Jurnal Ilmu Komputer, Teknologi Dan Informasi
V Vol 1, No. 2, Juli 2023, Hal 76 - 83
ISSN: **2963-0169** (Online - Elektronik)
https://journal.grahamitra.id/index.php/jurikti

Implementasi Algoritma Advanced Encryption Standard Untuk Kemanan Dokumen

Wahyu Putra[1], Muhammad Rizza Fahlevi[2], Ahmad Tri Hidayat[3]

Progam Studi Informatika, Fakultas Sains & Teknologi, Universitas Teknologi Yogyakarta, Yogyakarta, Indonesia
Jl. Siliwangi, Jl Ring Road Utara, Jombor Lor, Sendangadi, Kec. Mlati, Kab. Sleman, DIY , Indonesia
Email: [1]wahyueputra7@gmail.com, [2]necentareymizard@gmail.com

Abstrak- Data yang disimpan dalam sebuah dokumen memiliki tingkat keamanan yang sangat rentan, terlebih lagi jika dokumen tersebut tidak memiliki sistem keamanan untuk melindungi kerahasiaan dan keaslian dokumen tersebut. Salah satu cara untuk menjaga keamanan dan kerahasiaan dokumen adalah dengan menggunakan kriptografi. Kriptografi dikenal sebagai ilmu yang mempelajari teknik penyandian menggunakan matematika yang berkaitan dengan aspek keamanan informasi. Keamanan informasi yang dimaksud dapat berupa keabsahan data, kerahasiaan data, kredibilitas data, integritas data, dan autentikasi data. Dalam kriptografi terdapat algoritma-algoritma yang dapat digunakan untuk meningkatkan keamanan dokumen, salah satunya adalah algoritma *Advanced Encryption Standard* (AES). *Advanced Encryption Standard* adalah salah satu jenis kriptografi simetris dimana kunci yang digunakan untuk proses enkripsi dan dekripsi sama. Aplikasi enkripsi dekripsi yang dibuat berbasis desktop dengan harapan aplikasi ini dapat menjadi alternatif dalam membantu meningkatkan keamanan dokumen. Pada aplikasi yang dibuat dokumen yang dapat dienkripsi adalah dokumen-dokumen dengan format yang paling sering dijumpai yaitu dokumen dengan format .docx, dan .pdf.

Kata Kunci: Keamanan data, Kriptografi, AES, Desktop, Dokumen

Abstract- *Data stored in a document has a very vulnerable security level, especially if the document does not have a security system to protect the confidentiality and authenticity of the document. One way to maintain the security and confidentiality of documents is to use cryptography. Cryptography is known as a science that studies encryption techniques using mathematics related to aspects of information security. Information security in question can be in the form of data validity, data confidentiality, data credibility, data integrity, and data authentication. In cryptography there are algorithms that can be used to improve document security, one of which is the Advanced Encryption Standard (AES) algorithm. Advanced Encryption Standard is a type of symmetric cryptography in which the key used for the encryption and decryption process is the same. A desktop-based encryption and decryption application with the hope that this application can be an alternative to help improve document security. In the application that is made, documents that can be encrypted are documents with the most frequently encountered formats, namely documents in the .docx and .pdf formats..*

Keywords*: Data Security, Cryptography, AES, Desktops, Documents*

1. PENDAHULUAN

Keamanan dan kerahasiaan dokumen menjadi sangat rentan terhadap penyadapan dan pencurian sehingga mengakibatkan kerugian terhadap pemilik dokumen. Salah satu contoh dari kasus kehilangan data yang pernah terjadi seperti bocornya data-data sensitif suatu instansi (contoh kasus, "Serangan Cloudbleed ke Cloudflare yang mengakibatkan bocornya data-data klien perusahaan tersebut pada awal tahun 2017"). Ada pula kasus kebocoran data yang terjadi di indonesia dimana instansi yang menjadi korban dari kebocoran data tersebut dialami oleh instansi pemerintah(contoh kasus, "Kebocoran Data Bank Indonesia diamana sebanyak lebih dari 52 ribu dokumen yang berasal dari 200 komputer pada tahun 2022"). Menurut Velumadhaca Rao dan Selvamani (2015) kehilangan atau kebocoran data dapat berdampak serius pada bisnis, merek, dan kepercayaan organisasi. Dari hasil survey yang dilakukan didapatkan bahwa pencegahan kebocoran data dianggap sebagai faktor terpenting dengan tantangan 88% Kritis dan Sangat penting. Demikian pula pemisahan dan perlindungan data berdampak 92% pada tantangan keamanan [1], [2], [3].

Metode dalam meningkatkan keamanan data terus dikembangkan seiring dengan meningkatnya ancaman terhadap kebocoran data itu sendiri. Jika melihat dari sejarahnya, sebelum adanya perangkat komputer informasi disimpan dengan cara yang tradsional yaitu informasi tersebut akan dicetak pada lembaran kertas sehingga lembaran kertas tersebut akan menjadi sebuah dokumen yang memuat informasi penting tergantung dari tingkat kualitas data yang tertulis didalamnya. Pada awal sejarah saat dimana awal mula baca-tulis dan pesan telah ada, penyampaian pesan dilakukan dengan cara menuliskan pesan rahasia untuk menjaga kerahasiaan pesan tersebut. Akan tetapi cara tersebut masih belum efektif karna pesan masih dapat diketaui oleh orang lain apabila pesan tersebut bocor, karna pada saat itu telah banyak orang yang telah mengetahui baca-tulis. Untuk mencegah hal tersebut maka mereka mengembangkan metode-metode keamanan untuk melindungi kerahasiaan pesan, salah satunya adalah enkripsi. Metode enkripsi dilakukan dengan cara mengacak-acak isi pesan menjadi barisan-barisan yang tidak dapat dibaca sebelum pesan tersebut dikirim ke penerima pesan. Agar penerima pesan dapat membaca pesan tersebut, sebelumnya telah ditentukan terlebih dahulu cara agar pesan yang diacak-acak tersebut dapat diubah kembali kedalam bentuk pesan asli sehingga pesan tidak akan dapat dibaca oleh orang lain meskipun pesan tersebut bocor.

Perkembangan teknologi informasi membuat kegiatan penyampaian pesan dapat dilakukan dengan melalui jaringan internet. Meskipun mengirim pesan melalui jaringan internet terbilang cukup tersembunyi karna pengiriman pesan dapat langung oleh pengirim kepada penerima bukan berarti pesan tersbut tidak dapat diketahui oleh pihak lain. Pesan dapat disadap oleh pihak lain apabila pesan tersebut tidak dilindungi oleh sistem keamanan yang baik. Maka dari

itu untuk meningkatkan kemanan dan kerahasiaan pesan dapat diterapkan metode enkripsi pada pesan sehingga apabila pesan tersebut disadap atau dicuri, pesan tidak dapat dibaca dan diketahui oleh pencuri karna pesan telah diacak. Metode inipun dapat diterapkan pada sebuah dokumen elektronik dimana data-data didalamnya akan diacak menggunakan algoritma enkripsi menjadikan dokumen tersebut seperti dokumen dengan isi yang tidak jelas dan karuan.

Pada penelitian sebelumnya yang dilakukan oleh Berita E.W, Sidiq P. (2020), dibuat sebuah sistem dengan mengimplementasikan *algoritma advanced enrcryption standard* pada enkripsi dan dekripsi dokumen rahasia ditintelkam polda DIY. Pada penelitian ini *algoritma advanced encryption* (AES) standard diimplementasikan kedalab bentuk bahasa pemrogramam PHP berbasis web. Dalam sistem yang dibuat pada proses enkripsi dan dekrip memiliki waktu yang berbeda-beda tergantung dari ukuran dari dokumen. Format dokumen yang dapat dienkripsipun beragam, mulai dari .doc, .docx, .xls, .xlsx, .pdf dan .txt [4].

2. METODOLOGI PENELITIAN

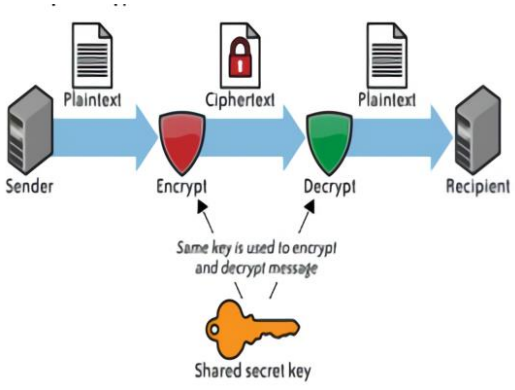
2.1 Tahapan Pelitian

Tahapan penelitian yang dilakukan peneliti dalam pembuatan aplikasi melalui beberapa tahap, diantara lain adalah [5]:

a. Observasi
   Observasi dilakukan dengan cara pengamatan secara langsung ke lapangan untuk merumuskan permasalahan sehingga dilakukan penelitian guna menyelesaikan permasalahan tersebut. Pada tahap observasi peneliti juga dapat melakukan pengumpulan data yang diperlukan dalam penelitian seperti dokumen-dokumen yang akan dilakukan proses enkripsi.
b. Studi Pustaka
   Pada tahap ini peneliti melakukan pengumpulan data berupa refrensi yang relavan dengan penelitian yang sedang dilakukan saat ini. Tahapan ini diperlukan guna menjadi acuan dan pembanding oleh peneliti serta mendapatkan data yang tidak didapatkan dalam proses observasi. Sumber dari studi pustaka dapat berupa jurnal, web resmi, buku dan sumber lain dengan kasus yang sama.
c. Pengumpulan data
   Selain data yang diperoleh dari tahap observasi dan studi pustaka pengumpulan data juga dilakukan dengan cara wawancara terhadap pihak terkait.
d. Perancangan Sistem
   Pada perancangan sistem peneliti akan membuat model dari alur sistem yang akan dibuat secara *logic* yang digambarkan dalam bentuk flowchart, usecase, activity diagram, dan rancangan antarmuka.
e. Implementasi
   Algoritma AES akan diimplementasi kan dengan menggunakan bahasa pemrogaram C#.
f. Pengujian
   Pada tahap ini peneliti akan melakukan pengujian terhadap sistem yang dibuat dan membandingan hasil dari pengujian aplikasi dalam berbagai kondisi parameter.

2.2 Enkripsi

Menurut Gunawan et al (2021) *Cryptography* adalah ilmu yang membahas tentang ilmu penyandian, *encryption* adalah metode dalam *cryptography* dimana data yang bermacam-macam panjangnya/ukurannya diubah/diacak menjadi data yang panjangnya tetap. Pada buku berjudul *Contemporary Cryptography*, Oppliger (2005) Jika transformasi dari bentuk asli ke bentuk acak dapat dikembalikan, kriptografi juga dapat diartikan sebagai proses mengubah kembali data yang terenkripsi menjadi bentuk yang dapat dipahami. Artinya kriptografi dapat diartikan sebagai proses untuk melindungi melindungi data dalam arti yang luas. Alur proses untuk enkripsi dan dekripsi dapat dilihat pada gambar berikut [6], [7]:



Gambar 1. Alur proses enkripsi[6]

Dapat diliha pada gambar 1 diatas dimana menggambarkan sebuah proses dalam pengenkripsian sebuah pesan. Pada gambar tersebut menggambarkan proses enkripsi dengan menggunakan algoritma simetris dimana kunci yang digunakan untuk pengenkripsian dan dekripsi pesan sama. Pesan akan diubah menggunakan algoritma yang telah ditentukan berserta kunci agar pesan dapat diengkripsi. Jika penerima pesan ingin membaca pesan yang dienkripsi tersebut, maka penerima pesan harus melakukan proses dekripsi terlebih dahulu pesan tersebut menggunakan kunci yang sama dengan kunci saat melakukan proses enkripsi.

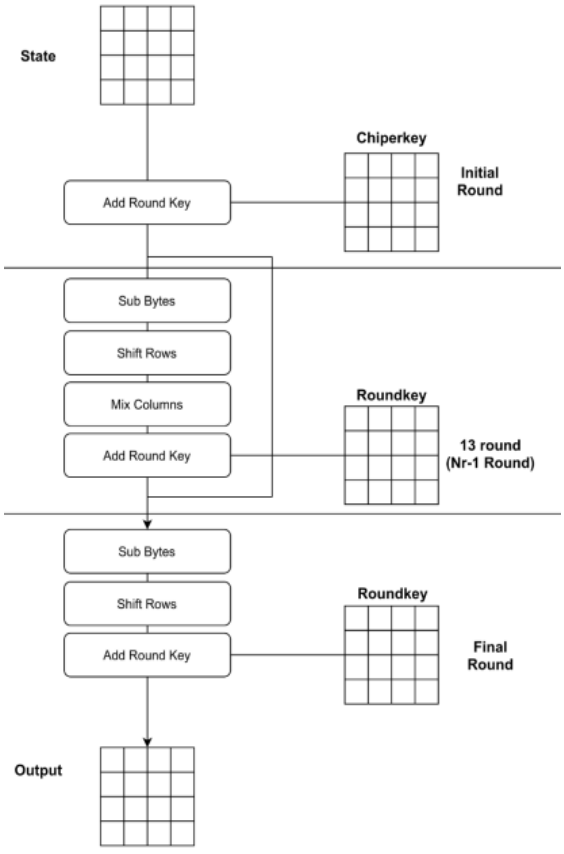
2.3 *Advanced Encryption Standard*

Pada tahun 1997, *National Institute of Standard and Technology* (NIST) di Amerika Serikat mengeluarkan algoritma *Advanced Encryption Standard* (AES) untuk menggantikan *Data Encryption Standard* (DES). Algoritma AES di desain menggunakan block chiper minimal dari blok 128 bit input dan menggunakan 3 panjang ukuran kunci (*3-key-sizes*) yang berbeda, yaitu kunci 128 bit, 192 bit, dan 256 bit. Algoritma AES setiap blok dienkripsi dalam sejumlah putaran tertentu, sebagaimana halnya pada algoritma DES. Berikut pada tabel dibawah menunjukkan banyaknya putaran kunci pada algoritma AES [8] :

Tabel 1. Putaran Kunci AES

AES (Bits)	Panjang Kunci (Nk Words)	Ukuran Blok (Nb Words)	Jumlah Putaran (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES256	8	4	14

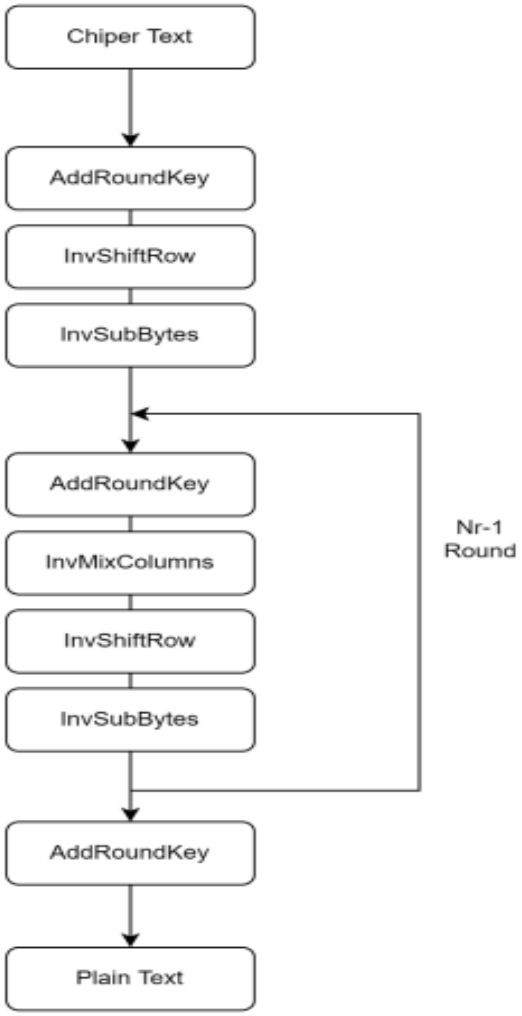
Dalam proses enkripsi dengan menggunakan algoritma AES, terdapat 4 jenis transformasi *bytes*, yaitu *SubBytes*, *ShiftRows*, *Mixcolumns*, dan *AddRoundKey*. Gambaran untuk keempat proses tersebut dapat dilihat pada gambar berikut:



Gambar 2. Proses enkripsi AES [9].

Pada gambar dapat dilihat bahwa, pada awal proses enkripsi, *input* yang telah disalinkan ke dalam *state* akan mengalami transformasi *byte AddRoundKey*. Setelah itu, state akan mengalami transformasi *SubBytes*, *ShiftRows*, *Mixcolumns*, dan *AddRoundKey* secara berulang-ulang sebanyak Nr(jumlah putaran). Proses ini dalam algoritma AES

disebut sebagai *round function*. *Round* yang terakhir sedikit berbeda dengan *round-round* sebelumnya dimana pada *round* terakhir, *state* tidak mengalami transformasi *Mixcolumns* (I. Hajar, 2022) [9].



Gambar 3. Proses dekripsi AES [9].

Untuk proses dekripsi, transformasi *cipher* dapat dibalikkan dan diimplementasikan dalam arah yang berlawanan untuk menghasilkan *inverse cipher* yang mudah dipahami untuk algoritma AES. Transformasi *byte* yang digunakan pada *invers cipher* adalah *InvShifRows*, *InvSubBytes*, *InvMixcolumns*, dan *AddRoundKey* [9].

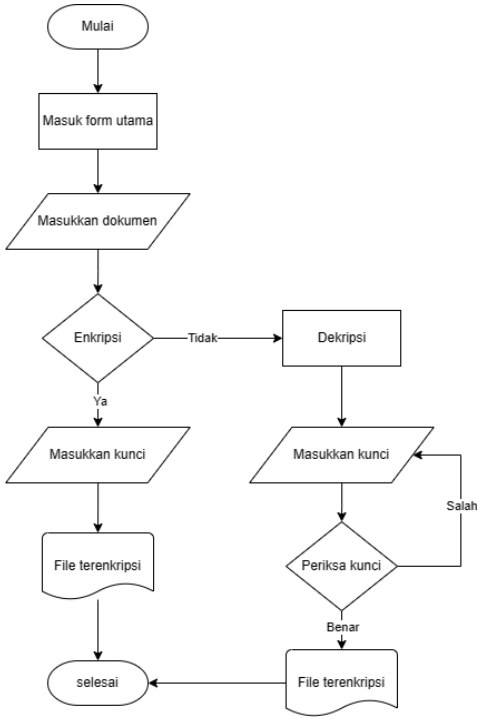
3. HASIL DAN PEMBAHASAN

Iplementasi algoritma untuk keamanan dokumen diterapkan kedalam bahasa pemrograman C# berbasis desktop. Bahasa pemrograman C# merupakan bagian kerangka dari .Net dan dimaksudkan untuk menjadi bahasa pemrograman dengan tujuan umum sederhana yang dapat digunakan untuk mengembangkan berbagai jenis aplikasi, termasuk aplikasi konsol, windows, web, dan seluler (B. Raharjo, 2020). Untuk menguji sistem yang dibuat, sistem akan diuji dengan melakukan proses enkripsi dan dekripsi dokumen dengan beberapa jenis format seperti .docx, .pdf, dan .txt [10].

3.1 Alur sistem

Gambaran untuk alur sistem yang dibuat dapat dilihat pada gambar 4. Pada gambar diatas dapat dilihat dimana proses untuk melakukan enkripsi atau dekripsi pada sistem yang dibuat. Saat membuka aplikasi pengguna akan masuk ke dalam form utama aplikasi dimana proses enkripsi dan dekripsi dapat dilakukan. Sistem akan meminta pengguna untuk memasukkan dokumen yang dimana dokumen dapat dipilih dari direktori perangkat yang digunakan. Setelah memasukkan dokumen akan ada pilihan untuk enkripsi atau dekripsi dokumen tersebut. Untuk proses enkripsi pengguna perlu menentukan *private key* agar dokumen yang dienkripsi nantinya dapat di dekripsi kembali ke bentuk semula.Untuk proses dekripsi pengguna perlu memasukkan dokumen yang telah terenkripsi dan *private key* yang digunakan saat mengenkripsi dokumen. Jika *private key* yang dimasukkan salah maka sistem akan menolak proses dekripsi dan meminta pengguna untuk memasukkan ulang *private key* yang benar.

Jurnal Ilmu Komputer, Teknologi Dan Informasi
V Vol 1, No. 2, Juli 2023, Hal 76 - 83
ISSN: **2963-0169** (Online - Elektronik)
https://journal.grahamitra.id/index.php/jurikti



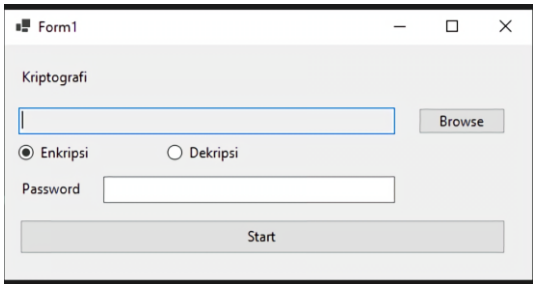
Gambar 4. Alur sistem

3.2 Implementasi

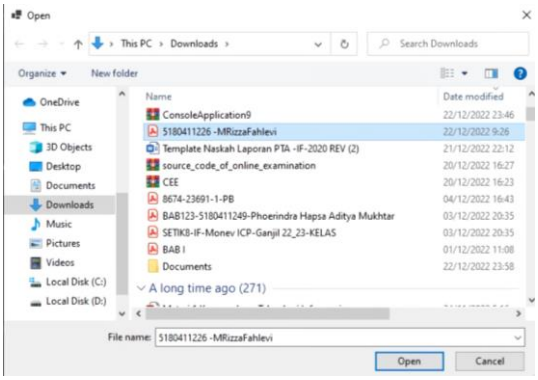
Pada bagian ini akan manmpilkan hasil dari implementasi algoritma AES menjadi sebuah aplikasi perangkat lunak untuk mengenkripsi dokumen. Dengan adanya implementasi, akan diketahui apakah penerapan algoritma AES dapat digunakan untuk meningkatkan keamanan dokumen.

3.2.1 Tampilan Utama Aplikasi

Tampilan utama pada aplikasi dapat dilihat pada gambar 5. Seperti yang digambarkan pada alur sistem pada gambar 4, tampilan utama pada aplikasi ini akan menampilkan sebuah form. Pada form ini pengguna akan diminta untuk memasukkan dokumen dimana dokumen dapat diambil dari direktori perangkat seperti yang ditampilkan pada gambar 6.



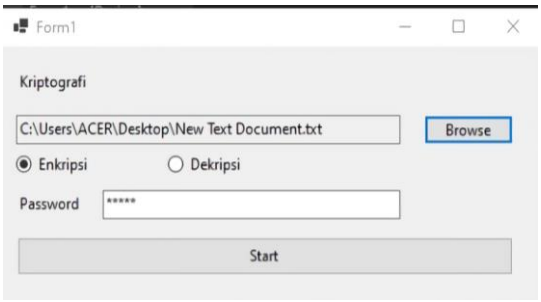
Gambar 5. Halaman utama



Gambar 6. Proses pengambilan dokumen

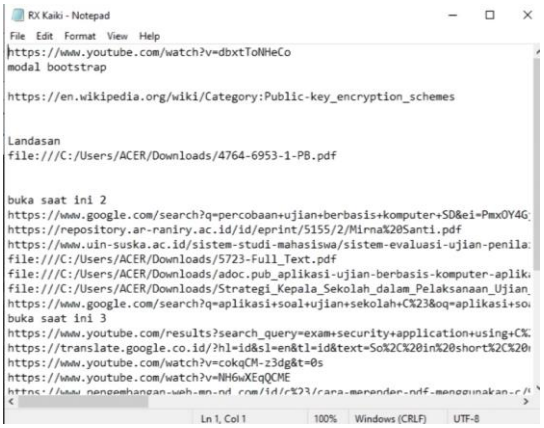
3.2.2 Proses

Pada bagian ini menampilkan pengujian terhadap aplikasi untuk proses enkripsi dan dekripsi. Pada proses pengujian menggunakan beberapa format dokumen untuk dilakukan proses enkripsi guna mengetahui apakah dokumen terenkripsi atau tidak. Format dokumen yang akan dilakukan uji coba adalah format dokumen yang sering kali dijumpai seperti .docx, .pdf, dan .txt.



Gambar 7. Proses Enkripsi

Pada gambar 7 dapat dilihat proses dari enkripsi yang dilakukan. Form telah telah diisi sesuai dengan kebutuhan sistem untuk menjalankan perintah pengguna dimana proses yang dilakukan ada proses enkripsi. Setelah memilih proses pengguna juga memasukkan private key/password yang digunakan sebagai salah satu syarat agar proses enkripsi dapat dijalankan. Pada gambar 8 dapat dilihat kondisi dari file sebelum dienkripsi, file tersebut memuat beberapa informasi yang dibutuhkan oleh pengguna. Hasil dari proses enkripsi dapat dilihat pada gambar 9 dimana isi dari file tersebut telah diubah ke dari *plain text* yang dapat dibaca menjadi *chiper text* acak yang tidak dapat dibaca dan tidak memuat informasi apapun.

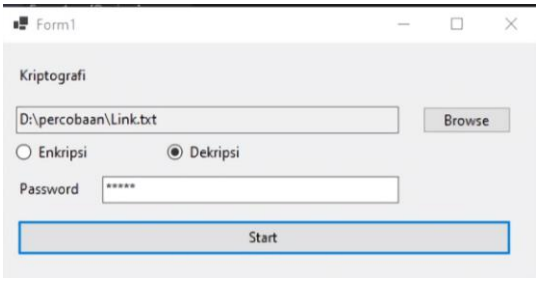


Gambar 8. Dokumen sebelum dienkripsi

Gambar 9. Hasil enkripsi

Untuk proses dalam melakukan proses dekripsi tidak jauh berbeda saat melakukan proses enkripsi. pada gambar 10 dapat dilihat form yang digunakan untuk proses dekrip sama dengan proses enkripsi, namun pada pilihan proses yang akan dilakukan pengguna akan memilih proses dekripsi untuk mendekripsi file yang terenkripsi. Pengguna juga akan memasukkan private key/password untuk mendekripsi file dimana private key/password sama dengan yang

digunakan saat melakukan enkripsi. Jika private key/password tidak sama maka sistem akan menolak proses dekripsi dan file tidak akan didekripsi. Hasil dari proses dekripsi dapat dilihat pada gambar 11. Setelah mengalami proses dekripsi, file yang berisi chiper text akan diubah kembali menjadi plaint text yang dapat dibaca.



Gambar 10. Proses dekripsi

Gambar 11. Hasil dekripsi

4. KESIMPULAN

Dari peneltian dan uji coba yang telah dilakukan pada implementasi algoritma AES untuk keamanan dokumen dapat disimpulkan bahwa penerapan metode enkripsi menggunakan algoritma AES dapat diterapkan untuk membantu meningkatkan keamanan dokumen. Dari hasil uji coba sistem, diketahui dokumen yang sebelumnya berisi *plain text* diubah menjadi bentuk *chiper text* dalam bentuk simbol-simbol yang sulit dipahami sehingga informasi yang terkandung di dalam dokumen tidak langsung diketahui oleh pihak lain meskipun dokumen dicuri atau dimiliki oleh pihak lain. Metode keamanan dengan enkripsi dapat digunakan oleh suatu instansi seperti perusahaan dan instansi resmi dalam membantu menjaga keamanan informasi terkait instansi tersebut. Penambahan format dokumen yang dapat di enkripsi dapat menjadi penyempurnaan sistem yang akan dibuat dimasa mendatang agar batasan sistem dalam proses enkripsi dan dekripsi dapat lebih luas dan beragam.

REFERENCES

[1] D. M. Agustinus, "Serangan Cloudbleed ke Cloudflare yang mengakibatkan bocornya data-data klien perusahaan tersebut pada awal tahun 2017," *Liputan6*, 2017. https://www.liputan6.com/tekno/read/2868280/bug-sebabkan-data-pengguna-situs-perusahaan-as-bocor (accessed Dec. 07, 2022).

[2] B. A. Fahmi, "Ahli IT : Data Bocor Bank Indonesia Berasal dari Lebih 200 Komputer," *katadata*, 2022. https://katadata.co.id/desysetyowati/digital/61ee713f52c6d/ahli-it-data-bocor-bank-indonesia-berasal-dari-lebih-200-komputer (accessed Dec. 12, 2022).

[3] R. Velumadhava Rao and K. Selvamani, "Data security challenges and its solutions in cloud computing," *Procedia Comput. Sci.*, vol. 48, no. C, pp. 204–209, 2015, doi: 10.1016/j.procs.2015.04.171.

[4] B. E. Widodo and A. S. Purnomo, "Implementasi Advanced Encryption Standard Pada Enkripsi Dan Dekripsi Dokumen Rahasia Ditintelkam Polda Diy," *J. Tek. Inform.*, vol. 1, no. 2, pp. 69–77, 2020, doi: 10.20884/1.jutif.2020.1.2.21.

[5] M. Dr. Umar Sidiq, M.Ag Dr. Moh. Miftachul Choiri, *Metode Penelitian Kualitatif di Bidang Pendidikan*, vol. 53, no. 9. 2019. [Online]. Available: http://repository.iainponorogo.ac.id/484/1/METODE PENELITIAN KUALITATIF DI BIDANG PENDIDIKAN.pdf

[6] I. Gunawan, S. Tinggi, and T. Ronggolawe, "KEAMANAN DATA :," no. January, 2021.

[7] G. J. Simmons, *Contemporary Cryptography.*, vol. 2. 1983. doi: 10.5860/choice.43-2161.

[8] O. C. Abikoye, A. D. Haruna, A. Abubakar, N. O. Akande, and E. O. Asani, "SS symmetry for Information Security," pp. 1–16, 2019.

[9] I. Hajar, "Pengamanan Arsip dengan Algoritma Enkripsi AES-256 untuk Web App E-Arsip Yayasan Universitas Islam Sumatera Utara," *Hello World J. Ilmu Komput.*, vol. 1, no. 2, pp. 76–89, 2022, doi: 10.56211/helloworld.v1i2.13.

[10] B. Raharjo, "Pemrograman Bahasa C#," 2020.