E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 01 Nomor 01 Maret 2023

Implementasi Kriptografi Vigenere Cipher untuk Keamanan Data Informasi Desa

[1]Erva Irianti, [2*]Dewi Fatmarani Surianto, [3]Ainun Zahra Adistia, [4]Muh. Juharman, [5]Jumadil Ahmad Safi'i

[12345]Universitas Negeri Makassar, Jl. A.P. Pettarani, Kota Makassar, Sulawesi Selatan

Email: ervairianti3@gmail.com[1], dewifatmaranis@unm.ac.id[2], annzahradistia@gmail.com[3], muhjuharman@gmail.com[4], jumadilahmadsafi21@gmail.com[5]

Received : 13 Januari 2023
Accepted : 25 Februari 2023
Published : 6 Maret 2023

ABSTRAK

Keamanan data pada informasi desa menjadi isu yang sangat penting karena memuat banyak data informasi desa. Data yang penting tidak bisa dipungkiri bahwasanya data bisa diedit atau diubah oleh orang yang tidak berhak. Sehingga data tersebut menjadi tidak aman. Oleh karena itu, butuh Teknik untuk mengamankan data yaitu menggunakan Teknik kriptografi klasik *Vigenere Cipher*, untuk menjaga keamanan dan kerahasiaan pesan atau informasi agar tidak dapat dibaca oleh sembarang orang, maka dirancang aplikasi berbasis desktop dengan menggunakan bahasa pemrograman java yang dilakukan pada *software* Netbeans IDE untuk mengimplementasikan algoritma *vigenere cipher* sebagai salah satu Teknik untuk mengamankan informasi desa.

Kata Kunci: Keamanan Data, Kriptografi, *Vigenere Cipher*, Bahasa Pemrograman Java

ABSTRACT

Data security on village information is a very important issue because it contains a lot of village information data. Important data cannot be denied that data can be edited or changed by unauthorized persons. So the data becomes insecure. Therefore, a technique is needed to secure data, namely using the classic Vigenere cipher cryptography technique, to maintain the security and confidentiality of messages or information so that it cannot be read by anyone, a desktop-based application is designed using the Java programming language which is carried out on the Netbeans IDE software to implementing the vigenere cipher algorithm as a technique for securing village information.

Keywords: Data Security, Cryptography, Vigenere Cipher, Java Programming Language

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 01 Nomor 01 Maret 2023

1. PENDAHULUAN

Peranan teknologi informasi saat ini sangat dibutuhkan dalam kegiatan sehari-hari baik dalam kegiatan pemerintahan, kesehatan, pendidikan, perbankan, dan instansi lainnya. Penggunaan komputer terkoneksi satu dengan yang lain melalui jaringan dengan berbagai media transmisi. Hampir seluruh pekerjaan pada setiap instansi, khususnya pada kantor desa menggunakan komputer terutama dalam pengolahan data informasi desa yang memungkinkan adanya kejahatan *cyber* yang dapat membocorkan, merusak data atu informasi desa. Sistem keamanan data Program Keluarga Harapan (PKH), Bantuan Pangan Non Tunai (BNPT) dan Bantuan Langsung Tunai (BLT) perlu diamankan agar tidak terjadi kejahatan *cyber*. Sistem keamanan data dapat dibangun dengan menggunakan sebuah ilmu (Febrianingsih & Hafiz, 2019). Kriptografi digunakan untuk menjaga keamanan data atau informasi, baik informasi yang ditransmisikan melalui saluran komunikasi maupun informasi yang disimpan pada media penyimpanan. Hampir semua kehidupan saat ini dilingkupi oleh kriptografi sebagai alat untuk menjamin keamanan, kerahasiaan informasi yang menggunakan persamaan matematis untuk melakukan proses enkripsi dan deskripsi. Teknik ini untuk mengkonversi data ke dalam bentuk kode-kode tertentu agar informasi tidak dapat terbaca oleh siapapun kecuali pihak yang berhak (Silalahi & Sindar, 2020).

Berbagai cara dilakukan untuk mengamankan data ataupun informasi diantaranya yaitu menggunakan ilmu kriptografi. Kriptografi merupakan ilmu yang mempelajari tentang bagaimana cara menjaga agar data atau informasi tetap aman. Beragam macam Teknik digunakan untuk upaya mengamankan data atau informasi yang sangat penting (Triana et al., 2020).

Ada berbagai cara yang dapat digunakan untuk melakukan keamanan data dan informasi, salah satunya adalah dengan menggunakan teknik kriptografi metode *Vigenere cipher* yang merupakan salah satu algoritma kriptografi klasik yang diperkenalkan pada abad 16 atau pada tahun 1986. Algoritma kriptografi diterbitkan oleh seseorang yang berasal dari negara Prancis yaitu Vigenere dan Blaise, dan algoritma ini sebelumnya telah dijelaskan dalam buku *La Cifra del Sig. Giovan Batista Belaso*, sebuah buku yang ditulis oleh Giovan Batista Belaso, pada tahun 1553 (Karman & Nurhasan, 2019).

Cara kerja dari *Vigenere cipher* yaitu mengenkripsi pesan plainteks dengan cara memindahkan huruf pada pesan tersebut sejauh kunci deret alphabet (Silalahi & Parlina, 2021).

2. METODE PENELITIAN

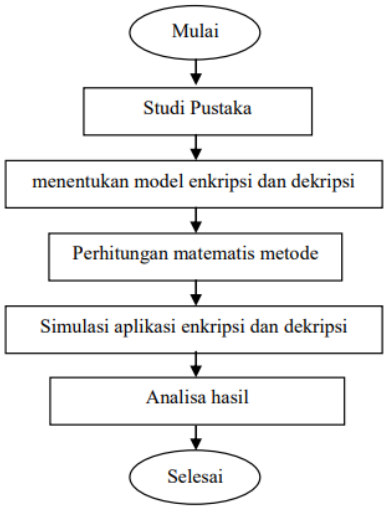
2.1 Jenis Penelitian

Jenis penelitian yang dilakukan adalah penelitian terapan yaitu penelitian yang bertujuan untuk menyelesaikan masalah dengan mengaplikasikan teori yang mendasari penelitian yang dikaji terlebih dahulu menyusun konsep-konsep yang berkaitan dengan kriptografi secara matematis (Febrianingsih & Hafiz, 2019).

Metode penelitian ini meliputi penentuan model enkripsi, penyelesaian algoritma enkripsi, pembuatan simulasi enkripsi dan analisa hasil dari simulasi enkripsi (Karman & Nurhasan, 2019). Diagram alir perancangan simulasi pada penelitian ini secara lengkap dapat dilihat pada Gambar di bawah ini.

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 01 Nomor 01 Maret 2023



Gambar 1. Jenis Penelitian

Gambar diatas dapat diketahui penelitian ini dimulai dari studi pustaka, setelah menemukan permasalahan kemudian menentukan model enkripsi dan dekripsi, langkah selanjutnya adalah menentukan perhitungan matematis. Setelah menentukan perhitungan matematis dibuat aplikasi simulasi sebagai uji coba dari perhitungan matematis tersebut dan di analisa apakah sudah benar atau belum (Maricar & Sastra, 2018).

2.2 Metode Pengembangan Sistem

Metode pengembangan sistem yang penulis gunakan dalam penelitian ini adalah metode *Extreme Programming*. *Extreme Programming* yaitu sebuah metode dalam pengembangan sistem yang dilakukan untuk membuat pembaruan sistem yang berjalan (Silalahi & Parlina, 2021). Berikut ini tahapan-tahapan yang akan dilakukan dengan menggunakan metode *Extream Programming* :

1) *Planning*/Perencanaan

Tahap perancanaan dimulai dari pengumpulan kebutuhan yang membantu tim teknikal untuk memahami konteks bisnis dari sebuah aplikasi. Selain itu pada tahap ini mendefinisikan output yang akan dihasilkan, fitur yang dimiliki oleh aplikasi dan fungsi dari aplikasi yang dikembangkan.

2) *Design*/Perancangan

Metode ini menekankan desain aplikasi yang sederhana, bagaimana sebuah aplikasi bisa berjalan dengan baik.

3) *Coding*/Pengkodean

Konsep utama dari tahapan pengkodean pada extreme programming adalah bagaimana menyusun kode yang sederhana sehingga mudah dipahami.

4) *Testing*/Pengujian

Tahap ini lebih fokus pada pengujian fitur dan fungsionalitas dari aplikasi.

2.3 Perancangan Sistem

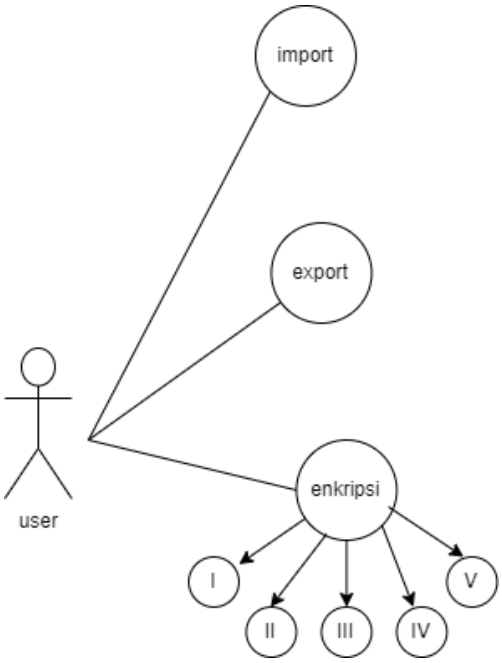
Tahap perancangan sistem adalah setelah tahap analisa sistem selesai dilakukan, maka analisa sistem mendapatkan gambaran dengan jelas tentang apa yang harus dilakukan, selanjutnya analisa sistem memikirkan bagaimana membentuk sistem tersebut. Adapun alat rancang yang digunakan adalah sebagai berikut:

a. *Use Case*

Use case merupakan bagian terpenting dari fungsionalitas yang dimiliki *system* yang akan menggambarkan bagaimana seseorang akan menggunakan dan memanfaatkan *system*. Diagram ini juga mendekripsikan apa yang akan dilakukan oleh *system*. Diagram *use case* pusat peminjaman ruangan dan peralatan dilihat dari gambar dibawah ini.

E-ISSN: 2986-7258
P-ISSN : 2986-724X

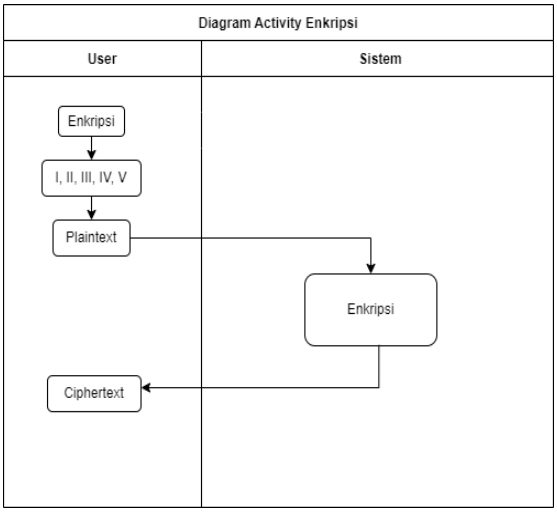
PISCES Volume 01 Nomor 01 Maret 2023



Gambar 2. *Use Case*

b. Diagram *Activity*

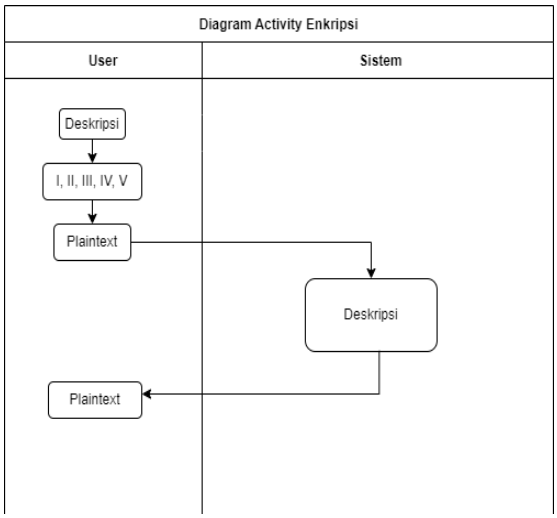
Diagram *activity* memberikan gambaran rancangan alur disetiap fungsi yang ada di dalam *system*. Diagram *activity* menggambarkan berbagai alir aktivitas dalam *system* yang sedang dirancang, bagaimana masing-masing alir berawal *decision* yang mungkin terjadi, dan bagaimana mereka berakhir.



Gambar 3. Diagram *Activity* Enkripsi

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 01 Nomor 01 Maret 2023



Gambar 4. Diagram *Activity* Deksripsi

Gambar di atas dapat dilihat panel kiri atas merupakan pilihan antara enkripsi atau dekripsi, kemudian di sampingnya ada pilihan untuk melakukan pergeseran antara 1 sampai 5 pergeseran, dan di bawah panel itu adalah *input* untuk *plaintext* yaitu teks yang akan di enkripsi, kemudian di bawah panel itu ada *chiper text* yaitu hasil dari proses enkripsi. Pada panel sebelah kanan merupakan fitur untuk *import* dan *export*, yaitu fitur untuk mengambil file yang ada di dalam komputer kemudian *export* untuk menyimpan hasil enkripsi ke dalam komputer dengan bentuk file teks yang bisa dibuka dengan notepad (Rakhman & Kurniawan, 2015).

3. HASIL DAN PEMBAHASAN

Penelitian yang dilakukan membutuhkan aplikasi berbasis desktop untuk mengimplementasikan keamanan data informasi administrator desa dengan menggunakan algoritma *vigenere cipher* sebagai pengujian keamanan data setiap informasi yang ada.

Keamanan data kependudukan menjadi sangat penting karena memuat beberapa informasi yang penting didalamnya seperti nama penerima Program Keluarga Harapan (PKH), Bantuan Pangan Non Tunai (BPNT), Kartu Indonesia Pintar (KIP), Bantuan Langsung Tunai (BLT) Dana Desa, yang hanya dimuat dalam bentuk sebuah file Microsoft Excel yang sangat tidak terjamin keamanannya dan dengan mudah diubah ataupun dimanipulasi oleh orang yang tidak berkepentingan. Sehingga dalam menyelesaikan permasalahan tersebut maka dibutuhkan suatu aplikasi yang mampu melakukan enkripsi, deskripsi guna untuk mengamankan data Kependudukan Desa.

Proses enkripsi dengan sandi *Vigenere* dapat ditulis matematis, dengan menggunakan penjumlahan dan operasi modulus,

Pi = (Ci – Ki) mod 26

Atau

Ci = (Pi + Ki) – 26 kalau hasil penjumlahannya Pi dan Ki lebih dari 26

Rumus Deskripsi *Vigenere cipher*

Pi = (Ci – Ki) mod 26

Atau

Ci = (PI – Ki) + 26 kalau hasil pengurangan Ci dengan Ki kurang pada :

Ci = Nilai decimal karakter *Ciphertext* ke-i

Pi = Nilai decimal karakter *plaintext* ke-i

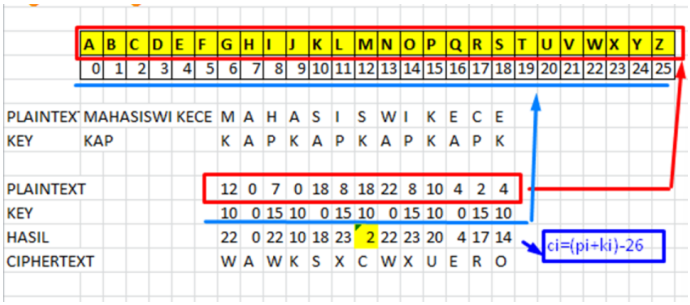
Ki = Nilai decimal karakter kunci ke-i

Nilai decimal karakter A = 0, B=1, C=2 … Z=25

Algoritma *Vigenere* Secara Matematis :

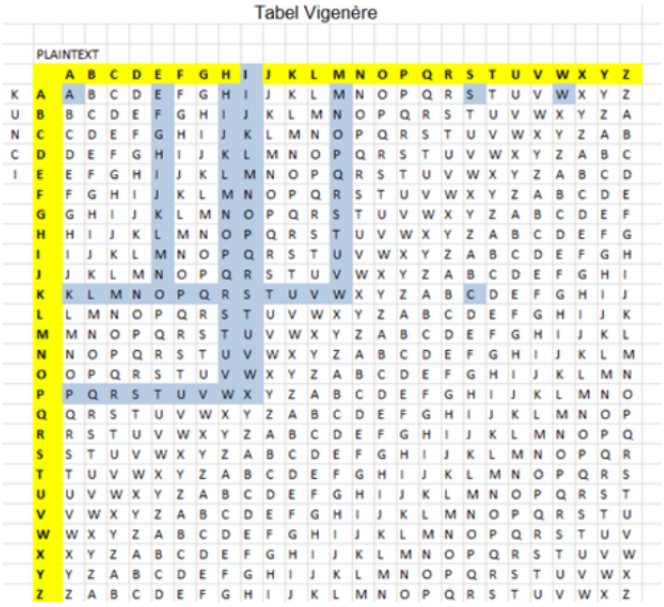
E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 01 Nomor 01 Maret 2023



Gambar 5. Algoritma *Vigenere* Matematis

Cara Kerja Menggunakan Tabel Algoritma *Vigenere cipher* :

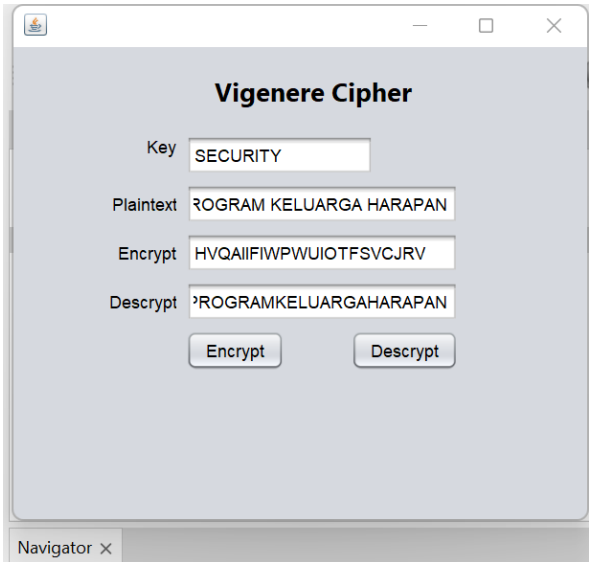


Gambar 6. Tabel *Vigenere*

Tampilan aplikasi berbasis desktop menggunakan *Vigenere cipher* :

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 01 Nomor 01 Maret 2023



Gambar 7. Tampilan Aplikasi

Sebagai uji coba aplikasi :
Key : SECURITY
Plaintext : PROGRAM KELUARGA HARAPAN
Encrypt : HVQAIIFIWPWUIOTFSVCJRV
Descrypt : PROGRAMKELUARGAHARAPAN

Konsep algoritma implementasi *vigenere cipher* yaitu ketika pengguna ingin melakukan enkripsi pesan atau menyandikan pesan, maka pengguna harus memiliki dan memasukkan *key* terlebih dahulu kemudian memasukkan pesan *plaintext*. Setelah itu klik *button encrypt* untuk menghasilkan pesan *encrypt* secara otomatis (Wiharto & Irawan, 2018).

4. KESIMPULAN DAN SARAN

Dari hasil penelitian yang telah dilakukan didapatkan kesimpulan bahwa kesadaran terhadap keamanan informasi data pada desa masih rendah. Hal tersebut ditunjukkan dari kurangnya kesadaran untuk mengamankan diri dari aplikasi yang kurang bisa dipercaya sehingga informasi pribadi dapat diubah atau disebar.

REFERENSI

Febrianingsih, R., & Hafiz, A. (2019). IMPLEMENTASI KRIPTOGRAFI BERBASIS CAESAR CHIPER UNTUK KEAMANAN DATA. *Jik*, 7(2), 81–86. doi: 10.35959/jik.v7i2.163.

Silalahi, I., & Sindar, A. (2020). Penerapan Kriptografi Keamanan Data Administrasi Kependudukan Desa Pagar Jati Menggunakan SHA-1. *Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)*, 3(2). doi: 10.32672/jnkti.v3i2.2413.

Triana, F., Endri, J., & Salamah, I. (2020). Implementasi Teknik Kriptografi CAESAR CIPHER Untuk Keamanan Data Informasi Berbasis Android. *Jurnal RESTI : Rekayasa Sistem dan Teknologi informasi*, 4(4), 627-634.

Karman, J., & Nurhasan, A. (2019). PERANCANGAN SISTEM KEAMANAN DATA INVENTORY BARANG DI TOKO NANDA BERBASIS WEB MENGGUNAKAN METODE KRIPTOGRAFI VIGENERE CIPHER. *jti*, 11(1), 29–36. doi: 10.32767/jti.v11i1.451.

Silalahi, R., Parlina, I., Sumarno, Gunawan, I., Saputra, W. (2021). IMPLEMENTASI ALGORITMA CAESAR CIPHER DAN ALGORITMA RSA UNTUK KEAMANAN DATA SURAT WASIAT PADA KANTOR

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 01 Nomor 01 Maret 2023

NOTARIS/PPAT ROBERT TAMPUBOLON, S.H. *Jurnal Sosial dan Teknologi (SOSTECH)*, 1(4), 282-293. doi: 10.36418/jurnalsostech.v1i4.64.

Maricar, M., A., & Sastra, N., P. (2018). Efektivitas Pesan Teks Dengan Cipher Substitusi, Vigenere Cipher, dan Cipher Transposisi. *JTE*, 17(1), 59. doi: 10.24843/MITE.2018.v17i01.P08.

Rakhman, A., A., & Kurniawan, A., W. (2015). IMPLEMENTASI ALGORITMA KRIPTOGRAFI RIVEST SHAMIR ADLEMAN (RSA) DAN VIGENERE CIPHER PADA GAMBAR BITMAP 8 BIT. Jurnal Teknologi Informasi (Techno.com), 14(2), 122-134.

Wiharto, Y., & Irawan, A. (2018). Sistem Kehadiran Menggunakan Quick Respone Code Dengan Enkripsi Algorithm Message Digest 5 dan Vigenere cipher Pada SpeedCom IT Consulting. *Jurnal Sistem Komputer dan Kecerdasan Buatan*, 2(1), 42-56.