

Penerapan Kriptografi Vigenere Cipher Pada Kekuatan Kata Sandi Di Sistem Aplikasi Puskesmas

Application of Vigenere Cipher Cryptography on Password Strength in Community Health Center Application Systems

Zhafira Abadiningrum Khafianti¹, D. Wita Aeni², Ariqoh Zulaika Zuhrah³

Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa³

Email: @zhafirakhafianti19@gmail.com , @witaeni126@gmail.com *,
@ariqohzulaika@gmail.com*

Abstract

Information security in the Puskesmas application is crucial for protecting patient health data. One method that can be applied to increase data security is to use cryptographic algorithms. This research aims to examine the application of Vigenere Cipher to the strength of passwords used in Puskesmas applications. Vigenere Cipher was chosen because of its ability to provide a good level of security and adequate encryption-decryption process speed. This research methodology involves analyzing the strength of passwords in the Puskesmas application, implementing Vigenere Cipher, and evaluating system performance. The research results show that the application of Vigenere Cipher is able to increase password security by overcoming several weaknesses that may exist in previously existing encryption methods. Performance evaluation also shows that the encryption-decryption process can be carried out efficiently without sacrificing overall application performance. This research contributes to the development of information security in Community Health Center applications and can be used as a reference for improving health data security at the institutional level. In addition, the findings of this study can serve as a basis for further research in the development of more sophisticated cryptographic methods to protect sensitive information in the health sector. The main contribution of this research is the introduction of cryptographic methods that are effective in improving information security at the Community Health Center level. It is hoped that the results of this research can become a basis for further development in protecting health information effectively in the public health service environment.

Keywords – Cryptography, Vigenere Cipher, Encryption – Decryption, Data Protection

Abstrak

Keamanan informasi dalam aplikasi Puskesmas menjadi suatu hal yang krusial untuk melindungi data kesehatan pasien. Salah satu metode yang dapat diterapkan untuk meningkatkan keamanan data adalah dengan menggunakan algoritma kriptografi. Penelitian ini bertujuan untuk mengkaji penerapan Vigenere Cipher pada kekuatan kata sandi yang digunakan di dalam aplikasi Puskesmas. Vigenere Cipher dipilih karena kemampuannya dalam memberikan tingkat keamanan yang baik dan kecepatan proses enkripsi-dekripsi yang memadai. Metodologi penelitian ini melibatkan analisis kekuatan kata sandi yang ada pada aplikasi Puskesmas, implementasi Vigenere Cipher, dan evaluasi kinerja sistem. Hasil penelitian menunjukkan bahwa penerapan Vigenere Cipher mampu meningkatkan keamanan kata sandi dengan mengatasi beberapa kelemahan yang mungkin ada pada metode enkripsi yang sudah ada sebelumnya. Evaluasi kinerja juga menunjukkan bahwa proses enkripsi-dekripsi dapat dilakukan dengan efisien tanpa mengorbankan performa aplikasi secara keseluruhan. Penelitian ini memberikan kontribusi pada pengembangan keamanan informasi di dalam aplikasi Puskesmas dan dapat dijadikan acuan untuk peningkatan keamanan data kesehatan pada tingkat institusional. Selain itu, temuan penelitian ini dapat menjadi dasar

untuk penelitian lebih lanjut dalam pengembangan metode kriptografi yang lebih canggih untuk melindungi informasi sensitif di bidang kesehatan. Kontribusi utama penelitian ini adalah pengenalan metode kriptografi yang efektif dalam meningkatkan keamanan informasi di tingkat Puskesmas. Diharapkan hasil penelitian ini dapat menjadi landasan untuk pengembangan lebih lanjut dalam melindungi informasi kesehatan secara efektif di lingkungan pelayanan kesehatan masyarakat.

Kata Kunci – Kriptografi, Vigenere Cipher, Enkripsi – Dekripsi, Perlindungan Data

Pendahuluan

Dalam era kemajuan teknologi informasi, keamanan data menjadi aspek yang sangat krusial, terutama dalam konteks sistem aplikasi Puskesmas. Sistem ini menyimpan informasi sensitif seperti riwayat medis pasien, resep obat, dan informasi pribadi lainnya. Oleh karena itu, perlindungan terhadap data tersebut menjadi suatu keharusan untuk mencegah akses yang tidak sah dan kebocoran informasi yang dapat merugikan pasien dan lembaga kesehatan. Pada latar belakang ini, penelitian ini menggali aspek keamanan sistem aplikasi Puskesmas, khususnya pada kekuatan kata sandi yang digunakan dalam mekanisme keamanan. Keberhasilan sebuah sistem keamanan sangat bergantung pada kualitas dan kekuatan algoritma kriptografi yang diterapkan. Salah satu metode kriptografi yang dikenal tangguh dan dapat diterapkan secara efektif adalah Vigenere Cipher.[1] Tetapi banyak dari para pengguna password yang membuat password secara sembarangan tanpa mengetahui kebijakan pengamanan (password policy) dan bagaimana membuat password yang kuat (strong password). Mereka tidak sadar dengan bahayanya para ‘penyerang’ (attacker) yang dapat mencuri atau mengacak-acak informasi tersebut. Jadi, dapat dikatakan bahwa password sudah menjadi bagian dalam kehidupan kita. Pengembangan teknologi informasi dalam dunia kesehatan, khususnya melalui sistem aplikasi Puskesmas, telah memberikan kontribusi signifikan terhadap efisiensi dan akurasi dalam manajemen data pasien. Namun, seiring dengan kemajuan ini, risiko keamanan informasi juga semakin meningkat. Sistem aplikasi Puskesmas yang mengandung data sensitif, seperti riwayat medis, resep obat, dan informasi identitas pasien, menjadi target potensial bagi pihak yang tidak bertanggung jawab.[2]

Ketidakamanan dalam penyimpanan dan pengelolaan data kesehatan dapat menyebabkan konsekuensi serius, seperti penyalahgunaan informasi medis, pencurian identitas, dan bahkan ancaman terhadap integritas dan kerahasiaan pasien. Oleh karena itu, perlunya penerapan langkah-langkah keamanan yang lebih efektif dan canggih menjadi suatu kebutuhan mendesak. Pada konteks ini, penerapan algoritma kriptografi Vigenere Cipher diharapkan dapat memberikan lapisan keamanan tambahan dengan menyulitkan upaya peretasan atau dekripsi yang dilakukan oleh pihak yang tidak berwenang. Dengan mengamankan kata sandi, data pasien dapat lebih terlindungi dan integritas sistem dapat tetap terjaga. Melalui pemahaman yang mendalam terhadap tantangan keamanan yang dihadapi oleh sistem aplikasi Puskesmas, penelitian ini bertujuan untuk menghadirkan solusi yang konkret dan dapat diimplementasikan untuk meningkatkan keamanan informasi dalam konteks kesehatan. Dengan menggabungkan keahlian dalam bidang kriptografi dengan kebutuhan khusus dalam dunia kesehatan, penelitian ini berusaha untuk memberikan kontribusi positif terhadap pengembangan keamanan sistem aplikasi Puskesmas.[3]

Tinjauan Pustaka

Kata Yunani cryptos dan graphia, yang diterjemahkan sebagai “menulis secara rahasia,” adalah asal mula kriptografi. Kajian kriptografi berfokus pada bagaimana pesan yang diberikan oleh pengirim dapat diterima dengan aman oleh penerima. Untuk mencegah pihak lain mengetahui informasi yang terkandung pada data, kriptografi bekerja untuk menjamin kerahasiaannya. Enkripsi digunakan untuk mengkonversikan informasi atau data menjadi versi baru yang aman dan nyaris tidak bisa diidentifikasi sebagai informasi asli. Ada dua prosedur dalam ilmu kriptografi yaitu enkripsi dan dekripsi. Tingkat kepercayaan, integritas data, otentikasi entitas serta otentikasi keaslian data hanyalah sebagian kecil dari konsep matematika yang berkaitan dengan perlindungan informasi yang dipelajari dalam kriptografi.

Vigenère cipher adalah salah satu algoritma kriptografi klasik yang diperkenalkan pada abad 16 atau kira-kira pada tahun 1586. Algoritma kriptografi ini dipublikasikan oleh seorang diplomat dan juga kriptologis yang berasal dari Prancis, yaitu Blaise de Vigenère, namun sebenarnya algoritma ini telah digambarkan sebelumnya pada buku La Cifra del Sig. Giovan Batista Belaso, sebuah buku yang ditulis oleh Giovan Batista Belaso, pada tahun 1553.

Vigenère cipher dikenal luas karena cara kerjanya yang mudah dimengerti dan dijalankan serta bagi para pemula akan sulit untuk dipecahkan. Pada saat kejayaannya, Vigenère Cipher dijuluki sebagai le chiffre indéchiffrable (bahasa Prancis: “sandi yang tak terpecahkan”). Teknik dari Vigenère Cipher dapat dilakukan dengan 2 cara yaitu Angka dan Huruf.

$$C_i = (P_i + K_i) \bmod 26$$

$$P_i = (C_i - K_i) \bmod 26$$

Dimana:

C_i = nilai desimal karakter ciphertext ke- i

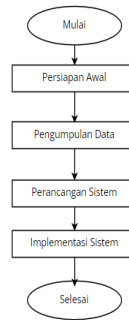
P_i = nilai desimal karakter plaintext ke- i

K_i = nilai desimal karakter kunci ke- i $26 =$ jumlah huruf dari abjad (a-z)

Metode Penelitian

A. Kerangka Penelitian

Penelitian ini menggunakan desain eksperimen kuasi-kontrol. Kelompok eksperimen akan menerima penerapan Kriptografi Vigenère Cipher pada kata sandi, sedangkan kelompok kontrol tidak akan mengalami perubahan pada sistem kata sandi. Pendekatan ini memungkinkan pengukuran dampak penerapan kriptografi terhadap kekuatan kata sandi di lingkungan aplikasi Puskesmas.



Gambar 1. Kerangka Penelitian

B. Uraian Kerangka Kerja Penelitian

1. Persiapan Awal

Analisis kelemahan keamanan kata sandi, evaluasi infrastruktur, dan kebutuhan implementasi Kriptografi Vigenere Cipher.

2. Pengumpulan Data

Penulis melakukan pengumpulan data untuk melakukan tinjauan literatur referensi terkait dengan kriptografi vigenere cipher berbasis web pada judul jurnal yang diangkat. Pengambilan data selama periode tertentu, mencakup perekaman log keamanan dan respons pengguna.

3. Perancangan sistem.

Pada tahap ini penulis merancang aplikasi puskesmas berbasis web ini dengan mengimplementasikan vigenere cipher dan menggunakan bahasa pemrograman PHP.

4. Implementasi Sistem

Tahap ini pengimplementasian program dan menjalankan aplikasi dengan melakukan proses enkripsi dan dekripsi pada kekuatan kata sandi di dalam aplikasi.

C. Ruang Lingkup

Fokus utama penelitian ini adalah pada sistem aplikasi Puskesmas yang digunakan untuk manajemen data pasien, resep obat, dan informasi kesehatan lainnya. Penelitian difokuskan pada keamanan kata sandi dalam sistem ini. Penelitian mencakup pengembangan dan implementasi Kriptografi Vigenere Cipher pada proses autentikasi kata sandi di dalam aplikasi Puskesmas. Ini mencakup perubahan pada sistem autentikasi yang ada.

D. Penerapan Vigenere Cipher pada kekuatan kata sandi di dalam sistem aplikasi puskesmas berbasis web

1. Analisis keamanan kata sandi yang ada

Sebelum implementasi, lakukan analisis menyeluruh terhadap keamanan kata sandi yang saat ini digunakan dalam aplikasi Puskesmas. Identifikasi kelemahan dan potensi risiko yang dapat dieksploitasi oleh pihak yang tidak berwenang

2. Integrasi algoritma kriptografi pada autentikasi kata sandi

Implementasikan algoritma Kriptografi Vigenere Cipher pada proses autentikasi kata sandi di dalam aplikasi Puskesmas. Pastikan bahwa setiap kata sandi yang disimpan atau dibaca melalui sistem mengalami proses enkripsi dan dekripsi menggunakan kunci yang sesuai.

3. Penyesuaian pengaturan kunci

Tentukan dan kelola pengaturan kunci dengan bijak. Kunci dalam Kriptografi Vigenere Cipher merupakan elemen kritis, sehingga pemilihan, penyimpanan, dan rotasi kunci harus diatur dengan cermat untuk meningkatkan keamanan

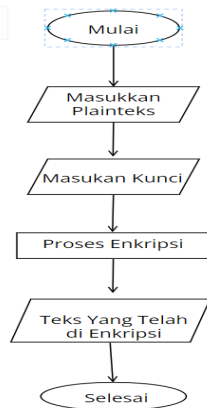
4. Uji coba dan validasi

Lakukan uji coba intensif terhadap implementasi Kriptografi Vigenere Cipher. Uji coba melibatkan verifikasi bahwa enkripsi dan dekripsi berfungsi dengan benar, serta mengevaluasi performa sistem setelah penerapan.

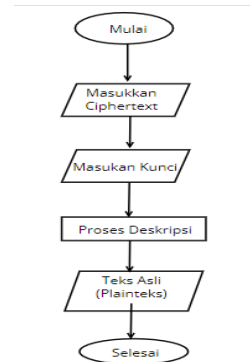
Hasil dan pembahasan

A. Perancangan Sistem

Berikut ini adalah flowchart proses enkripsi yang akan dibangun pada aplikasi menggunakan metode Vigenere Cipher.



Gambar 2. Flowchart Proses Enkripsi



Gambar 3. Flowchart Proses Dekripsi

Pada flowchart enkripsi diatas terdapat alur proses untuk mengenkripsi teks sehingga mendapatkan hasil teks yang telah terenkripsi. Sedangkan Pada flowchart dekripsi terdapat alur proses untuk mendeskripsikan teks yang telah di enkripsikan menjadi teks asli.

B. Implementasi Vigenere Cipher Sederhana

Dalam penerapan algoritma Vigenere Cipher diperlukan plainteks atau pesan yang akan dienkripsikan. Plainteks yang akan dilakukan dalam penyediaan ini adalah :

Plainteks : MOTOR

Key : VARIO

Plainteks	Urutan Alfabet	Key	Urutan Alfabet		Ciphertext
M	12	V	21	17	R
R	14	A	0	14	O
T	19	R	17	2	C
O	14	I	8	6	G
R	17	O	14	3	D

Tabel 1. Proses Enkripsi

Tabel diatas merupakan proses implementasi enkripsi pada teks MOTOR dan key VARIO, dan menghasilkan prosedur enkripsi tersebut menjadi teks ciphertext ROCGD.

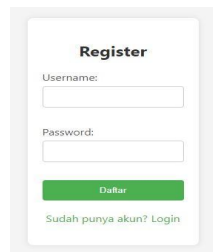
Ciphertext	Urutan Alfabet	Key	Urutan Alfabet		Plainteks
R	12	V	21	12	M
O	14	A	0	14	R
C	19	R	17	19	T
G	14	I	8	14	O
D	17	O	14	17	R

Tabel 2. Proses Deskripsi

Tabel diatas merupakan proses implementasi deskripsi pada teks ROCGD key VARIO, dan menghasilkan prosedur deskripsi tersebut menjadi teks asli yaitu MOTOR.

C. Implementasi ke dalam Sistem Aplikasi Puskesmas

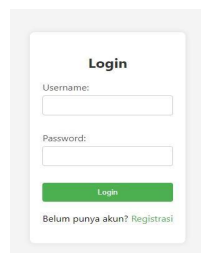
a. Registrasi Sistem



Gambar 4. Proses Registrasi

Pada proses register ini, pengguna diminta memasukkan username dan membuat password yang diinginkan, lalu proses enkripsi terjadi di dalam sistem, dan setelah pengguna memasukkan username dan password maka hasil registrasi pengguna yang tersimpan di dalam database menggunakan password yang telah terenkripsi.

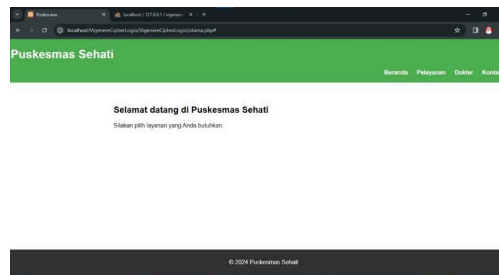
b. Login Sistem



Gambar 5. Proses Login

Pada proses login pun sama, disini proses deskripsi terjadi di dalam sistem. Jadi untuk password yang dimasukkan oleh pengguna di awal register dan telah terenkripsi di database diubah lagi ke dalam bentuk deskripsi. Hal ini terjadi karena penulis meletakann rumus enkripsi dan deskripsi di dalam sistem. Jadi yang harus dilakukan pengguna saat login adalah, memasukkan username dan passoword yang sama persis dengan saat register.

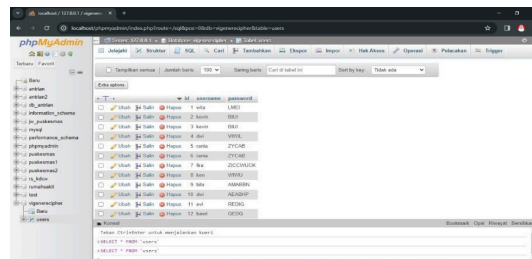
c. Halaman Dashboard



Gambar 6. Halaman Utama Sistem Aplikasi Puskesmas

Halaman ini adalah halaman utama yang muncul Ketika pengguna login ke dalam aplikasi puskesmas.

d. Database



Gambar 7. Database

Gambar diatas merupakan database sistem aplikasi puskesmas, jadi pada saat proses register sistem otomatis mengenkrip password yang dibuat oleh pengguna. Hal ini dilakukan sebagai bentuk pengamanan data pengguna apabila suatu saat terjadi kebocoran database, password yang ada di dalam database adalah bentuk password yang telah terenkripsi dan bukan bentuk password asli yang dibuat oleh pengguna.

Kesimpulan

Berdasarkan perolehan hasil studi dan desain aplikasi kriptografi menggunakan metode vigenere cipher terdapat kesimpulan pada penelitian ini yaitu aplikasi kriptografi ini bisa dipakai untuk menyandikan informasi atau data penting dengan mengubahnya menjadi kata sandi yang tidak bisa diketahui oleh individu yang tidak berwenang. Dan dengan melakukan proses dekripsi pada aplikasi kriptografi ini maka data atau teks bisa kembali ke teks asli yang bisa dibaca setelah dilakukan proses enkripsi.

Untuk peneliti lebih lanjut dari pemaparan mengenai perancangan aplikasi Kriptografi Vigenere Cipher sampai pada tahapan implementasi masih perlu dilakukan pengembangan sistem agar dapat menjadi aplikasi yang sempurna seperti menambahkan metode kriptografi lainnya sehingga lebih variatif serta memperindah tampilan agar lebih interaktif dan menarik.

Daftar Rujukan

[1] Maulana, D. K. ., Tanjung, S. M. ., Ritonga, R. S. ., & Ikhwan, A. . (2023). Penerapan Kriptografi Vigenere Cipher Pada Kekuatan Kata Sandi . Jurnal Sains Dan Teknologi (JSIT)

- [2] S. Aulansari, D. Sawitri, and A. Ikhwan, "APPLICATION OF VIGENERE CIPHER CRYPTOGRAPHY ON WEB-BASED TEXT MESSAGE DATA SECURITY", JINTEKS, vol. 4, no. 4, pp. 421-426, Nov. 2022.
- [3] Afandi, M. I., & Nurhayati, N. (2021). Implementasi Algoritma Vigenere Cipher Dan Atbash Cipher Untuk Keamanan Teks Pada Aplikasi Catatan Berbasis Android. *It (Informatic Technique) Journal*
- [4] S. Alasi and P. Fitriani, "Peningkatan Keamanan untuk Password menggunakan Algoritma Vigenere Cipher," *J. Mantik Penusa*, 2022, [Online].
- [5] B. H. Situmorang, S. Sinurat, and K. Tampubolon, "Implementasi Algoritma Atbash Untuk Menyandikan Pesan Teks Berbasis Android," *J. Pelita Inform.*, vol. 7, no. 2, pp. 157–161, 2018
- [6] Riski, A., Kamsyakawuni, A., & Arif, M. Z. (2018). IMPLEMENTASI VIGENERE CIPHER PADA PENGAMANAN DATA MEDIS. *Jurnal Riset Dan Aplikasi Matematika*, 02(01), 23–30.
- [7] Astuti, D., & Sundari, C. (2022). IMPLEMENTASI ALGORITMA VIGENERE CIPHER UNTUK ENKRIPSI DAN DEKRIPSI PADA PERESEPAN DATA OBAT DI PUSKESMAS MERTOYUDAN 1 KABUPATEN MAGELANG. *Jurnal Teknik Informasi Dan Komputer (Tekinkom)*, 5(2), 341–350. <https://doi.org/10.37600/tekinkom.v5i2.534>
- [8] Arrijal, I. M. (2016). Penerapan Algoritma Kriptografi Kunci Simetris Dengan Modifikasi Vigenere Cipher Dalam Aplikasi Kriptografi Teks. *E-Journal, Vol. 3*(No. 1).
- [9] Padede, A. M. H., Manurung, H., & Filina, D. (2017). Algoritma Vigenere Cipher Dan Hill Cipher Dalam Aplikasi Keamanan Data Pada File Dokumen. *E-Journal, Vol. 10*(No. 2).
- [10] E. S. Mulyani, I. W. Agustin, L. Herfiyanti, and ..., "Perancangan Sistem Informasi Kelengkapan Berkas Klaim BPJS IGD Menggunakan Visual Studio di Rumah Sakit Muhammadiyah Bandung," *JATISI (Jurnal Tek. ...)*, 2022, [Online]. Available: <https://jurnal.mdp.ac.id/index.php/jatisi/article/view/2167>
- [11] Y. T. Andita, H. Aspriyono, and ..., "Application of the Vigenere Cipher Algorithm in Database Security of Employee Performance Values at the South Bengkulu Regency Education and Culture Office," *J. Komput. ...*, 2022, [Online]. Available: <http://jurnal-unived.com/index.php/JK/article/view/40>
- [12] S. A. Zebua, "Modifikasi Algoritma Vigenere Cipher dengan Pembangkit Kunci Random Number Generator Dalam Pengamanan Citra Digital," *J. Comput. Informatics Res.*, 2022, [Online]. Available: <https://journal.fkpt.org/index.php/comforch/article/view/345>
- [13] Amin, M. M. (2016). IMPLEMENTASI KRIPTOGRAFI KLASIK PADA KOMUNIKASI BERBASIS TEKS. *Jurnal Pseudocode*, 3(2), 129–136.
- [14] Nurnawati, E. K. (2005). ANALISIS KRIPTOGRAFI MENGGUNAKAN ALGORITMA VIGENERE CIPHER DENGAN MODE OPERASI CIPHER BLOCK CHAINING(CBC). *Jurnal Teknologi Academia Ista*, 10, 121–127.
- [15] Gunadhi, E., & Sudrajat, A. (2016). PENGAMANAN DATA REKAM MEDIS PASIEN MENGGUNAKAN KRIPTOGRAFI VIGÈNERE CIPHER. *Jurnal Agoritma*, 13(2), 295–301. <http://jurnal.sttgarut.ac.id>