Implementation of Cryptography with the Caesar Cipher Method to Secure Data Files in Java NetBeans

Implementasi Kriptografi dengan Metode *Caesar Cipher* untuk Mengamankan Data *File* di *Java NetBeans*

Haryanzelina Bancin[1], Mira Aripin Panjaitan[2], Sabrina Putri[3], Adnan Buyung Nasution[4]
[1,2,3,4]Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sumatera Utara
E-mail: [1]anzelbancin50@gmail.com, *[2]mirapanjaitan1@gmail.com, [3]sabrputri@gmail.com, [4]adnanbuyungn3@gmail.com

Abstract – *The rapid development of information and telecommunications technology makes it easier for us to carry out activities in the form of confidential files or data, therefore data security is needed to secure confidential files. This research was conducted to implement Caesar cipher cryptography. Where Cryptography can only be carried out by certain people who understand its use so that Cryptography can be categorized as a safe place to store confidential data. This system uses the caesar cipher algorithm which is processed with the Java NetBeans program to produce ciphertext. Where files that can be encrypted are text document files with the .txt extension. txt data is a Domain Name Service (DNS) data type that contains text information sources for sources within the domain, by adding to the domain a file with the .txt extension can be used for various important purposes. The result of this research is a cryptographic implementation of the Caesar cipher method to secure data files in Javanetbeans. So it can be concluded that data security using the Caesar Cipher method is proven to work on Java Netbeans.*

Keywords *— cryptography, javanetbeans, txt*

Abstrak – Pesatnya perkembangan teknologi informasi dan telekomunikasi yang memudahkan kita untuk melaksanakan aktifitas data dalam bentuk *file* ataupun data yang bersifat rahasia. Sehingga teknik diperlukan pengamanan data untuk mengamankan *file* yang bersifat rahasia. Penelitian ini dilaksanakan untuk membuat implementasi kriptografi *Caesar Cipher*. Dimana Kriptografi hanya dapat dilakukan oleh orang-orang tertentu yang paham akan penggunaannya sehingga Kriptografi dapat dikategorikan sebagai tempat yang aman untuk menyimpan data yang bersifat rahasia. Sistem ini mengaplikasikan algoritma *Caesar Cipher* yang diproses dengan program *Java NetBeans* sehingga menghasilkan *ciphertext*. Dimana *file* yang bisa diproses enskripsi adalah *file* dokumen berbentuk teks berekstensi *.txt*. Data *txt* yaitu jenis data *Domain Name Service* (DNS) yang berisi sumber informasi teks untuk sumber yang berada dalam domain, dengan menambahkan ke dalam domain *file* yang berekstensi *.txt* dapat digunakan untuk berbagai keperluan penting. Hasil dari penelitian ini adalah sebuah implementasi kriptografi metode *Caesar Cipher* untuk mengamankan data file di *Java NetBeans*. Maka dapat disimpulkan bahwa Pengamanan data menggunakan Metode *Caesar Cipher* terbukti dapat dilakukan pada *Java Netbeans*.

Kata Kunci *— java netbeans, kriptografi, txt*

1. PENDAHULUAN

Perkembangan teknologi yang semakin meningkat membuat banyaknya pengguna yang memanfaatkannya. Tidak ada bedanya pada bidang teknologi komputer yang digunakan baik bagi

 doi: https://doi.org/10.32503/jtecs.v3i1.3210

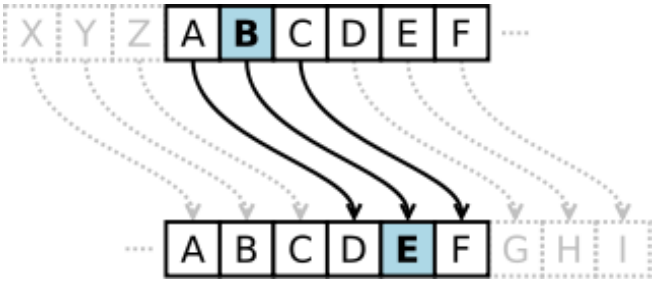
personal hingga organisasi seperti perusahan. Pekerjaan yang sebelumnya bisa dikerjakan secara manual beberapa telah dialihkan pengerjaannya menggunakan komputer. Pengguna komputer tersebut tentu memiliki kerahasiaan yang harus dijaga, maka munculah sebuah keamanan data yang ditujukan untuk mengamankan dokumen dari pengguna. Pengamanan komputer yang berhubungan dengan keamanan dokumen agar terhindar dari kebocoran data dari pihak yang berhubungan langsung dengan data.

Masalah keamanan menjadi salah satu aspek penting dari sebuah sistem informasi. Untuk masalah keamanan saat ini masih sering tidak dipedulikan, sedangkan hal tersebut sangat penting dalam pengamanan data atau informasi yang bersifat rahasia bertujuan untuk mengamankan informasi dari sebuah dokumen dan mengurangi dampak kerugian [1]. Menurut *G.J. Simons*, keamanan informasi merupakan bagaimana kita dapat mencegah penipuan (*cheating*) atau setidaknya mendeteksi penipuan dalam sistem data dimana data itu sendiri tidak memiliki arti fisik [2]. Salah satu langkah untuk mengamankan, menghindari kebocoran data adalah dengan kriptografi. Kriptografi menyajikan kata atau karakter dengan tampilan yang disamarkan. Salah satu cara kriptograpi yang dipakai untuk proses enkripsi ke dekripsi adalah dengan metode *Caesar Cipher*.

Istilah kriptografi itu sendiri berasal dari bahasa Yunani, diambil dari kata *Crypto* yang berarti *secret* atau rahasia, dan *Graphein* yang memiliki arti *writing* atau tulisan. Jadi pengertian dari kriptografi adalah *secret writing* atau tulisan rahasia [3]. Kriptografi merupakan suatu ilmu dan seni yang digunakan untuk menjaga kerahasiaan dari sebuah pesan dengan cara kerja membuat kode kedalam bentuk yang tidak dapat dimengerti lagi. Terdapat dua proses dalam ilmu kriptograpi, yaitu melakukan proses enskripsi dan deskripsi. Proses enskripsi memberi sandi *plaintext* (pesan yang telah dienskripsi atau diberikan kode) ke *chipertext* (teks sandi). Pesan yaitu data atau informasi yang bisa dibaca dan dipahami dari makna pesan tersebut.

Kriptografi adalah suatu cara untuk menyembunyikan pesan dimana pesan tersebut hanya dapat diketahui oleh orang tertentu dimana pesan itu seringkali disebut dengan enskripsi. Penelitian untuk mengamankan data dengan menggunakan Teknik kriptografi telah dilakukan [4]–[6]. Saat ini enskripsi dengan metode *Rivest Shamir Adleman* (RSA) telah banyak dikembangkan, dimana metode tersebut memakai 2 kunci yaitu kunci publik serta kunci pribadi. Kunci tersebut bisa diatur dimana semakin panjang *bit* pembentukan kunci maka semakin sukar untuk dipecahkan sebab sulitnya memfaktorkan 2 bilangan yang sangat besar dan itu disebut aman meskipun tidak pernah dibuktikan aman atau tidaknya. Tujuan dari kriptografi adalah untuk menjaga kerahasiaan (*confidentiality*), atau untuk menjaga pesan agar tidak dibaca oleh pihak yang tidak bersangkutan. Integritas data (*data integrity*), menjamin bahwa pesan tersebut masih asli dan tidak diubah atau dimanipulasi selama proses pengiriman. Otentikasi (*authentication*), untuk mengidetifikasi kebenaran dari pihak bersangkutan. *Non-repudiation* menjaga entitas yang bersangkutan melakukan suatu penyangkalan [7].

Metode *Caesar Cipher* ditemukan oleh *Julius Caesar* yang pada masa itu merupakan Kaisar Romawi. Metode ini digunakan untuk menyandikan pesan militer yang dikirim kepada panglima perang dan pesan resmi lain [8]. Sandi *Caesar* atau disebut juga dengan sandi geser merupakan salah satu metode enskripsi yang paling mudah dan terkenal. Gambar 1 merupakan ilustrasi kerja dari Sandi *Caesar* yang mengganti setiap huruf dengan menggeser tiga huruf menjadi teks sandi.



Gambar 1. Sandi *Caesar* Mengganti Setiap Huruf Dengan Menggeser Tiga Huruf Menjadi Teks Sandi

File yaitu kumpulan data dan informasi yang berbentuk teks yang tersimpan dalam komputer. *File* juga merupakan entitas dari data yang disimpan di dalam *folder* tergantung dari penggunanya dapat diakses serta digunakan oleh pengguna, *file* memiliki ekstensi yang berbeda sesuai dengan kegunaan dan jenis *file* [9].

Bahasa pemrograman *Java* dapat dioperasikan pada komputer maupun pada telepon genggam. *Java* juga merupakan bahasa pemrograman yang *portable* yang berarti mudah untuk digunakan karena hanya perlu menuliskan kode sekali dan dapat dijalankan disemua *platform*. Bahasa pemrograman ini awalnya dikembangkan oleh *James* sementara masih terkait dengan *Sun Microsystems*, *Gosling* saat ini bergabung dan menjadi bagian dari *Oracle* dan dipublikasikan pada 1995 [10]. *NetBeans* merupakan salah satu aplikasi pengembangan dengan lingkungan yang bebas (*open source*), yang terintegrasi dengan IDE (*Integrated Development Environment*). IDE memiliki dukungan pengembangan aplikasi pada beberapa bahasa pemrograman seperti *Java*, HTML5, PHP, dan C++. Hal tersebut memungkinkan membantu pengembangan aplikasi *Dekstop*, seluler, dan *Web* [11].

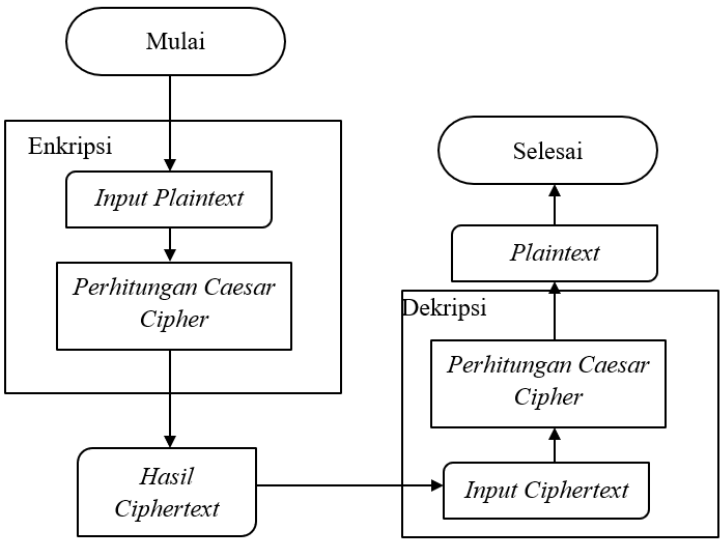
Penelitian ini melakukan kriptografi data dengan metode *Caesar Cipher* untuk mengamankan data *file* di *Java NetBeans*. Penelitian ini dilakukan untuk penulis bisa membantu menjaga keamanan data *file* dokumen, mengetahui penerapan kriptografi pada *Java NetBeans*. Batasan masalah dalam penelitian ini adalah:

a. Data atau *file* dokumen berekstensi *txt*.
b. Sistem dirancang untuk menjaga kerahasiaan dokumen sampai ketangan pemilik.

Dari penelitian ini diharapkan dapat membuat aplikasi yang dapat digunakan untuk melakukan pengamanan data dengan menggunakan metode *Caesar Cipher* di *Java NetBeans*.

2. METODE PENELITIAN

Penelitian ini menggunakan algoritma *Caesar Cipher* yang diproses dengan program *Java NetBeans* sehingga menghasilkan *ciphertext*. Diagram alur yang diterapkan dalam proses ini dapat dilihat pada Gambar 2 dibawah.



Gambar 2. *Flowchart* Algoritma *Caesar Cipher*

Penelitian ini dimulai dengan memasukkan data yang akan diproses. Data yang diproses masih berbentuk *plaintext*. *Plaintext* merupakan sebuah pesan atau informasi yang akan dikirim dalam bentuk

 doi: https://doi.org/10.32503/jtecs.v3i1.3210

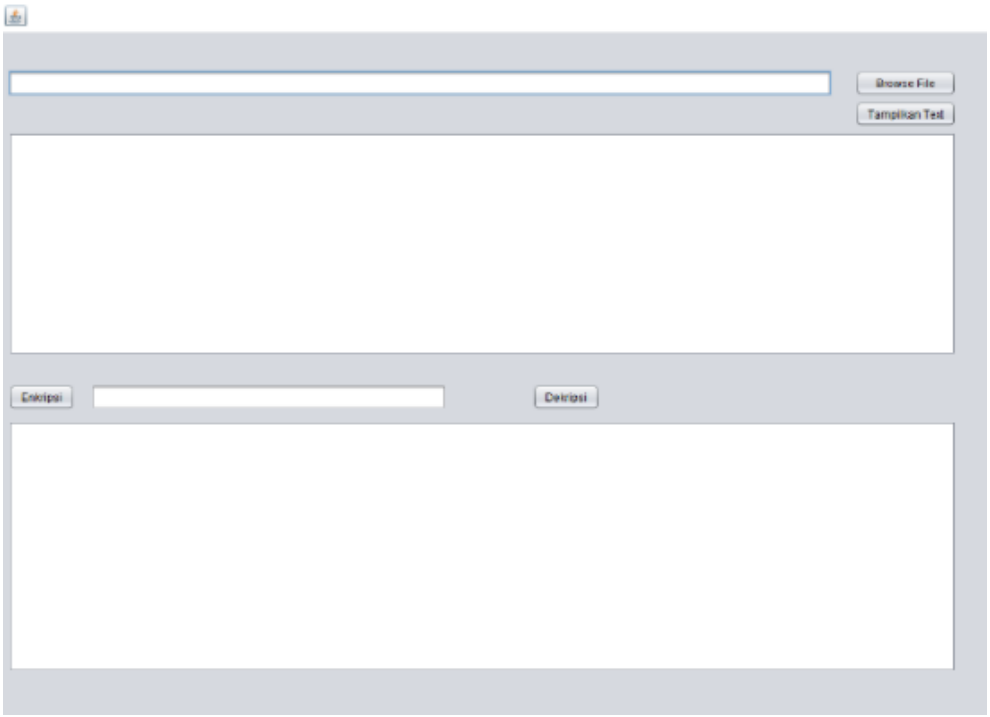
format yang mudah terbaca atau masih dalam bentuk yang asli. Selanjutnya pesan *plaintext* akan diproses menggunakan proses enskripsi. Enskripsi adalah sebuah proses yang diterapkan untuk merubah pesan asli menjadi *ciphertext* [12]. *Ciphertext* merupakan sebuah pesan yang telah dienskripsikan (tersandi) dan tidak bisa dibaca karena pesan ini merupakan hasil dari enskripsi data. Untuk membuka dan membaca pesan maka dilakukan proses deskripsi. Deskripsi merupakan proses mengubah data yang telah dienskripsi atau disandikan menjadi data asli kembali (*plaintext*). Kunci atau *key* merupakan sebuah bilangan yang dirahasiakan dan dimanfaaatkan dalam proses enskripsi dan deskripsi data [13]. Algoritma *Caesar Cipher* merupakan sebuah metode yang digunakan untuk melakukan proses enskripsi deskripsi data [14].

3. HASIL DAN PEMBAHASAN

Pembahasan terhadap hasil penelitian dan pengujian yang diperoleh disajikan dalam bentuk uraian teoritik, baik secara kualitatif maupun kuantitatif. Hasil percobaan implementasi kriptografi dengan metode *Caesar Cipher* yang diperoleh adalah sebagai berikut.

3.1. Halaman Utama

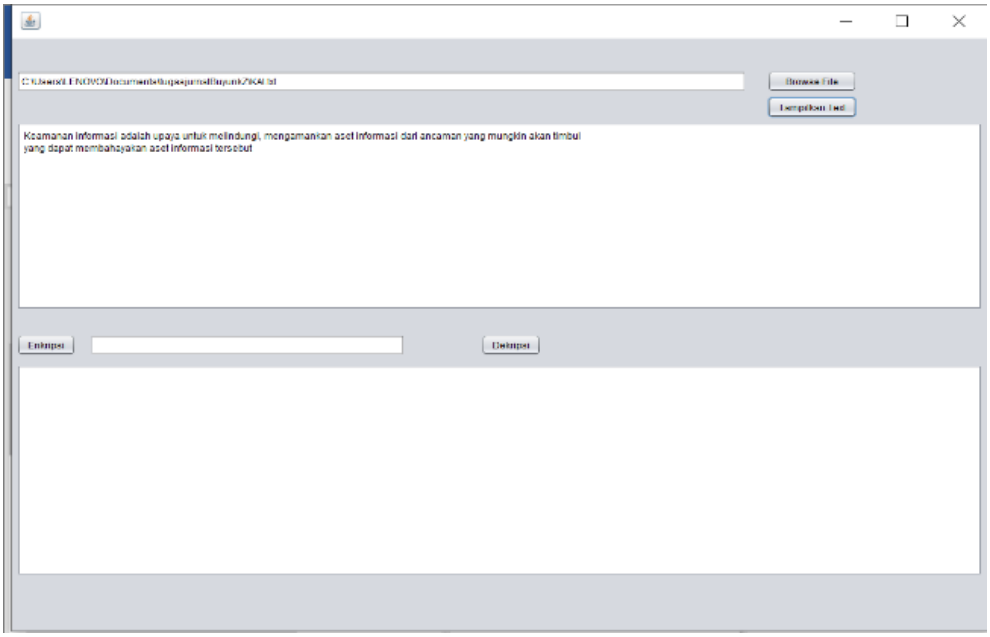
Pada halaman utama yang ditunjukkan oleh Gambar 3 ini menampilkan tampilan awal yang berisikan menu yang dapat dipilih dan digunakan. Pada bagian tengah antara *button* enskripsi dan deskripsi terdapat kolom untuk memasukkan *password*.



Gambar 3. Halaman Utama

3.2. Halaman Input Data dan Enkripsi

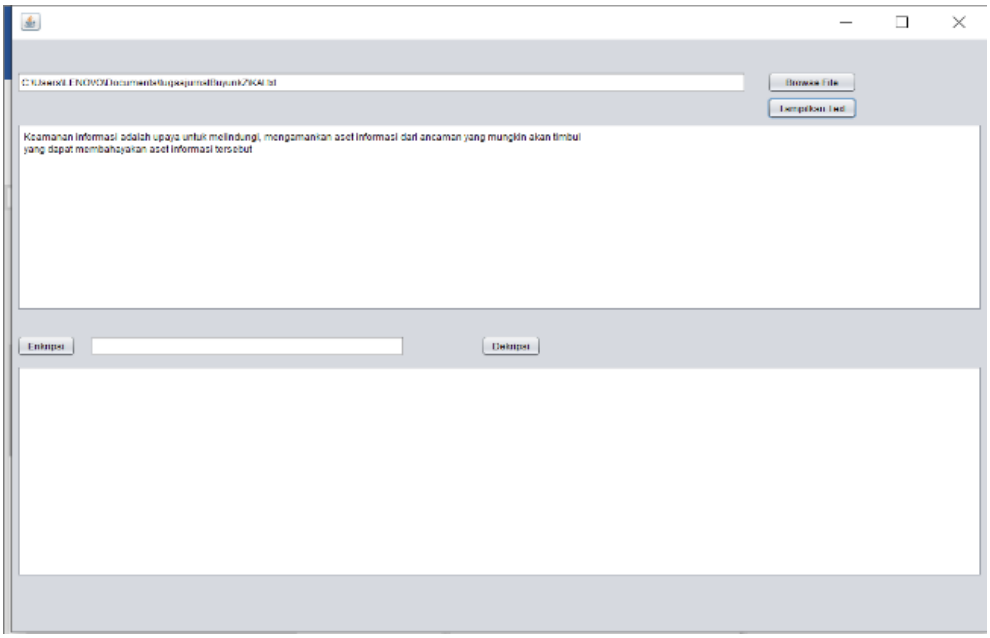
Dalam halaman ini pengguna bisa memasukkan *file* yang dapat di masukkan dengan menekan tombol "*Browse File*" lalu menekan "Tampilkan *Text*", maka teks yang dimasukkan akan muncul.



Gambar 4. Halaman *Input* Data

Dari tampilan Gambar 4 menunjukkan bahwa halaman *input* data berfungsi yang ditandai dengan berfungsinya tombol "*Browse File*" dan tombol "Tampilkan *Text*".

Proses enskripsi data seperti pada Gambar 5 merupakan data asli yang tidak akan ditampilkan lagi dan hanya akan menampilkan data yang sudah disandi.



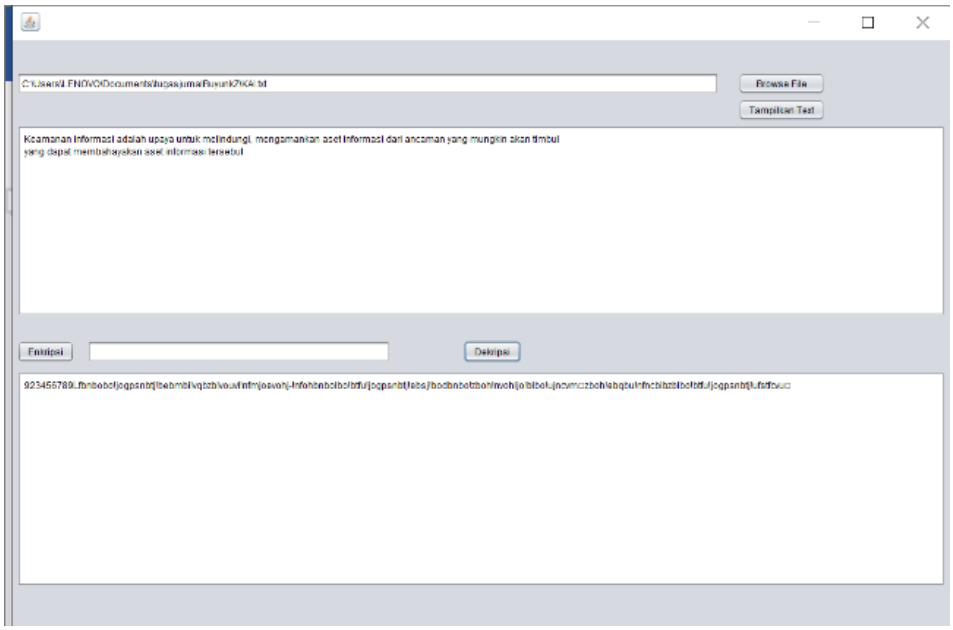
Gambar 5. Tampilan Enskripsi

Dari tampilan Gambar 5 menunjukkan bahwa sistem dapat melakukan proses enskripsi yang ditandai dengan munculnya data enskripsi pada kolom enskripsi.

 doi: https://doi.org/10.32503/jtecs.v3i1.3210

3.3. Proses Dekripsi

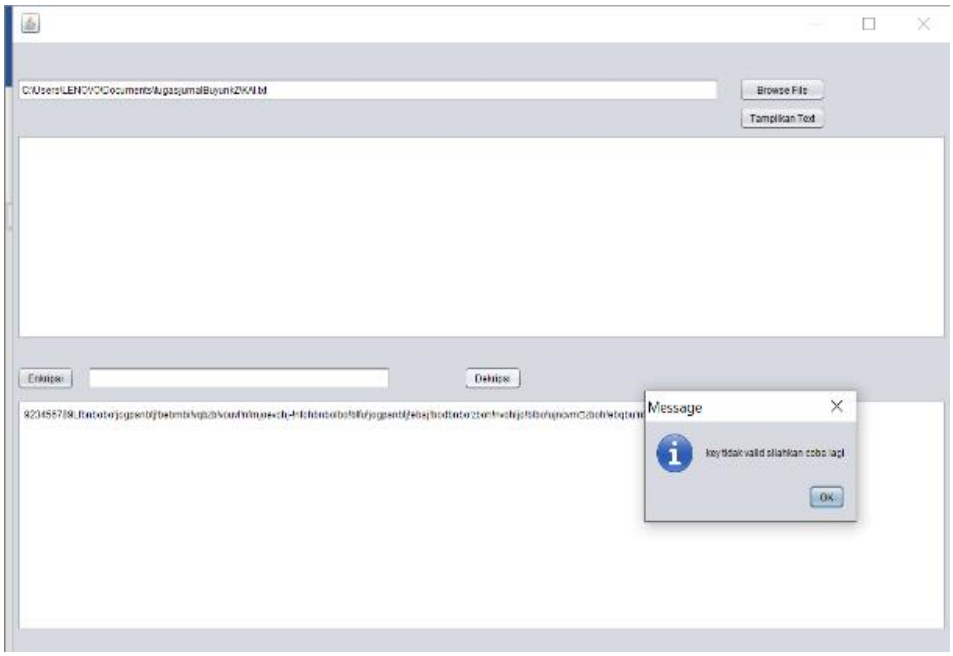
Proses deskripsi seperti yang ditunjukkan oleh Gambar 6, dimana data yang ditampilkan dengan sandi akan ditampilkan menjadi data yang asli.



Gambar 6. Tampilan Proses Deskripsi

Dari tampilan Gambar 6 menunjukkan bahwa sistem dapat melakukan proses deskripsi yang ditandai dengan munculnya data hasil deskripsi pada kolom deskripsi.

Tampilan gambar 7 menampilkan pesan jika *password* yang dimasukkan saat proses deskripsi salah.



Gambar 6. Tampilan Proses Deskripsi

Dari pengujian proses deskripsi pada Gambar 7 menampilkan pesan *key* tidak valid jika *password* yang dimasukkan salah saat proses deskripsi, sehingga dapat disimpulkan bahwa metode *Caesar Cipher* dapat berfungsi untuk mengamankan data *file* di *Java Netbeans*.

4. KESIMPULAN

Berdasarkan hasil penelitian pada implementasi kriptografi dengan metode *Caesar Cipher* untuk mengamankan data *file* di *Java Netbeans* maka dapat disimpulkan bahwa pengamanan data menggunakan Metode *Caesar Cipher* terbukti dapat dilakukan pada *Java Netbeans*.

Dimana kriptografi hanya bisa dilakukan oleh orang-orang tertentu yang paham akan penggunaannya sehingga kriptografi dapat dikategorikan sebagai tempat yang aman untuk menyimpan data yang bersifat rahasia. Dan juga *Caeser Cipher* (sandi geser) merupakan salah satu metode enskripsi yang paling sederhana dan terkenal.

Dalam penelitian ini *file* yang bisa diproses enskripsi adalah *file* dokumen yang berbentuk teks berekstensi *.txt*. Diharapkan dalam penelitian selanjutnya pengamanan data bisa lebih bervariasi dan dapat dikembangkan dan diterapkan kesemua *file* dengan sempurna.

DAFTAR PUSTAKA

[1] A. Teguh, F. Alhamdi, and R. F. Siahaan, "Penerapan Kriptografi Dalam Pengamanan Pesan Text Berbasis Android Dengan Menggunakan Metode Rijndael," Jurnal Mahajana Informasi, vol. 6, no. 2. 2021.

[2] A. Ramadhani, "Keamanan Informasi," Nusant. - J. Inf. Libr. Stud., vol. 1, no. 1, p. 39, 2018, doi: 10.30999/n-jils.v1i1.249.

[3] T. Limbong, "Pengujian Kriptografi Klasik Caesar Chipper Menggunakan Matlab," Semin. Nas. Inov. dan Teknol. Inf. Sept., no. September 2015, pp. 77–80, 2015.

[4] F. Alfiah, R. Sudarji, dan D. T. al Fatah, "Aplikasi Kriptografi Dengan Menggunakan Algoritma Elgamal Berbasis Java Desktop Pada Pt. Wahana Indo Trada Nissan Jatake," ADI Bisnis Digital Interdisiplin Jurnal, vol. 1, no. 1, 2020, doi: 10.34306/abdi.v1i1.114.

[5] O. Dakhi, M. Masril, R. Novalinda, J. Jufrinaldi, dan A. Ambiyar, "Analisis Sistem Kriptografi dalam Mengamankan Data Pesan Dengan Metode One Time Pad Cipher," INVOTEK: Jurnal Inovasi Vokasional dan Teknologi, vol. 20, no. 1, 2020, doi: 10.24036/invotek.v20i1.647.

[6] Y. Yusfrizal, "Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper Dan Rsa Berbasis Android," JTIK (Jurnal Teknik Informatika Kaputama), vol. 3, no. 2, hlm. 29–37, 2019.R. Santi, "Implementasi Algoritma Enkripsi Playfair pada File Teks," None, vol. 15, no. 1, p. 246766, 2010.

[7] khairani Puspita and M. R. Wayahdi, "Analisis Kombinasi Metode Caesar Cipher , Vernam Cipher , Dan Hill Cipher Dalam Proses Kriptografi," Semin. Nas. Teknol. Inf. dan Multimed. 2015, no. Februari, pp. 43–48, 2015.

[8] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced

Encryption Standard," Inform. Mulawarman J. Ilm. Ilmu Komput., vol. 10, no. 1, p. 20, 2016, doi: 10.30872/jim.v10i1.23.

[9] A. P. C. Udaksana and W. R. Kusaeri, "Rancang Bangun Aplikasi Digital School Dengan Java NetBeans IDE 8.1," Irons, pp. 332–336, 2018, [Online]. Available: https://jurnal.polban.ac.id/proceeding/article/view/1118/918.

[10] H. Dhika, N. Isnain, and M. Tofan, "Manajemen Villa Menggunakan Java Netbeans Dan Mysql," IKRA-ITH Inform. J. Komput. dan Inform., vol. 3, no. 2, pp. 104–110, 2019, [Online]. Available: https://journals.upi-yai.ac.id/index.php/ikraith-informatika/article/view/324.

[11] M. Metode Blowfish Dengan Bahasa Pemrograman Java Mohamad Natsir, K. Kunci, K. Simetris, and A. Blowfish, "Pengembangan Prototype Sistem Kriptografi Untuk Enkripsi Dan Dekripsi Data Office," Jurnal, vol. 6, pp. 2089–5615, 2016.

[12] G. A. Sahputra and T. Fatimah, "Implementasi Kripptografi Dengan Metode Algoritma Elgamal Untuk Keamanan Database Berbasis Java Desktop Pada PT. Makmur Supra Nusantara," Skanika, Vol. I, No. 1 Maret 2018, vol. 1, no. 1, pp. 309–315, 2018.

[13] M. D. Irawan, "Implementasi Kriptografi Vigenere Cipher Dengan Php," J. Teknol. Inf., vol. 1, no. 1, p. 11, 2017, doi: 10.36294/jurti.v1i1.21.