Enkripsi AES-256.

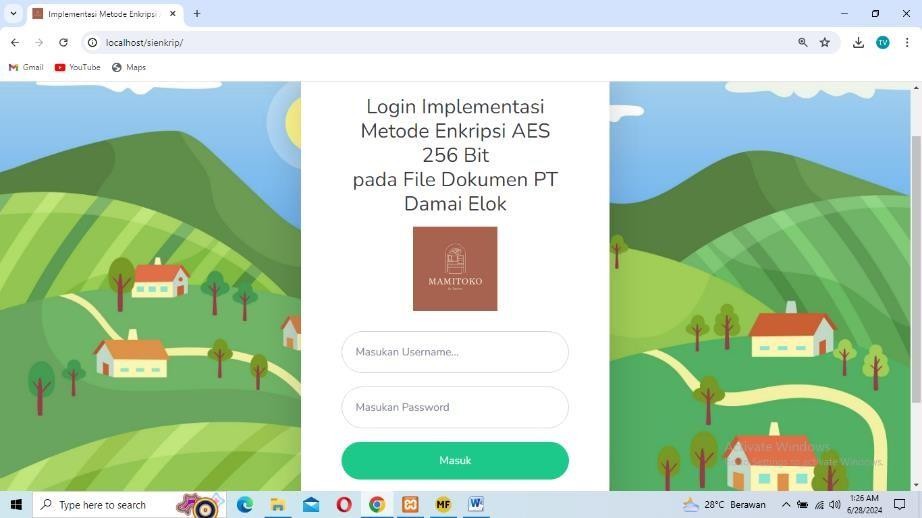


**Gambar 5.** *Enkripsi* AES- 256

Alur proses dari dekripsi dengan algoritma AES-256. Berikut gambar Flowchart Dekripsi AES-256.

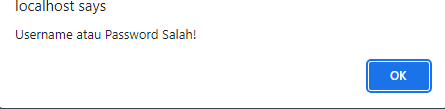
# Tampilan Layar

Layar login terdiri dari layar latar belakang, form login dengan nama pengguna, kata sandi dan tombol login. Ini adalah layar login.



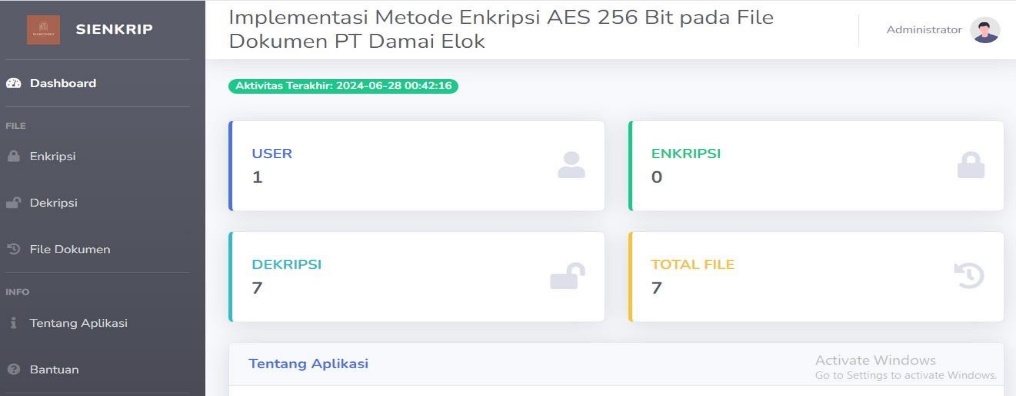
**Gambar 6.** Halaman *Login*

Pada Tampilan ini akan tampil jika username atau password yang di input salah sehingga menampilkan pesan berhasil ketika gagal login. Berikut Tampilan pesan gagal login.



**Gambar 7.** Pesan Gagal *Login*

Gambar profil di halaman beranda administrator menampilkan menu-menu yang meliputi dashboard, daftar file, enkripsi dan dekripsi. Ikon PT Damai Elok juga akan muncul di layar ini, menunjukkan jumlah file yang dienkripsi dan didekripsi. Di bawah ini adalah penjelasan singkat tentang program enkripsi, dan terdapat tombol logout di bagian bawah halaman. Layar ini muncul di layar utama administrator.



**Gambar 8.** Halaman Utama *Admin*

Pada layar daftar file operasi, terdapat tabel berisi file terenkripsi, yang meliputi identitas, nama dan nama file terenkripsi, ukuran, tanggal, status dan fungsi. Jika file didekripsi, format file dapat diubah, namun tabel tetap dienkripsi. Selain itu, terdapat menu untuk daftar file, enkripsi, dekripsi dan uninstall. Ini adalah deskripsi halaman daftar.



**Gambar 9.** Halaman Daftar Berkas *Admin*

Pada Tampilan ini enkripsi berkas admin. Berikut Tampilan layar enkripsi berkas admin.



**Gambar 10.** Enkripsi Berkas *Admin*

# Hasil Pengujian

Agar aplikasi ini berjalan dengan berhasil maka perlu di pastikan. Dengan melakukan pengujian pada aplikasi EnDe *file* yang telah dibuat. Jika tidak di uji coba aplikasi ini maka akan terjadi kegagalan pada program dan sistem aplikasinya. Di pengujian ini ada beberapa untuk mengetahui performa aplikasi, enkripsi *file* dan dekripsi *file* dengan AES-256, agar sistem yang terdapat didalam aplikasi berjalan dengan semestinya.

**Tabel 1.** Pengujian Enkripsi Berkas

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nama file awal | Ukuran asli file | Nama setelah file dienkripsi | Ukuran setelah file di enkripsi | Waktu Enkripsi |
| 11475-absensi-pim-25- feb -- 24-mar.xls | 75 KB | 59722-absensi-pim- 25-feb --24-mar.rda | 75 KB | 54.36 detik |
| 12980-  sam\_mamitoko.docx | 39.4297 KB | 2708-  sam\_mamitoko.rda | 39.4287 KB | 178.2 detik |
| 27189-pr---production--- 21062024.xlsx | 12.3135 KB | 22224-pr---  production--- 21062024.rda | 12.3135 KB | 1.27 detik |
| 49677-slip-gaji-harian- septu.xlsx | 17.9814 KB | 87984-slip-gaji- harian-septu.rda | 17.9814 KB | 37.85 detik |
| 9289-data-customer.xlsx | 33.0527 KB | 27723-data-  customer.rda | 33.0527 KB | 1.3 detik |

**Tabel 2.** Pengujian Dekripsi Berkas

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nama file awal | Path Berkas | Nama file setelah dienkripsi | Status | Waktu Dekripsi |
| 11475-absensi-pim-25- feb -- 24-mar.xls | *file*\_encrypt/59722  -absensi-pim-25- feb -- 24-mar.txt | 59722-absensi-pim- 25-feb --24-mar.rda | Deskripsi | 1.43Detik |
| 12980-  sam\_mamitoko.docx | *file*\_encrypt/2708- sam\_mamitoko.txt | 2708-  sam\_mamitoko.rda | Deskripsi | 40.28Detik |
| 27189-pr---production--- 21062024.xlsx | *file*\_encrypt/22224  -pr---production--- 21062024.txt | 22224-pr---  production--- 21062024.rda | Deskripsi | 1.22 Detik |
| 49677-slip-gaji-harian- septu.xlsx | *file*\_encrypt/87984  -slip-gaji-harian- septu.txt | 87984-slip-gaji- harian-septu.rda | Deskripsi | 57.46 Detik |
| 9289-data-customer.xlsx | *file*\_encrypt/27723  -data-customer.txt | 27723-data-  customer.rda | Deskripsi | 186.25 Detik |

# KESIMPULAN

Berdasarkan hasil tugas dengan membuat Implementasi Metode Enkripsi AES 256 Bit pada *File* PT.DAMAI ELOK dapat ditarik kesimpulan yaitu dengan adanya Implementasi Metode Enkripsi AES 256 Bit pada *File* ini dapat membantu untuk meminimalisir kebocoran dan penyalahgunaan data *file*, serta menjaga keamanan *file* yang dianggap penting untuk dijaga kerahasiaannya dari siapapun melalui proses enkripsi dengan Metode Enkripsi AES 256 Bit.

# DAFTAR PUSTAKA

1. Andriyanto, R., Khairijal, D. S., Prodi, T., Informatika, S., Tinggi, T., Dumai, J., Utama, K., Bukit, B. I. K., & Dumai, I. Penerapan Kriptografi AES Class Untuk Pengamanan URL WEBSITE Dari Serangan SQL INJECTION, Jurnal Teknik Informatika, 13(1), pp. 61-64, 2020.
2. Asih, I., Simbolon, R., Gunawan, I., Kirana, I. O., Dewi, R., & Solikhun, S. Penerapan Algoritma AES 128-Bit dalam Pengamanan Data Kependudukan pada Dinas Dukcapil Kota Pematangsiantar, Journal of Computer System and Informatics (JoSYC), 1(2), pp. 54-60, 2020.
3. Azhari, M., Perwitosari, J., & Ali, F. Jurnal Pendidikan Sains dan Komputer, Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES), 2(1), pp. 2809–476, 2022.
4. Cristy, N., & Riandari, F, Niolinda Cristy 1 , Fristi Riandari. Implementasi Metode Advanced Encryption Standard (AES 128 Bit) Untuk Mengamankan Data Keuangan, Jurnal Ilmu Komputer dan Sistem Informasi, 4(2), pp. 75, 2021.
5. Eka Putri, A., Kartikadewi, A., & Abdul Rosyid, L. A. 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. Applied Information System and Management (AISM), 3(2), pp. 69– 78, 2021.
6. Hulu, D., Nadeak, B., & Aripin, S. Implementasi Algoritma AES (Advanced Encryption Standard) Untuk Keamanan File Hasil Radiologi di RSU Imelda Medan, Konferensi Nasional Teknologi Infomasi dan Komputer, 4(1), pp. 78-86, 2020.
7. Sihombing, B., Patresia, D., Manrung, S., Ahadi, E., & Gunawan, I. Pengamanan Pesan Teks Menggunakan Kriptofrafi Algoritma Vigenere Chiper Dari Serangan Eavesdropping. Jurnal Teknik Informatika Kaputama (JTIK), 4(1), pp. 89-94, 2020.
8. Susanto, E., & Rizki, S. N. Perangkat Lunak Keamanan Berbasis File Menggunakan Algoritma Kriptografi Vigenere Cipher. Jurnal Comasie, 4(6), pp. 66-74, 2021.
9. Widyawan & Imelda. Pengamanan File Menggunakan Kriptografi Dengan Metode Aes-128 Berbasis Web Di Komite Nasional Keselamatan Transportasi, Jurnal Nasional Informatika dan Teknologi Jaringan, 4(1), pp. 15-22, 2021.
10. Zalukhu, K., Kom, S., Kom, M., & Murniyanti, S. Implementasi Sistem Keamanan Database Data Pelanggaran Hukum Disiplin Prajurit Menggunakan Algoritma Advanced Encryption Standard 128 Bit Pada Pengadilan Militer I-02 Medan, Jurnal Sistem Informasi, 2(1), pp. 88-93, 2020.