Jurnal Informatika Logika
Volume 1, Nomor 1, Februari 2024, Page 8-17
ISSN 0000-0000 (media online)
Available Online at https://idpress.ac.id/index.php/jil/index
DOI : --

Pengujian Algoritma Kriptografi Rijndael Untuk Keamanan Audio Menggunakan Visual Basic .Net

Tomy Satria Alasi[1] , Marwa Halim[2]
[12] STMIK Methodist Binjai, Sarjana Teknik Informatika, Binjai, Indonesia
Email: [1*]tomysatriaalasi@live.com, [2]marwahalim@methodistbinjai.sch.id
Email Penulis Korespondensi: tomysatriaalasi@live.com

Abstrak– Kriptografi merupakan salah satu ilmu yang digunakan untuk menjaga keamanan dan kerahasiaan data atau informasi sehingga data tidak dapat diketahui oleh pihak-pihak yang tidak berwenang. Proses pertukaran data atau informasi sangat sering dilakukan sehingga aspek keamanan terhadap isi data sangat perlu untuk mendapat perhatian khusus. Penelitian ini akan mengimplementasikan kriptografi algoritma AES 128 untuk menyandikan *file* digital, khususnya adalah *file* audio. Enkripsi dilakukan dengan menggunakan kunci tertentu, sehingga menghasilkan cipherdata yang tidak dapat dibaca ataupun dimengerti. Cipherdata tersebut dikembalikan seperti semula jika di deskripsi menggunakan kunci yang sama sewaktu mengenkripsi file tersebut. Perangkat lunak yang digunakan untuk merancang aplikasi adalah Visual Basic .Net. Algoritma AES dipilih untuk metode pengimplementasian pengamanan data audio. Penelitian ini secara khusus akan mengamati perubahan extensi dari file untuk proses enkripsi dan deskripsi, serta melihat apakah file akan rusak jika dienkripsi ataupun dideskripsi.

Kata Kunci: Kriptografi; Algoritma AES-128; Enkripsi; Deskripsi; File Audio;

Abstract– Cryptography is one of the sciences used to maintain the security and confidentiality of data or information so that data cannot be known by unauthorized parties. The process of exchanging data or information is very often carried out so that the security aspect of data content really needs special attention. This research will implement the AES 128 cryptographic algorithm to encode digital files, specifically audio files. Encryption is done using a specific key, resulting in a cipher that cannot be read or understood. The cipher data is restored as it was if decrypted using the same key when encrypting the file. The software used to design the application is Visual Basic. The AES algorithm was chosen for the method of implementing audio data security. This study will specifically observe changes in the extension of files for encryption and decryption, and see if files will be damaged if encrypted or decrypted.

Keywords: Cryptography; Aes-128 Algorithm; Encryption; Decryption; Audio Files;

1. PENDAHULUAN

Perkembangan teknologi komputer dan telekomunikasi yang cukup pesat masa kini berpengaruh pada penggunaan informasi[1]. Sehingga melahirkan sebuah istilah "*information-based society*" dimana kemampuan untuk mengakses dan menyediakan informasi[2] secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi atau lembaga, baik organisasi komersial (perusahaan), perguruan tinggi (akademisi), lembaga pemerintahan (birokrasi), maupun individual (pribadi). Seiring dengan perkembangan Teknologi telekomunikasi dan penyimpanan data dengan menggunakan komputer tersebut[3], memungkinkan pengiriman data jarak jauh yang relatif cepat dan murah. Dilain pihak pengiriman data jarak jauh melalui jaringan internet, gelombang radio maupun media lain yang digunakan masyarakat luas (public) sangat memungkinkan pihak lain dapat menyadap dan mengubah data yang dikirim. Perkembangan internet salah satunya sebagai sarana komunikasi merupakan teknologi yang mampu menyikapi persoalan-persoalan yang semakin kompetitif saat ini, terbukti dengan pemakai internet yang sudah mendunia[4]. Semakin mudahnya mendapatkan akses dari internet membuat dunia seolah-olah tidak ada batasan lagi, sehingga adanya internet memang sejalan dengan era globalisasi dan kebijakan pasar bebas[5]. Dibalik perkembangan dan pemanfaatan internet yang demikian pesat, ternyata ada bahaya yang mengancam yakni fenomena yang kurang disadari oleh para user (pengguna internet) pemula[6], yaitu user yang kurang memahami tentang keamanan data[7][8]. Untuk meminimalkan kemungkinan terjadinya tindak kejahatan di internet inilah diperlukan teknologi keamanan informasi, khususnya sistem dan mesin enkripsi (penyandian)[9][10]. Enkripsi merupakan bagian dari cabang kriptografi, dimana algoritma kriptografi untuk penyandian telah mengalami perkembangan dan perbaikan dari masa ke masa[11]. Sehingga proses tersebut menghasilkan algoritma yang memuaskan, misalnya DES, IDEA, RSA, dan lain-lain. AES lahir pada November 2001 dengan pencetus Rijmen dan Daemen (Rijndael) cukup mengejutkan dunia kriptografi[12], karena pada saat itu menyisihkan empat finalis algoritma lainnya yang cukup popular yaitu MARS, RC6, Serpent, dan Twofish. AES diberlakukan secara efektif pada tahun 2002 dan mendapatkan sertifikat dari NIST, AES memang dipersiapkan untuk penerapan software, firmware, hardware atau kombinasinya[13]. Jadi, suatu hal yang cukup wajar bila usaha pengembangannya banyak dan bervariasi[3][2][14][15]. Kelebihan dari Algoritma Rijndael adalah memiliki properti ketahanan terhadap semua jenis serangan yang telah diketahui, kesederhanaan rancangan, dan kekompakan kode serta kecepatan komputasi pada berbagai platform.

Masalah yang akan dibahas dalam pembuatan sistem pengamanan file audio dengan menggunakan kriptografi Rijndael adalah bagaimana mengamankan file audio dengan alogaritma kriptografi AES:Rijndael 128 bit. Kemduian bagaimana merancang aplikasi untuk pengamanan file audio dengan metode AES 128 bit.

Submitted: **01/01/2024**; Accepted: **15/02/2024**; Published: **01/02/2024**

Jurnal Informatika Logika
Volume 1, Nomor 1, Februari 2024, Page 8-17
ISSN 0000-0000 (media online)
Available Online at https://idpress.ac.id/index.php/jil/index
DOI : --

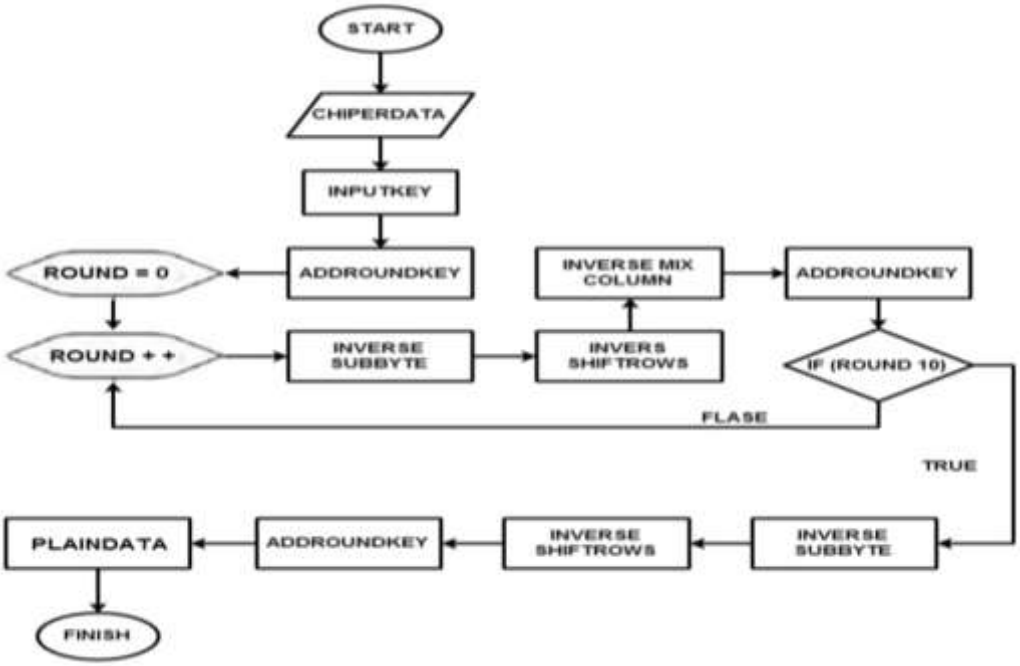
2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Adapun metodologi penelitian yang digunakan adalah :
Studi literatur, studi literatur ini dilakukan untuk mengumpulkan dan mempelajari *block chiper*, kunci simetris, dan algoritma kriptografi yaitu Rijndael melalui sumber-sumber yang dimiliki oleh penulis antara lain, sumber literatur berupa buku dan situs internet. Dengan pendekatan, Menjelaskan tentang fenomena pentingnya pengamanan data, kriptografi adalah salah satu jawabannya. Algoritma kriptografi yang cukup popular pada tahun 80-an adalah DES akan tetapi diganti dengan AES yang mempunyai banyak kelebihan dan keunggulan dari DES, terutama dalam kekuatan pemecahan kunci Algoritmanya. Menjelaskan kriptografi dari sejarahnya, teknik, dan metode serta landasan yang menjadi dasar terbentuknya teknik-teknik yang digunakan dalam Algoritma AES. Menjelaskan teknik yang membangun algoritma AES, tetapi sebelumnya dijelaskan dulu tentang pengertian dan kemampuan AES sebagai penghantar kepada algoritmanya. Menjelaskan simulasi program sebagai hasil dari gambaran model Algoritma AES dengan panjang kunci 128 *bit*. Menjelaskan kesimpulan dan saran penelitian lebih lanjut.

3. HASIL DAN PEMBAHASAN

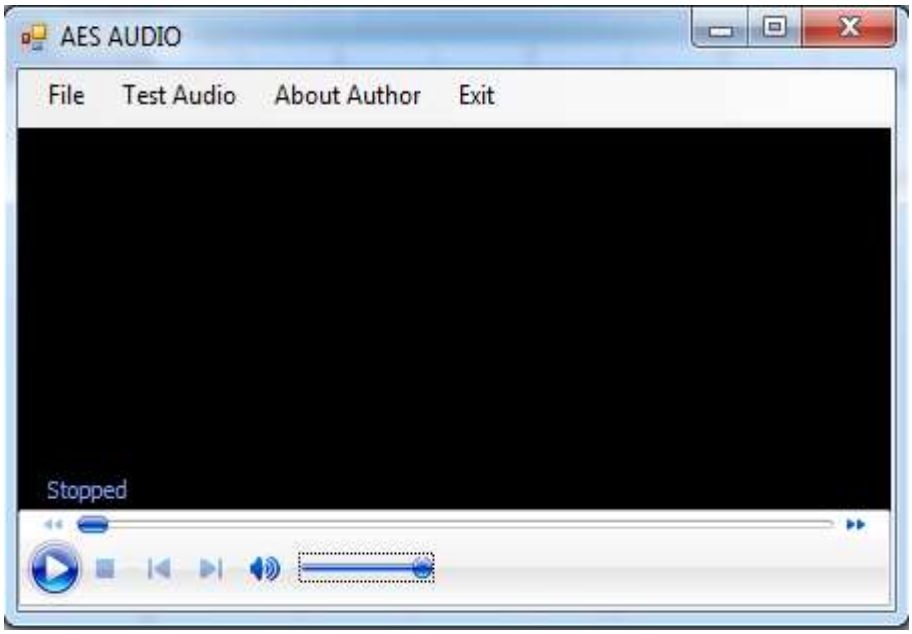
Pada proses deskripsi dilaksanakan dengan cara membagi cipherdata(data terenkrip) berdasarkan *blockcipher* (*round*),dan selanjutnya password yang di inputkan oleh user kemudian akan melewati proses add round key yang akan menjadwalkan password sebanyak 10 kali,yang nantinya akan digunakan dalam proses deskripsi yang menggunakan perulangan sebanyak 10 kali. Proses deskripsi sendiri terdiri dari empat proses terpisah yang akan dilakukan sebanyak 10 kali perulangan dengan aturan,pada perulangan pertama hingga ke sembilan akan melewati proses invers sub bytes, invers shiftrows, invers mix columns dan add round key. Sedangkan perulangan ke 10 akan menghilangkan proses invers mix columns yang akan menandakan akhir dari proses deskripsi cipherdata(data terenkrip).



Gambar 1. Flowchart Proses Deskripsi

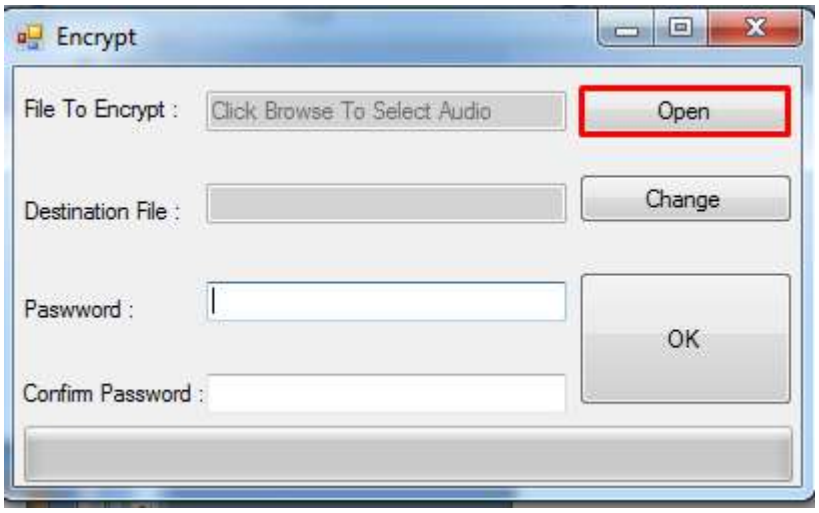
Submitted: **01/01/2024**; Accepted: **15/02/2024**; Published: **01/02/2024**

Jurnal Informatika Logika
Volume 1, Nomor 1, Februari 2024, Page 8-17
ISSN 0000-0000 (media online)
Available Online at https://idpress.ac.id/index.php/jil/index
DOI : --



Gambar 2. Interface Utama

Pada gambar ditampilkan interface awal dari aplikasi yang dirancang. Pada halaman ini tampilan aplikasi berfokus pada penginputan data awal (*plaindata*) yang akan diproses dan sekaligus mengarahkan pengguna dalam pelaksanaan proses enkripsi.

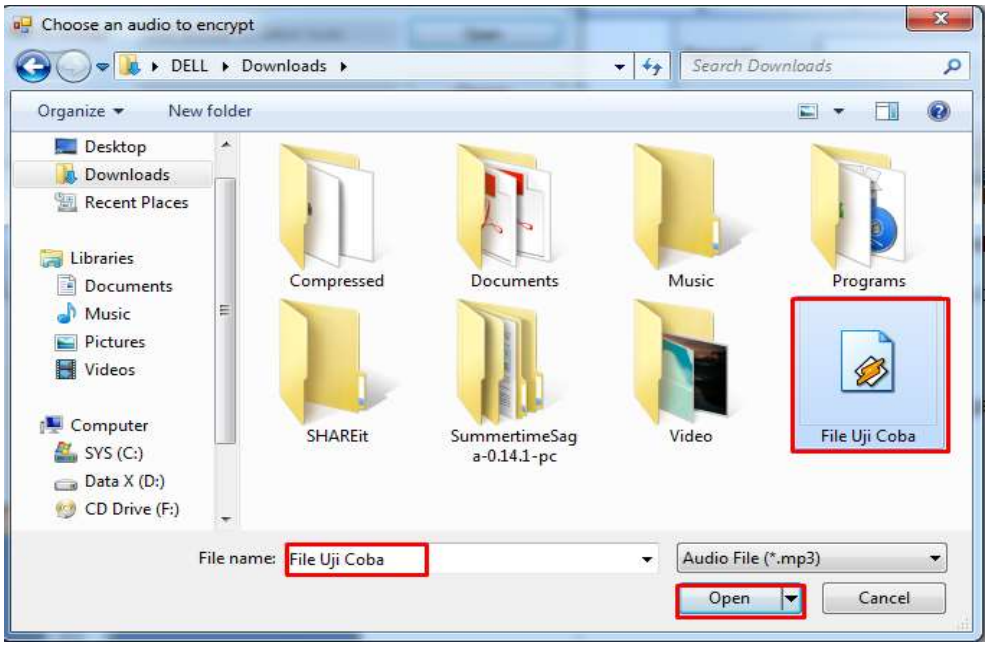


Gambar 3. Gambar Interface Enkrip

Setelah pengguna melewati halaman pertama user akan memilih data yang akan melewati proses enkripsi. Pada gambar tampak tampilan halaman enkripsi, pada halaman ini pengguna akan diarahkan untuk memilih data yang akan dienkrip dengan menekan tombol "*open"* yang kemudian akan memindahkan pengguna pada halaman load untuk memilih data.

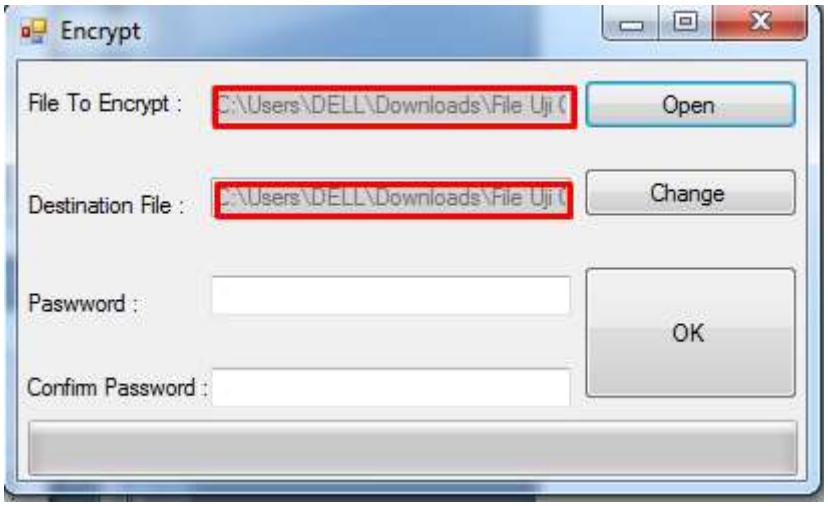
Submitted: **01/01/2024**; Accepted: **15/02/2024**; Published: **01/02/2024**

Jurnal Informatika Logika
Volume 1, Nomor 1, Februari 2024, Page 8-17
ISSN 0000-0000 (media online)
Available Online at https://idpress.ac.id/index.php/jil/index
DOI : --



Gambar 3. *Browse File Audio*

Setelah pengguna menekan tombol ”*open*” selanjutnya pengguna akan dipindahkan pada windows explorer yang akan membantu pengguna untuk memilih data yang akan di enkrip, penggunaan load data dengan memanfaatkan eindows explorer ini mengikuti standar *load data* pada aplikasi-aplikasi berbasis windows lainnya dengan tujuan untuk membuat user lebih nyaman dan mampu memahami fungsi sistem dengan baik. Pada gambar tampak bahwasanya file dengan nama “File Uji Coba” dipilih untuk melewati proses enkripsi. Perlu diingatkan kembali bahwasanya data yang mampu dibaca oleh sistem adalah data dengan ekstensi .mp3 atau file audio, apabila user membuka data selain dari ekstensi yang telah ditentukan sebelumnya dipastikan sistem tidak dapat berjalan sesuai dengan tujuan pembuatannya dan tidak mampu menyelesaikan proses yang diperintahan oleh pengguna.

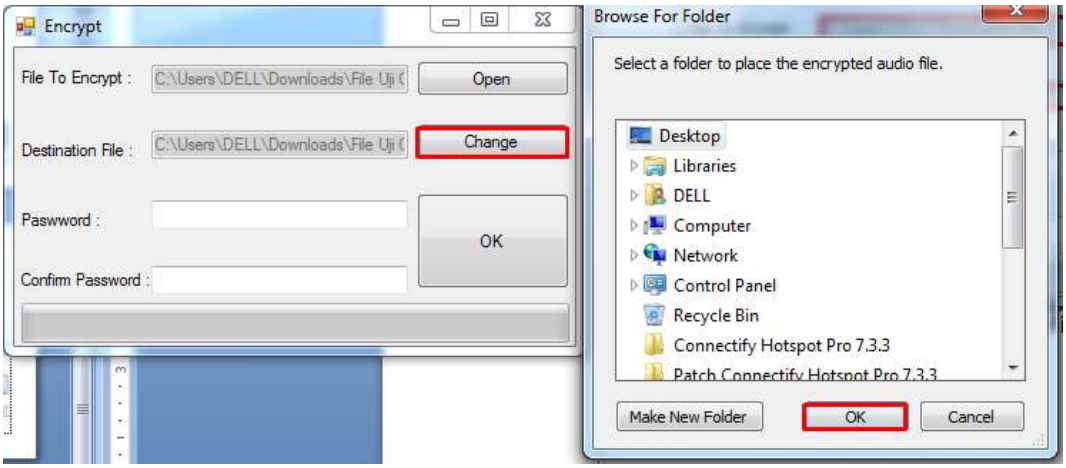


Gambar 4. Hasil Setelah File Audio Di Open

Setelah pengguna menyelesaikan pross pemilihan data dan menekan tombol “*Open*”, pengguna akan dikembalikan pada tampilan halaman encrypt. Setelah data yang dipilih siap dibuka, selanjutnya pengguna juga dapat menyesuaikan tempat penyimpanan data hasil enkripsi dengan menentukan directory tempat penyimpanan data atau *destination file* dengan menekan tombol change seperti yang dapat dilihat pada gambar dapat dilihat bahwa pengguna akan dipindahkan kedalam halaman *change file destination* setelah tombol change ditekan dan pengguna bebas untuk menentukan directory dan folder mana yang akan dijadikan tempat penyimpanan hasil enkripsi data sesuai dengan gambar.

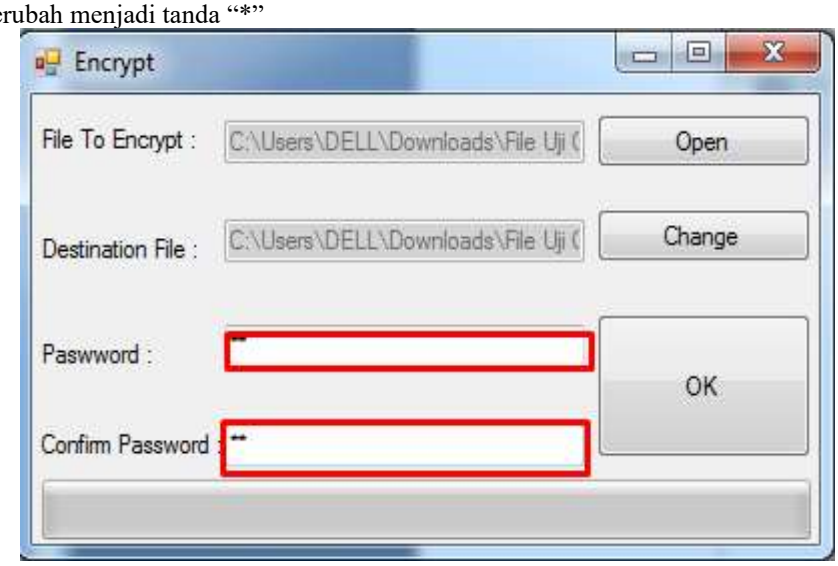
Submitted: **01/01/2024**; Accepted: **15/02/2024**; Published: **01/02/2024**

Jurnal Informatika Logika
Volume 1, Nomor 1, Februari 2024, Page 8-17
ISSN 0000-0000 (media online)
Available Online at https://idpress.ac.id/index.php/jil/index
DOI : --



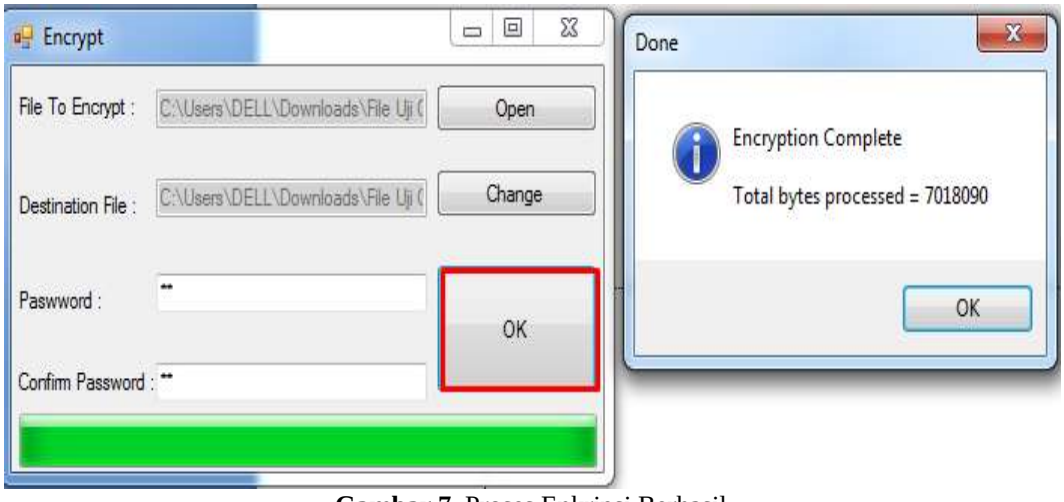
Gambar 5. Menetukan Lokasi File Hasil Enkrip

Proses selanjutnya adalah memasukkan password yang akan digunakan untuk proses enkripsi. Pada gambar dapat dilihat bahwa dalam proses penginputan password sistem yang dirancang oleh penulis mengharuskan penulis untuk memasukkan pasword sebanyak dua kali. Password yang pertama dan confirmasi password pada text box yang kedua. Hal ini dilakukan untuk memastikan user mengingat dan memverifikasi ulang password yang mereka input. Penambahan confirm password dianggap cukup penting oleh pembuat sistem dikarenakan password yang diinput oleh pengguna tidak akan tampak pada text box karena password secara otomatis akan berubah menjadi tanda "*"



Gambar 6. Memasukkan Password Enkripsi

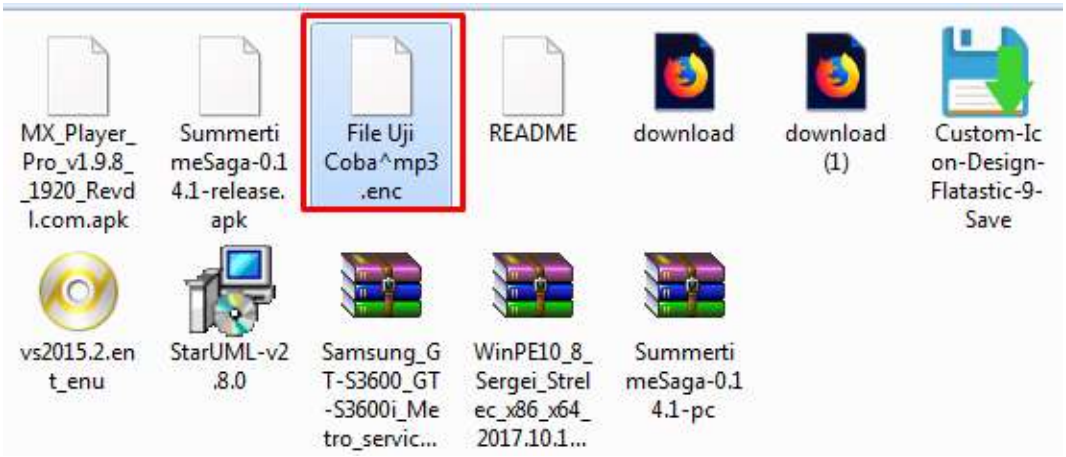
Setelah penginputan dan konfirmasi password selanjutnya pengguna dapat melanjutkan proses untuk mengenkripsi data dengan menekan tombol "OK" yang ada pada halaman encrypt seperti yang tampak pada gambar.



Gambar 7. Proses Enkripsi Berhasil

Submitted: **01/01/2024**; Accepted: **15/02/2024**; Published: **01/02/2024**

Jurnal Informatika Logika
Volume 1, Nomor 1, Februari 2024, Page 8-17
ISSN 0000-0000 (media online)
Available Online at https://idpress.ac.id/index.php/jil/index
DOI : --

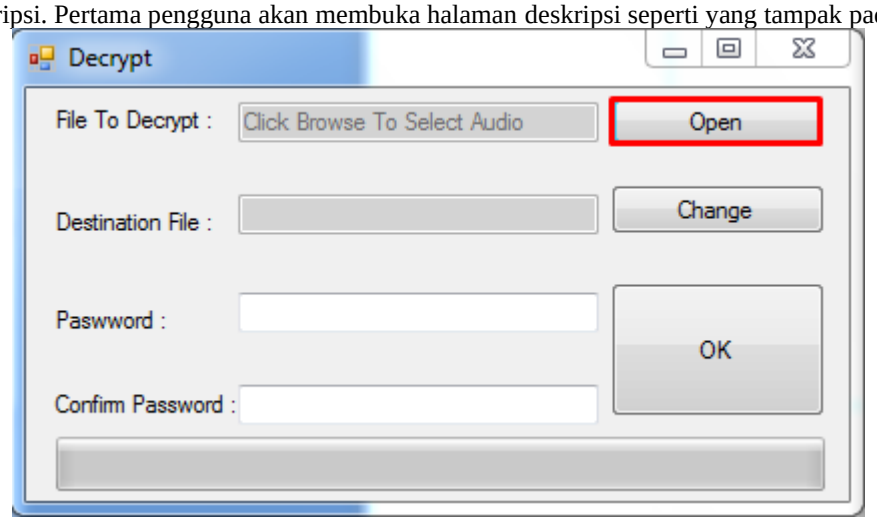


Gambar 8. File Hasil Enkripsi

Setelah proses enkripsi selesai file hasil enkripsi akan disimpan sesuai dengan tempat penyimpanan data hasil enkripsi yang sebelumnya sudah ditentukan oleh pengguna. Perlu diberitahukan bahwa data hasilenkripsi akan menjadi data yang tidak terbaca dikarenakan dua hal. Data hasil enkripsi akan tidak terbaca dikarenakan file sudah melewati hasil enkripsi sehingga susunan bit data menjadi berbeda sama sekali. Dan ekstensi data hasil enkripsi tidak lagi menjadi .MP3 namun menjadi .enc. Ekstensi data ini tidak dapat dibuka dikarenakan ekstensi ini hanyalah simbolik untuk data hasil enkripsi (enc singkatan dari encrypt)

Gambar 9. Tampilan Awal Deskripsi

Selanjutnya setelah proses enkripis selesai dan sistem telah menghasilkan data enkrip, pengguna dapat mengembalikan kondisi data agar dapat kembali dibaca. Proses deskripsi secara algoritma merupakan kebalikan dari proses enkripsi. Pertama pengguna akan membuka halaman deskripsi seperti yang tampak pada gambar

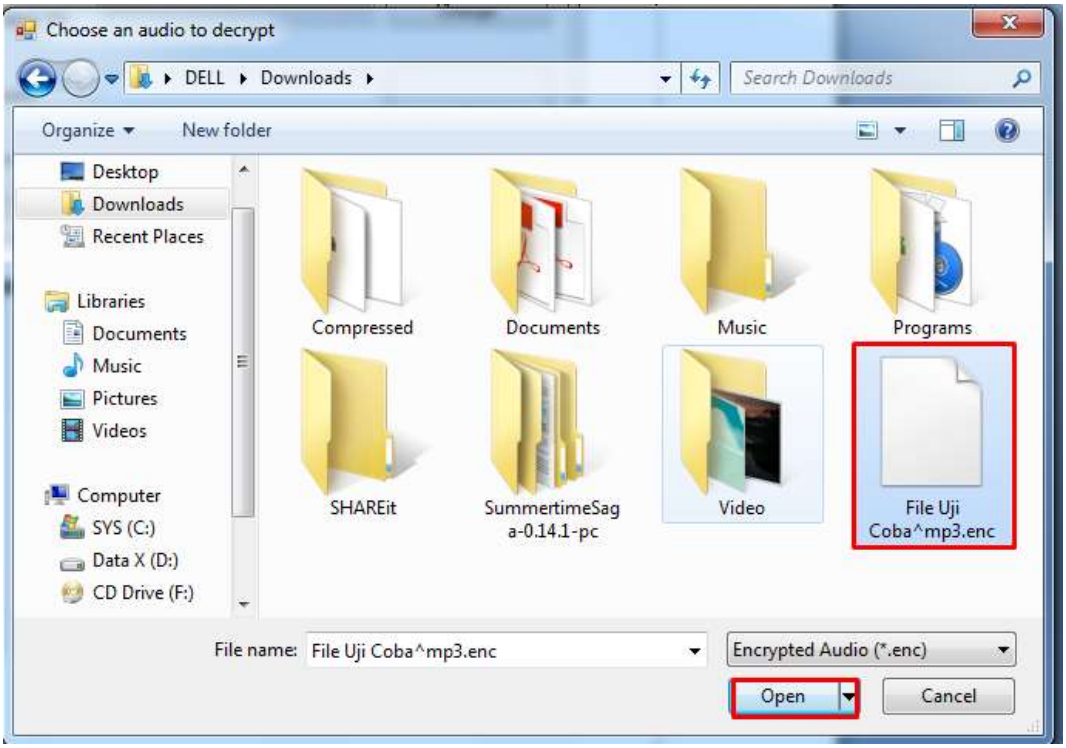


Gambar 10. Memilih audio yang akan di dekrip

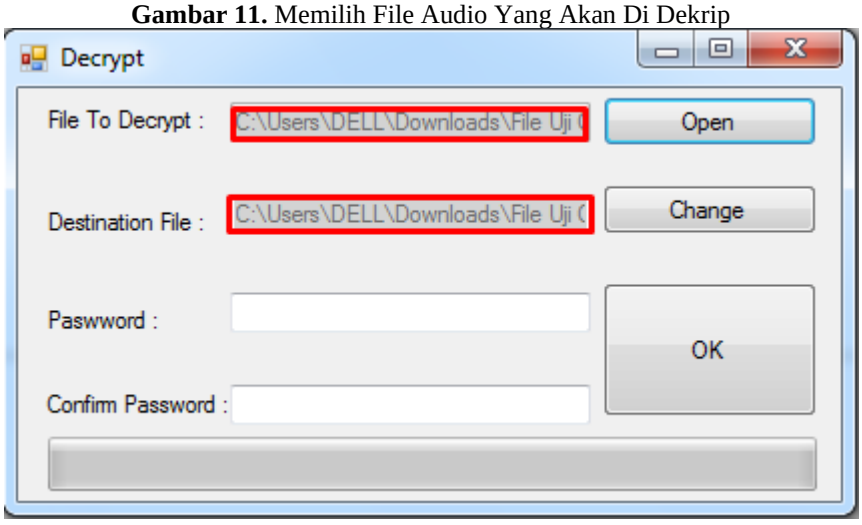
Kemudian pengguna akan membuka data hasil enkripsi yang sebelumnya sudah disimpan pada directori tertentu dengan menekan tombol “open” seperti yang tampak pada gambar dibawah.

Submitted: **01/01/2024**; Accepted: **15/02/2024**; Published: **01/02/2024**

Jurnal Informatika Logika
Volume 1, Nomor 1, Februari 2024, Page 8-17
ISSN 0000-0000 (media online)
Available Online at https://idpress.ac.id/index.php/jil/index
DOI : --

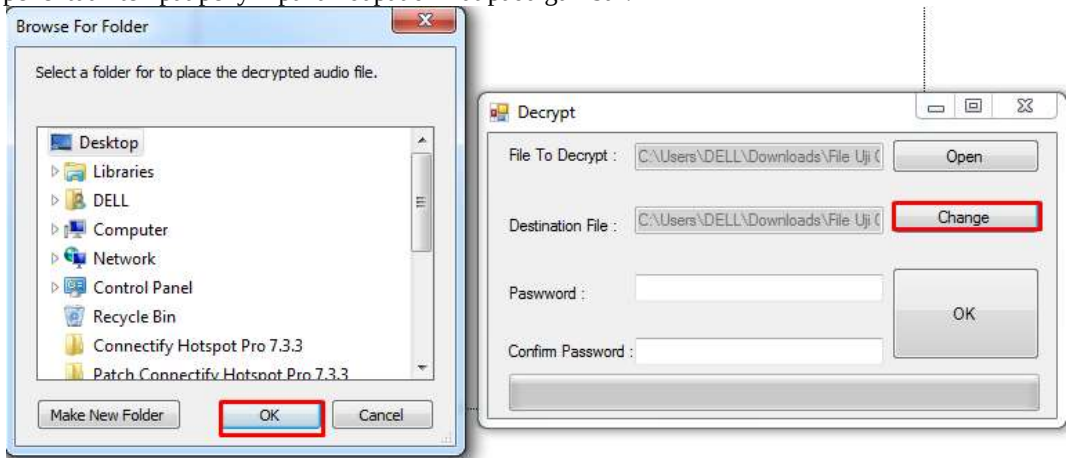


Gambar 11. Memilih File Audio Yang Akan Di Dekrip



Gambar 12. Setelah File Audio Di Open

Kemudian setelah membuka dan memasukkan data hasil enkripsi pada halaman dekrip seperti yang tampak pada gambar, pengguna akan menentukan kembali tempat penyimpanan data hasil deskripsi dengan proses yang sama dengan menentukan tempat penyimpaan data seperti pada halaman enkripsi sebelumnya, proses penentuan tempat penyimpanan dapat dilihat pada gambar.

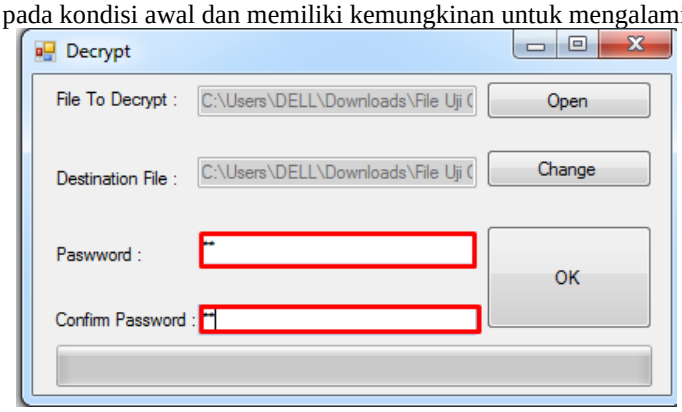


Gambar 13. Menentukan Lokasi Penyimpanan File

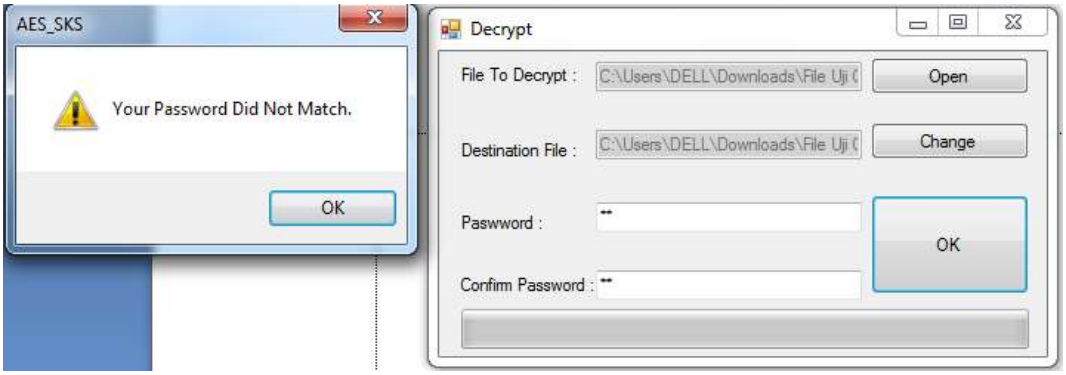
Submitted: **01/01/2024**; Accepted: **15/02/2024**; Published: **01/02/2024**

Jurnal Informatika Logika
Volume 1, Nomor 1, Februari 2024, Page 8-17
ISSN 0000-0000 (media online)
Available Online at https://idpress.ac.id/index.php/jil/index
DOI : --

Setelah pengguna selesai menentukan tempat penyimpanan data hasil deskripsi, selanjutnya pengguna akan kembali memasukkan password yang sbelumnya digunakan untuk mengekripsi data seperti yang tampak pada gambar. Perlu ditekankan kembali bahwasanya password yang digunakan untuk deskripsi haruslah sama dengan password yang digunakan pada saat proses enkripsi. Apabila password yang digunakan tidak sama, maka data tidak akan kembali pada kondisi awal dan memiliki kemungkinan untuk mengalami kerusakan data.

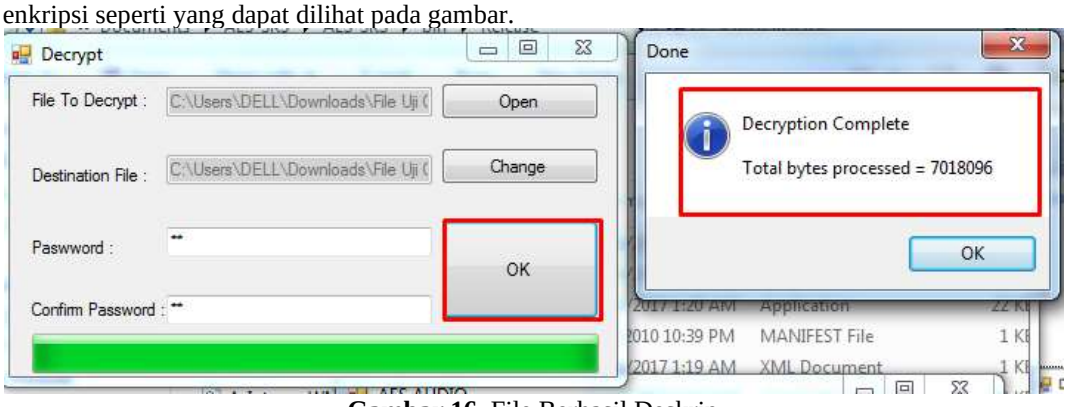


Gambar 14. User Memasukkan Password



Gambar 15. Gagal Mendekrip Jika Password Salah

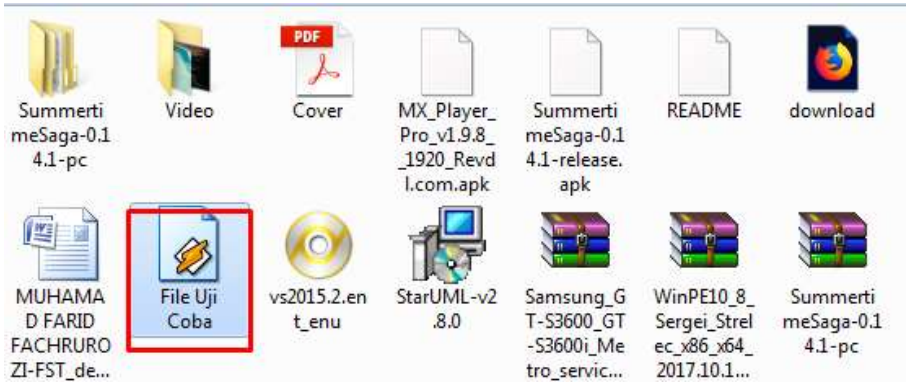
Penginputan password yang tidak sama dengan proses enkripsi akan menyebabkan sistem gagal melaksanakan proses deskripsi seperti yang dapat dilihat pada gambar diatas. Setelah password yang diinputkan oleh pengguna sesuai dengan password yang digunakan pada saat enkripsi selanjutnya pengguna akan menekan tombol “OK: dan sistem akan men-deskripsi data dan mengembalikan kondisi data pada saat sebelum melewati proses enkripsi seperti yang dapat dilihat pada gambar.



Gambar 16. File Berhasil Deskrip

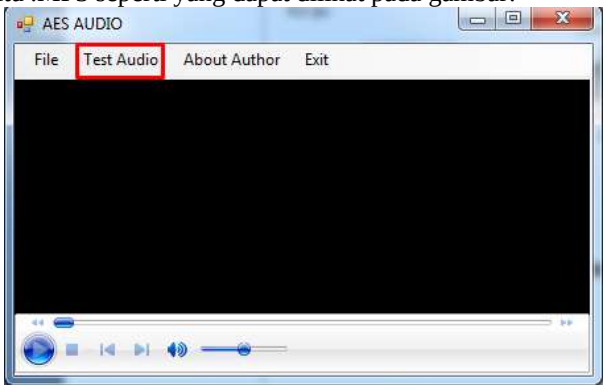
Submitted: **01/01/2024**; Accepted: **15/02/2024**; Published: **01/02/2024**

Jurnal Informatika Logika
Volume 1, Nomor 1, Februari 2024, Page 8-17
ISSN 0000-0000 (media online)
Available Online at https://idpress.ac.id/index.php/jil/index
DOI : --



Gambar 17. File Hasil Dekrip Kembali Berekstensi .Mp3

Setelah data berhasil dideskripsi data akan kembali memiliki ekstensi data yang sama seperti sebelum melewati proses enkripsi yaitu .MP3 seperti yang dapat dilihat pada gambar.



Gambar 18. Membuka Data Hasil Dekrip Untuk Di Uji

Gambar 19. Membuka Data Dengan Menekan Tombol Open

Setelah proses deskripsi selesai dan juga data hasil deskripsi telah disimpan pengguna da[at melakukan tes dengan membuka file hasil deskripsi seperti yang tampak pada gambar dan menjalankan file terebut dengan audio player yang terdapat pada sistem seperti yang tampak pada gambar.

Gambar 20. File Berhasil DI Baca Dan Bersuara

Dengan mampunya file dibuka kembali dan dapat menghasilkan audio yang sama dengan file sebelum di enkripsi maka sistem pun dapat dinyatakan mampu melakukan proses enkripsi dan deskripsi dengan baik.

Submitted: **01/01/2024**; Accepted: **15/02/2024**; Published: **01/02/2024**

Jurnal Informatika Logika
Volume 1, Nomor 1, Februari 2024, Page 8-17
ISSN 0000-0000 (media online)
Available Online at https://idpress.ac.id/index.php/jil/index
DOI : --

4. KESIMPULAN

AES: Rijndael merupakan algoritma yang cukup sulit untuk dipecahkan saat ini, karena belum ada serangan atau pemecahan yang benar-benar mampu secara analisis matematis dengan efektif dan efisien dengan alasan pola yang dibentuk cukup acak. Sehingga saat ini perkembangan digital sudah sangat berkembang karena itu keamanan data bukan hanya untuk pengolahan plaintext dan image namun juga untuk file audio. Dan kriptografi rijndael berhasil diaplikasikan untuk mengamankan data dan dapat berjalan dengan baik saat di impelentasikan untuk mengamankan data pada file audio.

REFERENCES

[1] S. M. N. Sipayung *et al.*, "Implementasi Dan Pengembangan E-Bisnis Era Revolusi Industri 4.0," in *Prosiding Seminar Nasional Sains dan Teknologi Terapan*, 2022.
[2] E. Ndruru and T. S. Alasi, "Algoritma Tripple Des Dalam Pengamanan File Dengan Usb Flashdisk," *J. Inf. Komput. Log.*, vol. 2, no. 4, 2022.
[3] T. S. Alasi, "Algoritma Hill Cipher Untuk Kebenaran Informasi pada Gambar dalam Media Sosial," *J. Inf. Komput. Log.*, vol. 2, no. 2, 2021.
[4] H. Simangunsong, M. A. Raharja, A. SE, and M. Cs, "Penerapan Algoritma Advanced Encryption Standard (AES-128) Dengan Mode ECB Dalam Pengamanan File".
[5] F. Nugraha and T. Arifin, "Voice Encryption and Decryption Using AES 128b Method With Secret Key," *SISTEMASI*, vol. 11, no. 1, pp. 97–107, 2022.
[6] Z. Arif and A. Nurokhman, "Analisis Perbandingan Algoritma Kriptografi Simetris Dan Asimetris Dalam Meningkatkan Keamanan Sistem Informasi," *J. Teknol. Sist. Inf.*, vol. 4, no. 2, pp. 394–405, 2023.
[7] T. S. Alasi and J. Sembiring, "Algoritma Blowfish Untuk Pengaman Pesan Teks," *J. Armada Inform.*, vol. 3, no. 1, pp. 215–223, 2019.
[8] M. Minarni, A. Ikram, I. Warman, and G. Y. Swara, "Implementasi Algoritma Vigenere Cipher Dan End Of File Pada Steganografi Video," *J. Minfo Polgan*, vol. 12, no. 2, pp. 432–441, 2023.
[9] A. D. E. IBRAHIM, "MENGGABUNGKAN TEKNIK STEGANOGRAFI DISCRETE WAVELET TRANSFORM DUA DIMENSI (2-D) DAN ALGORITMA KRIPTOGRAFI RSA PADA PERANCANGAN DAN ANALISIS KEAMANAN PESAN," UNIVERSITAS ISLAM NEGERI SULTAN SYARIF KASIM RIAU, 2022.
[10] M. Hasan, M. N. Dasaprawira, and others, "PENGUJIAN APLIKASI TABUNGAN SANTRI BERBASIS WEB DENGAN MENGGUNAKAN ALGORITMA KRIPTOGRAFI ADVANCE ENCRYPTION STANDARD (AES) 256.," *JOINICS (Journal Informatics Comput. Sci.*, vol. 1, no. 1, pp. 11–18, 2023.
[11] S. I. H. Abimanyu, D. Kusumaningsih, P. Purwanto, and W. Windarto, "IMPLEMENTASI ALGORITME ADVANCED ENCRYPTION STANDAR (AES-128) UNTUK MENGAMANKAN DOKUMEN PADA PT. JIA DREAMS COMMUNICATIONS," in *Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)*, 2023, pp. 88–96.
[12] L. B. Handoko and C. Umam, "Kombinasi Vigenere-Aes 256 dan Fungsi Hash Dalam Kriptografi Aplikasi Chatting," *Pros. Sains Nas. dan Teknol.*, vol. 12, no. 1, pp. 390–397, 2022.
[13] S. P. Ananda, S. Lukman, and others, "Analisa Metode Kriptografi Modern Advance Encryption Standard (AES) 128 Bit dalam Mengenkripsi dan Mendekripsi File Dokumen Digital: Array," *J. Ilm. KOMPUTASI*, vol. 21, no. 3, pp. 333–344, 2022.
[14] P. Fitriani and T. S. Alasi, "Pengamanan Pesan Dengan Teknik Steganografi Menggunakan Metode Least Significant Bit Pada Citra Digital," *J. Inf. Komput. Log.*, vol. 1, no. 2, 2019.
[15] T. S. Alasi and P. Fitriani, "Peningkatan Keamanan untuk Password menggunakan Algoritma Vigenere Cipher," *J. Mantik Penusa*, vol. 6, no. 1, pp. 1–10, 2022.

Submitted: **01/01/2024**; Accepted: **15/02/2024**; Published: **01/02/2024**