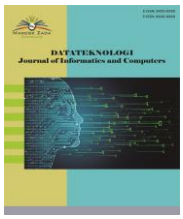
DATA TEKNOLOGI
Journal of Informatics and Computers
Vol. 1, No. 1, April (2023), Page 9-15
P-ISSN (2985-9689) & E-ISSN (2986-0687)



Penerapan Algoritma Advanced Encryption Standard Untuk Mengamankan File Gambar Pada Layanan Berbasis Web

Alwi Aulia[1], Heri Gunawan[2]

[1]Prodi Teknik Informatika, Fakultas Teknik dan Ilmu Komputer, Universitas Potensi Utama, Indonesia
[2]Prodi Rekayasa Perangkat Lunak, Fakultas Teknik dan Ilmu Komputer, Universitas Potensi Utama, Indonesia
*Corresponding Author. E-mail: alwiaulia21@gmail.com

Abstrak

Perkembangan teknologi yang semakin maju berdampak juga terhadap teknologi yang digunakan oleh masyarakat. Namun teknologi yang berkembang tidak selalu menghasilkan dampak positif. Salah satu dampak negatif dari teknologi adalah maraknya pencurian data pribadi seperti gambar yang dilakukan oleh pihak–pihak yang tidak bertanggung jawab. Pengamanan gambar melalui media elektronik memerlukan suatu proses yang dapat menjamin keamanan gambar tersebut. Gambar tersebut harus tetap rahasia dengan bertujuan untuk menjaga karahasiaannya terhadap akses orang-orang yang tidak berhak. Penelitian ini difokuskan pada perancangan sistem untuk mengamankan gambar dengan menggunakan algoritma AES (Advanced Encryption Standart) untuk mengenkripsi dan mendekirpsi gambar. Sistem dibangun berbasis web yang bertujuan untuk membantu pengguna agar mudah mengakses aplikasi yang dibuat karena bersifat online dan multiuser. Dengan demikian, hasil penelitian ini dapat memberikan kontribusi kepada publik dalam hal sarana pengamanan gambar, yaitu untuk melindungi gambar yang bersifat pribadi dan tidak seharusnya menjadi konsumsi masyarakat luas serta kemudahan akses aplikasi.

Kata kunci: aes, *web*, pengamanan gambar

Abstract

The development of increasingly advanced technology has an impact on the technology used by society. However, developing technology does not always produce a positive impact. One of the negative impacts of technology is the rampant theft of personal data such as images by irresponsible parties. Image security through electronic media requires a process that can guarantee the security of the image. The image must remain confidential with the aim of keeping it confidential from access by unauthorized persons. This research is focused on designing a system to secure images by using the AES (Advanced Encryption Standard) algorithm to encrypt and decrypt images. The system is built based on the web which aims to help users to easily access the applications created because they are online and multi-user. Thus, the results of this study can contribute to the public in terms of image security facilities, namely to protect images that are private and should not be consumed by the wider community as well as easy access to applications.

Keywords*: aes, web, image security*

PENDAHULUAN

Seiring dengan kemajuan teknologi informasi maka sangat diperlukan sebuah keamanan data terhadap kerahasiaan informasi yang saling dipertukarkan melalui jaringan internet, apa lagi jika data tersebut dalam suatu jaringan komputer yang terhubung atau terkoneksi dengan jaringan lain. Hal tersebut tentu saja menimbulkan resiko bila informasi yang

Submitted	Accepted	Published	
04-02-2023	06-02-2023	12-02-2023	: https://doi.org/10.56248/datateknologi.v1i1.46

sensitif dan berharga tersebut di akses oleh orang yang tidak bertangung jawab (Ibrahim, 2017). Salah satu dampak *negatif* dari teknologi adalah maraknya pencurian data pribadi seperti gambar yang dilakukan oleh pihak–pihak yang tidak bertanggung jawab, sehingga jika data pribadi diberitakan ke publik oleh orang yang tidak bertanggung jawab tersebut, akan menimbulkan dampak yang kurang etis bahkan dapat menjadi bahan *pornografi*. Hal ini terjadi karena belum banyak aplikasi yang mudah digunakan publik untuk mengamankan data pribadi khususnya gambar.

Kriptografi merupakan studi matematika yang mempunyai hubungan dengan aspek keamanan informasi seperti integritas data, keaslian entitas dan keaslian data. *Kriptografi* menggunakan berbagai macam teknik dalam upaya untuk mengamankan data termasuk gambar. Pengamanan gambar melalui media elektronik memerlukan suatu proses yang dapat menjamin keamanan gambar tersebut. Gambar tersebut harus tetap rahasia dengan bertujuan untuk menjaga karahasiaannya terhadap akses orang-orang yang tidak berhak (Simatupang, 2017)

AES merupakan algoritma block cipher dengan sistem permutasi dan substitusi. Ada tiga jenis algoritma *AES*, yaitu *AES*-128, *AES*-192, dan *AES*-256. Pengelompokan ini berdasarkan panjang kunci yang digunakan pada algoritma *AES*. Selain itu ada beberapa hal lain yang membedakan antar jenis algoritma *AES*, yaitu round yang digunakan. *AES*-128 menggunakan 10 round, *AES*-192 menggunakan 12 round, dan *AES*-256 menggunakan 14 round (Chandra, 2018). *AES* merupakan sistem penyandian blok yang bersifat non-feistel kerena *AES* menggunakan komponen yang selalu memiliki invers dengan panjang blok 128. Penyandian *AES* menggunakan proses yang berulang disebut dengan ronde. jumlah ronde yang digunakan oleh *AES* tergantung panjang kunci yang digunakan (Hasibuan, 2017).

Analisis kriptografi AES (Advanced Encryption Standard) berupa proses enkripsi dan dekripsi dengan AES dengan ukuran kunci 128-bit dalam mengamankan plaintext agar hanya bisa dibaca oleh pihak yang mengetahui secret key saja. dalam hal ini data yang akan dienkripsi pada aplikasi kriptografi ini adalah file berjenis dokumen teks, gambar, video, dan music (Hartato et al., 2019).

Peneliti menggunakan *AES* dikarenakan *AES* sebagai salah satu algoritma yang penting tentu memiliki berbagai kegunaan yang sudah diaplikasikan atau diimplementasikan di kehidupan sehari-hari yang tentu saja membutuhkan suatu perlindungan atau penyembunyian informasi di dalam prosesnya. Salah satu contoh penggunaan *AES* adalah pada kompresi 7-Zip dan WinZip.

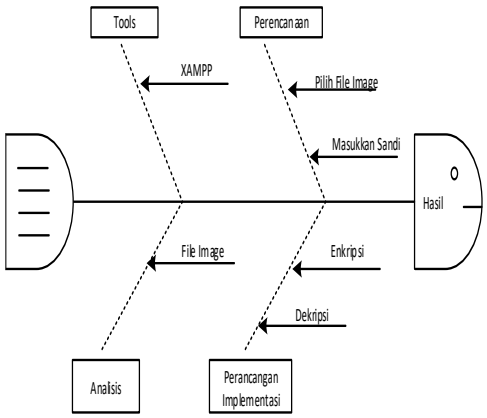
Fenomena yang ditemukan dalam penelitian ini yaitu jika data gambar tidak diamankan, data gambar bisa saja diakses oleh orang yang tidak bertanggung jawab dan pentingnya pengamanan untuk melindungi *privasi* atau kerahasiaan data. Penelitian ini difokuskan pada perancangan sistem untuk mengamankan gambar dengan menggunakan algoritma *AES (Advanced Encryption Standart)* untuk mengenkripsi dan mendekirpsi gambar. Sistem dibangun berbasis *web* yang bertujuan untuk membantu pengguna agar mudah mengakses aplikasi yang dibuat karena bersifat *online* dan *multiuser*. Dengan demikian, hasil penelitian ini dapat memberikan kontribusi kepada publik dalam hal sarana pengamanan gambar, yaitu untuk melindungi gambar yang bersifat pribadi dan tidak seharusnya menjadi konsumsi masyarakat luas serta kemudahan akses aplikasi.

Berdasarkan permasalahan tersebut, penulis mengangkat sebuah judul **"Penerapan Algoritma *AES (Advanced Encryption Standard)* Untuk Mengamankan File Gambar Pada Layanan Berbasis Web"**

P-ISSN (2985-9689) & E-ISSN (2986-0687)

METODE

Tahapan dalam penelitian ini dapat di modelkan dengan *Fishbone* metodologi penelitian. Adapun beberapa tahapan yang digunakan dalam penelitian ini adalah sebagai berikut :



Gambar 1. Prosedur Perancangan Sistem

Dalam pengembangannya metode *waterfall* memiliki beberapa tahapan yaitu : *requirement* (analisis kebutuhan), design sistem (*system design*), *coding*, pengujian program, pemeliharaan sistem

1. Analisis Kebutuhan

Peneliti menganalisis kebutuhan untuk perancangan sistem berupa *hardware* dan *software* yang nantinya akan digunakan untuk penelitian ini.

2. Desain Sistem

Pada tahap ini peneliti merancang sebuah desain aplikasi pengamanan gambar dengan menggunakan algoritma AES Serta menggunakan pemodelan UML yaitu *use case diagram, class diagram, activity diagram, dan sequence* diagram untuk perancangan system.

3. Penulisan Sinkode Program

Pada proses pengamanan gambar peneliti menggunakan bahasa pemrograman PHP dan menggunakan database MySQL dalam pembuatan system.

4. Pengujian Program

Pada tahap ini peneliti melakukan pengujian aplikasi pengamanan gambar apakah sudah dapat mengamankan gambar dengan baik dan benar.

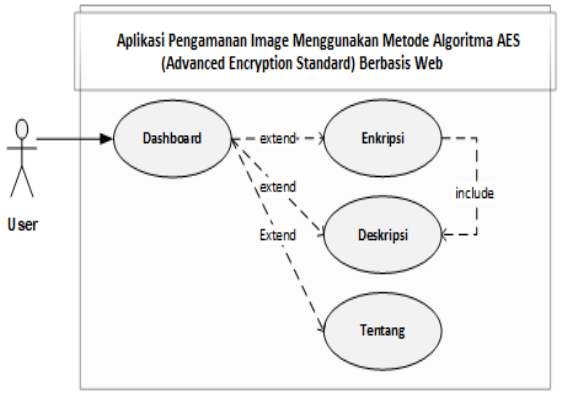
5. Pemeliharaan Sistem

Pada tahapan ini peneliti telah menyelesaikan seluruh penelitian baik teori maupun aplikasi yaitu Aplikasi Pengamanan Gambar Menggunakan Metode Algoritma *AES (Advanced Encryption Standard)* Berbasis *web*.

HASIL DAN PEMBAHASAN

Use Case Diagram

Sistem yang akan dirancang digambarkan dengan *usecase diagram* yang terdapat pada Gambar 2 berikut :



Gambar 2. Usecase Diagram

Berikut ini adalah tampilan hasil dari aplikasi *enkripsi* gambar dengan menggunakan algortima *AES*, untuk lebih jelasnya dapat di lihat pada gambar-gambar di bawah ini :

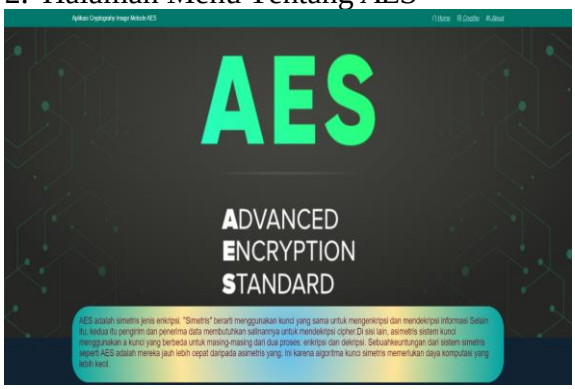
1. Halaman Utama

Gambar 3. Halaman Utama

Home merupakan tampilan halaman utama dari aplikasi enkripsi *image* dengan menggunakan algortima *AES*, pada bagian ini langsung di tampilkan halaman yang berfungsi untuk melakukan proses enkripsi dan dekripsi, pada bagain ini juga terdiri dari 3 (tiga) buah tombol menu yaitu tombol *Home*, Tentang *AES* dan *About*,

yang masing-masing memiliki fungsi berbeda.

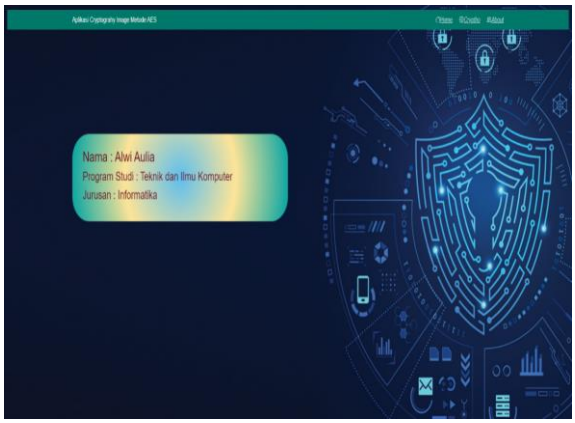
2. Halaman Menu Tentang *AES*



Gambar 4. Tampilan menu Tentang AES

Halaman ini berfungsi untuk menjelaskan secara singkat mengenai Algoritma *AES*

3. Halaman Menu *About*

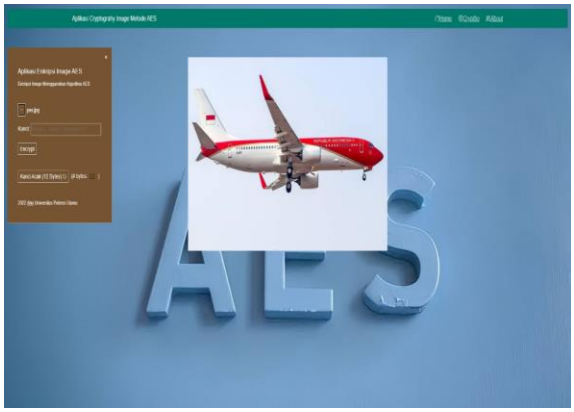


Gambar 5. Menu About

Halaman menu *About* adalah merupakan tampilan dari halaman yang menampilkan informasi singakat dari aplikasi dan juga informasi singkat dari pengembang aplikasi.

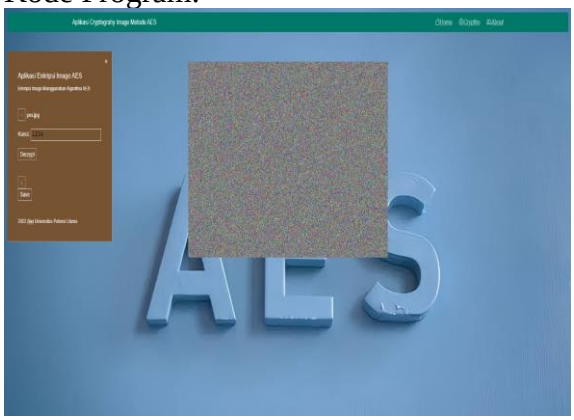
4. Halaman Menu Enkripsi

Halaman ini adalah halaman yang berfungsi untuk melakukan proses enkripsi, pada halaman ini pengguna dapat memilih *file image* yang akan di *enkripsi* dan memasukan kunci yang akan dipergunakan untuk melakukan proses enkripsi, seperti yang terlihat pada gambar 4 berikut ini :



Gambar 5. Halaman Enkripsi

Untuk melakukan proses enkripsi pada gambar yang diinginkan, hal pertama yang dilakukkan pengguna adalah memasukan kunci dimana kunci dapat berupa perpaduan angka, simbol atau huruf kecuali spasi, setelah memasukkan kunci, *user* harus memilih *folder* yang nantinya sebagai tempat penyimpanan untuk gambar, kemudian klik kotak gambar untuk memilih gambar yang ingin diamankan, setelah selesai memilih maka *user* harus memasukkan nama *file* hasil enkripsi untuk disimpan, proses pilih gambar dapat diulang sebanyak 4 kali agar tidak terlalu lama dalam proses *upload* berkas gambar ke dalam *web server*. Proses enkripsi akan diproses setelah pengguna memilih tombol *Encrypt*. Kode program untuk menampilkan gambar ke dalam kanvas dapat dilihat pada Kode Program.



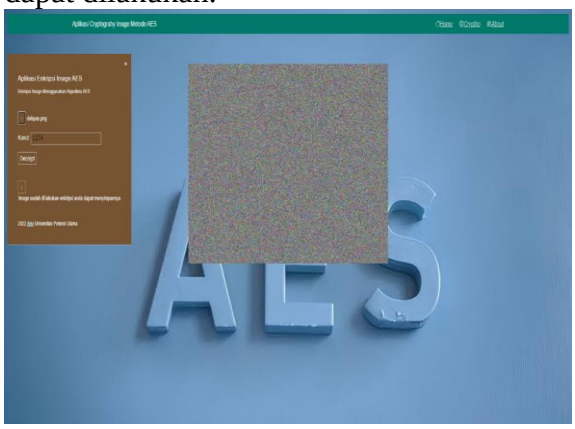
Gambar 6. Halaman Hasil Enkripsi

File yang dihasilkan dari proses *enkripsi* dapat di simpan kembali kedalam jenis *file* yang sama.

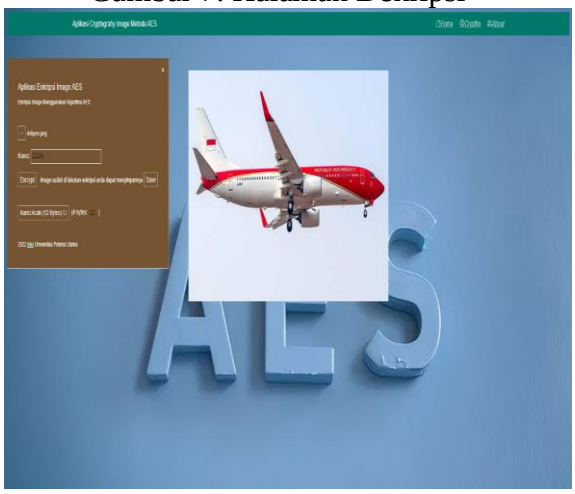
P-ISSN (2985-9689) & E-ISSN (2986-0687)

5. Halaman Dekripsi

Pada halaman dekripsi pengguna dapat memilih *image* yang telah di enkripsi, dan memasukan kunci yang sama dengan kunci yang dipergunakan saat melakukan proses dekripsi, jika kunci yang pergunakan tidak sama, maka proses dekripsi tidak dapat dilakukan.

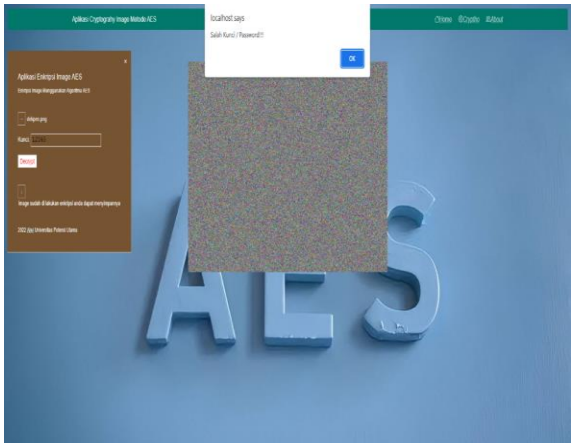


Gambar 7. Halaman Dekripsi



Gambar 8. Halaman Hasil Dekripsi

Untuk melakukan proses dekripsi pada gambar yang diinginkan, hal pertama yang dilakukkan pengguna adalah *user* harus mengklik kotak gambar untuk memilih gambar yang ingin di dekripsi. Lalu masukan kunci yang sama dengan kunci yang dipergunakan saat melakukan proses *enkripsi*, setelah memasukkan kunci, *user* harus mengklik menu dekripsi. Maka gambar akan kembali seperti gambar awal sebelum di Enkripsi.



Gambar 9. Halaman Kunci Salah

Jika melakukan proses dekripsi dengan memasukkan kunci yang salah atau berbeda maka proses enkripsi gagal dan *image* tidak mengalami proses dekripsi.

Skenario Pengujian

Pengujian ini bertujuan untuk memastikan bahwa aplikasi enkripsi gambar yang telah berhasil dibangun dapat berkerja dengan baik dan tidak ada terjadi kesalahan dalam proses pengoperasiannya

Tabel 1. Pengujian Menu

No	Pengujian	Target Pengujian	Pengamatan	Kesimpulan
1	Menu *Home*	Berpindah kehalaman *home* dari halaman sebelumnya dan menampilkan *form* utama enkripsi dan dekripsi	Menampilkan halaman *Home*	Hasil Pengujian Berhasil
2	Menu Tentang *AES*	Menampilkan halaman yang berisikan informasi singkat mengenai Algoritma *AES*	Menampilkan halaman Tentang *Aes*	Hasil Pengujian Berhasil
3	Menu *About*	Menampilkan informasi halaman dari menu *about*	Menampilkan Halaman *About*	Hasil Pengujian Berhasil

Tabel 2. Tabel Pengujian Enkripsi dan Dekripsi

No	Pengujian	Target Pengujian	Pengamatan	Kesimpulan
1	Enkripsi *file* dengan menggunakan *file image* yang berekstensi jpg,jpeg dan png	Menampilkan hasil Enkripsi dalam ukuran yang sama dan menampilkan hasil piksel secara acak. Hasil Enkripsi dapat tetap dibuka dengan menggunakan aplikasi *image Viewer* atau aplikasi sejenisnya.	Proses enkripsi berhasil, hasil enkripsi berupa piksel yang tersusun acak, dan dapat dibuka dalam aplikasi *image viewer* atau aplikasi sejenisnya.	Hasil Pengujian Berhasil
2	Dekripsi *file* dengan kunci berbeda	Melakukan proses dekripsi dengan menggunakan kunci yang berbeda dengan kunci yang dipergunakan saat melakukan proses enkripsi. Proses enkripsi gagal dilakukan.	Proses enkripsi gagal karena kunci tidak sesuai dan *image* tidak mengalami proses dekripsi	Hasil Pengujian Berhasil
3	Dekripsi dengan menggunakan Kunci yang benar	Mengembalikan *image* menjadi *image* asli	Berhasil melakukan proses dekripsi dan menghasilkan *image* asli	Hasil Pengujian Berhasil

Kelebihan dan Kekurangan Sistem

Berikut ini adalah kelebihan dan kekurangan sistem yang telah dibuat.

Kelebihan Sistem

Kelebihan sistem ini diantaranya yaitu :

1. Aplikasi menggunakan *user interface* yang sederhana, sehingga mudah untuk di pahami.
2. Dapat melakukan proses enkripsi terhadap *file* berektensi jpg, jpeg dan png.
3. Tidak ada pembatasan kapasitas *file* yang dipergunakan dalam melakukan proses enkripsi.
4. Hasil dari proses enkripsi tidak dapat di kenali.
5. *File* hasil proses enkripsi dan *dekripsi* dapat disimpan kedalam bentuk *file*.

Kekurangan Sistem

Berikut ini adalah kekurangan yang dimiliki aplikasi, diantanya adalah :

1. Aplikasi bersifat terbuka sehingga tidak menggunakan *login* untuk mengakses aplikasi.
2. Tidak ada penggunaan *database* di dalam aplikasi.
3. Proses utama yang ada didalam aplikasi hanya proses untuk melakukan enkripsi dan dekripsi.
1. Hanya dapat melakukan enkripsi terhadap *file image*.

KESIMPULAN

Dari hasil penelitian yang dilakukan, maka dapat di ambil kesimpulan sebagai berikut: 1). Algoritma *AES* merupakan algoritma yang sulit dipecahkan, karena algoritma *AES* 128 bit memiliki ruang kunci 2^{128} yang merupakan nilai yang sangat besar dan dianggap aman untuk digunakan sehingga terhindar dari *brute force attack*, 2). Pada proses enkripsi *AES* mengunakan 4 transformasi dasar dengan urutan trasformasi *subbytes*, *shiftrows*, *mixcolumns*, dan *addroundkey*. Sedangkan pada proses *dekripsi* mengunakan *invers* semua transformasi dasar pada algoritma *AES* kecuali *addroundkey* dengan urutan transformasi *invshiftrows*, *invsubbytes*, *addroundkey*,dan *invmixcolumns*, 3). Proses yang dibutuhkan untuk melakukan enkripsi terhadap sebuah *file* gambar memakan waktu yang relatif lama, tergantung dengan ukuran atau besar *file* dan kunci yang dipergunakan.

DAFTAR PUSTAKA

Chandra, R. V. H. (2018). *Analisa Performa Proses Enkripsi Dan Dekripsi Menggunakan Algoritme Aes-128 Pada Berbagai Format File*. (Doctoral dissertation, Universitas Brawijaya).

Ibrahim, A. A. (2017). Perancangan Pengamanan Data Menggunakan Algoritma AES (Advanced Encyption

Standard). *Jurnal Teknik Informatika, 3*(1), 53-60.

Hartato, E., Guanawan, I., Parlina, L., & Wanto, A. (2020). Analisis Algoritma *AES* Dalam Mengamankan Data Pada Kantor Walikota Pematang Siantar. *Means, 8*(2), 15-25.

Hasibuan, A. M. (2017). Rancang Bangun Aplikasi Keamanan Data Menggunakan Metode AES Pada Smartphone. *MEANS (Media Informasi Analisa dan Sistem), 1*(1), 29-35.

Simatupang, A. W. (2017). Aplikasi Pengamanan Data Gambar Dengan Menerapkan Algoritma Vigenere Chiper. *MEANS (Media Informasi Analisa dan Sistem), 1*(1),66-72.