JINTEKS (Jurnal Informatika Teknologi dan Sains)
Vol. 4 No. 4, November 2022, hlm. 421 – 426

ISSN 2686-3359 (Online)

PENERAPAN KRIPTOGRAFI VIGENERE CIPHER PADA KEAMANAN DATA PESAN TEKS BERBASIS WEBSITE

Suwinda Aulansari[1], Diah Sawitri[2*], Ali Ikhwan[3]
[1,2,3]Prodi Sistem Informasi, Sains Dan Teknologi, UIN Sumatera Utara
email: dsawitrii30702@gmail.com

ABSTRAK: Penelitian ini bertujuan untuk menghasikan aplikasi kriptografi yang bisa digunakan untuk mengontrol keamanan data pesan teks dengan menggunakan metode Vigenere Cipher. Vigenere Cipher adalah salah satu teknik yang bisa dipakai untuk melakukan enkripsi pesan teks agar informasi tidak dapat ditukar atau dibobol oleh pihak yang tidak seharusnya menerima pesan tersebut. Saat ini keamanan merupakan bagian penting dari sebuah sistem informasi sehingga dibutuhkan sistem keamanan data agar informasi tidak jatuh ketangan yang salah. Penelitian ini memakai metode penelitian studi pustaka yang bersumber dari berbagai jurnal dan eksperimen dengan cara perancangan dan implementasi sistem. Hasil akhir penelitian ini yaitu menghasilkan sebuah aplikasi keamanan data melalui proses enkripsi dan dekripsi dengan mengimplementasikan algoritma vigenere cipher agar dapat memberikan keamanan lebih ketat pada pesan teks.

Kata Kunci: Kriptografi, Pesan Teks, Vigenere Cipher.

ABSTRACT: *This study aims to produce cryptographic applications that can be used to control the security of text message data using the Vigenere Cipher method. Vigenere Cipher is one of the techniques that can be apply to encrypt text messages so that information cannot be exchanged or breached by parties who should not receive the message. Currently, security is a crucial component of an information system so that a data security system is needed so that information doesn,t crash into the wrong hands. This research uses a literature study research method sourced from various journals and experiments by designing and implementing systems. The final outcome of this learn is to result a data security application through an encryption and decryption process by applying the vigenere cipher algorithm in order to provide tighter security on text messages.*

Keywords: *Cryptography, Text Messages, Vigenere Ciphers.*

PENDAHULUAN

Masalah keamanan ataupun privasi data adalah bagian yang sangat diperlukan pada suatu sistem informasi. Hal tersebut, berkaitan juga tentang seberapa pentingnya informasi yang akan disampaikan pada proses pengiriman dan penerimaan pesan oleh pihak tertentu. Apabila informasi pada saat pengiriman dibajak dan disalahgunakan oleh pihak yang tidak seharusnya menerima pesan tersebut maka informasi tersebut akan menjadi tidak berguna. Khususnya di bidang komunikasi, teknologi berkembang sangat cepat dan dengan berbagai fitur yang telah tersedia. Kerahasiaan informasi harus dilindungi selama pembagian informasi jarak jauh tersebut. Oleh karena itu, informasi tersebut dapat dilindungi dengan menerapkan kriptografi. Teknik vigenere cipher dapat diterapkan menjadi salah satu metode kriptografi untuk pengkodean atau penyandian teks.

Kriptografi juga disebut sebagai ilmu tentang metode ilmu hitung yang berkaitan dengan komponen pengamanan sebuah informasi termasuk privasi, kredibilitas data, dan autentikasi. Kriptografi di dalam bidang studi sudah ada sejak lama. Julius Caesar, seorang penguasa Romawi, diketahui telah memakai pengkodean untuk mengirim sinyal rahasia sepanjang konflik.

Sebenarnya, enkripsi sandi Vigenere adalah suatu pengembangan dari Caesar Cipher. Masing-masing huruf dalam teks akan diubah dalam sandi Caesar menjadi huruf dengan penempatan abjad yang sedikit berbeda. Contohnya, pada sandi Caesar menggunakan tiga slide, A berubah menjadi D, B menjadi E, dan begitupun selanjutnya. Sandi Caesar yang digunakan dalam sandi Vigenere masing-masing memiliki nilai geser yang unik.

Berdasarkan pemaparan di atas, kami ingin mengimplementasikan sandi Vigenere dengan merancang sebuah sistem pembelajaran serta mengaplikasikan sandi Vigenere. Maka dari itu, kami mengangkat penelitian yang berjudul "Penerapan Kriptografi Vigenere Cipher pada Keamanan Data Teks Berbasis Web".

Penelitian terdahulu juga telah dilakukan yang berjudul "Implementasi Kriptografi Vigenere Cipher Dengan PHP". Penelitian tersebut dilaksanakan untuk mempraktekkan kriptografi Vigenere cipher. Desain sistem menggunakan teknik kooperatif dan deskriptif. Sistem kriptografi cipher Vigenere kemudian dibangun dengan pemodelan UML, analisis, dan deskripsi teks yang dapat diprogram memanfaatkan perangkat lunak PHP. Penelitian ini mengarah pada penggunaan PHP untuk mengimplementasikan sistem enkripsi cipher Vigenere[1].

ISSN 2686-3359 (Online)

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 [2]. Untuk mencegah pihak lain mengetahui informasi yang terkandung pada data, kriptografi bekerja untuk menjamin kerahasiaannya [3]. Enkripsi digunakan untuk mengkonversikan informasi atau data menjadi versi baru yang aman dan nyaris tidak bisa diidentifikasi sebagai informasi asli [4]. Ada dua prosedur dalam ilmu kriptografi yaitu enkripsi dan dekripsi [5]. 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 [6].

Blaise de Vigenere ialah seorang diplomat dan ahli kriptologi Prancis, pertama kali memperkenalkan sandi vigenere pada abad ke-16[7]. Kata kunci (key) akan digunakan untuk menyandikan data menggunakan teknik enkripsi kata sandi Vigenere [8]. Vigenere cipher memiliki keunggulan dibandingkan caesar cipher karena tahan terhadap teknik decoding yang dikenal sebagai frekuensi analisis [9]. Setiap huruf pada teks ringan diganti dengan huruf baru yang berbeda urutan yang diberikan [10].

Vigenere memiliki kunci yang mempunyai panjang tidak tentu. Panjang kunci dari vigenere cipher bisa lebih, kurang, atau sama dengan panjang plainteksnya. Kunci akan diulang jika panjangnya tidak sama dengan plainteks.

Rumus untuk enkripsi pada vigenere :

$$C_i = (P_i + K_i) \; mod \; 26 \qquad (1)$$

Rumus untuk dekripsi pada vigenere :

$$P_i = (C_i - K_i) \; mod \; 26 \qquad (2)$$

Keterangan :

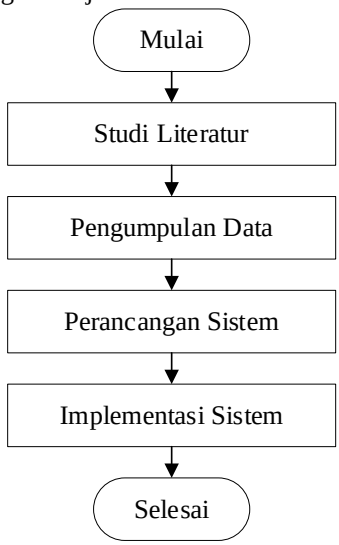
C_i = angka decimal dalam ciphertext ke-i
P_i = angka decimal dalam plaintext ke-i
K_i = angka decimal pada key ke-i
26 = jumlah huruf dari abjad (a-z)

Rasmus Lerdrorf menemukan PHP pertama kali pada tahun 1994. Untuk menandai blok skrip PHP, ada empat pasangan tag PHP berbeda yang dapat digunakan [11]. Bahasa pemrograman dinamis dibuat menggunakan program PHP [12]. Di antara bahasa HTML, PHP dapat disisipkan [13]. Penggunaan PHP membuat Web menjadi dinamis, membuatnya lebih sederhana dan efektif untuk memelihara situs web. PHP gratis untuk diunduh dari situs resminya dan merupakan perangkat lunak sumber terbuka yang disediakan dan dilisensikan tanpa biaya[14].

Program yang dikenal sebagai browser digunakan untuk mengakses web, aplikasi yang berisi dokumen multimedia [15]. Sebuah website terdiri dari sejumlah halaman web yang bisa diakses melalui World Wide Web (WWW) di Internet [16]. Dengan mengklik tautan dalam dokumen web yang terlihat di browser web, pengguna dapat menemukan informasi [17]. File-file di situs web terhubung melalui serangkaian halaman web yang terhubung [18]. Siapapun kini dapat memberikan informasi dengan menggunakan teknologi berkat web [19]. Dokumen informasi situs web dihubungkan bersama menggunakan URL (*Uniform Resource Locators*)[[20].

METODE PENELITIAN

A. Kerangka Kerja Penelitian



Gambar 1. Kerangka kerja Penelitian

B. Uraian Kerangka Kerja

Kerangka dalam studi ini dijabarkan melalui penjelasan dibawah ini:

1. Studi literatur

Tahap pertama dalam penelitian merupakan proses untuk melakukan tinjauan literatur referensi mengenai algoritma Vigenere Cipher dan hipotesis pendukung lainnya.

2. Pengumpulan data

Penulis melakukan pengumpulan data melalui jurnal yang terkait dengan Kriptografi

 ISSN 2686-3359 (Online)

Vigenere Cipher berbasis web dan yang terkait terhadap judul yang diangkat oleh penulis.

3. Perancangan Sistem

Pada tahap ini aplikasi Kriptografi Vigenere Cipher dirancang dengan mengimplementasikan bahasa pemrograman PHP.

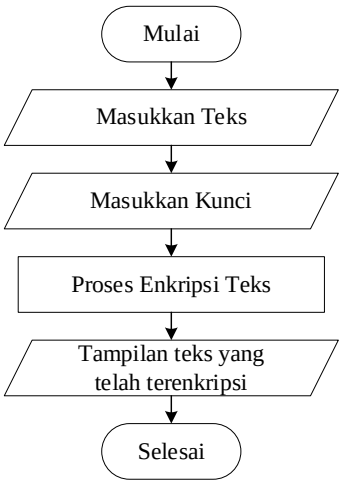
4. Implementasi Sistem

Tahap ini pengimplementasian dari program dilaksanakan dengan cara menjalankan aplikasi dan melakukan proses enkripsi dan deskripsi pada teks.

HASIL DAN PEMBAHASAN

A. Perancangan Sistem

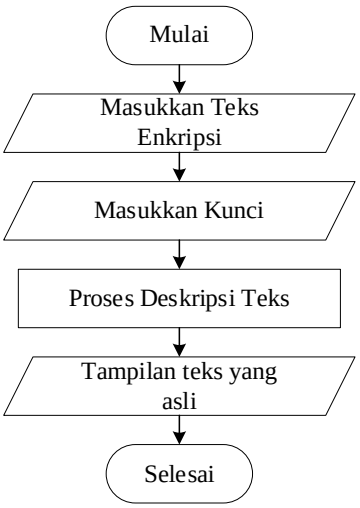
Berikut ini adalah flowchart proses enkripsi yang akan dibangun pada aplikasi menggunakan metode Vigenere Cipher.



Gambar 2. Flowchart Proses Enkripsi

Pada flowchart enkripsi terdapat alur proses untuk mengenkripsi teks sehingga mendapatkan hasil teks yang telah terenkripsi.

Berikut ini adalah flowchart alur deskripsi teks:



Gambar 3. Flowchart Proses Deskripsi

Pada flowchart dekripsi terdapat alur proses untuk mendeskripsikan teks yang telah di enkripsikan menjadi teks asli.

B. Implementasi

Dalam penerapan algoritma Vigenere Cipher diperlukan plainteks atau pesan yang akan dienkripsikan. Plainteks yang akan dilakukan penyandian adalah PESAN INI SANGAT RAHASIA dengan key ARMADA.

Plainteks = PESAN INI SANGAT RAHASIA

Key = ARMADA

Tabel 1. Proses Enkripsi

Plainteks	Urutan Alfabet	Key	Urutan Alfabet		Ciphertext
P	15	A	0	15	P
E	4	R	17	21	V
S	18	M	12	30	E
A	0	A	0	0	A
N	13	D	3	16	Q
I	8	A	0	8	I
N	13	A	0	13	N
I	8	R	17	25	Z
S	18	M	12	30	E
A	0	A	0	0	A
N	13	D	3	16	Q
G	6	A	0	6	G
A	0	A	0	0	A
T	13	R	17	36	K
R	17	M	12	29	D
A	0	A	0	0	A
H	7	D	3	10	K
A	0	A	0	0	A
S	18	A	0	18	S

 ISSN 2686-3359 (Online)

I	8	R	17	25	Z
A	0	M	12	12	M

Tabel diatas merupakan tabel prosedur enkripsi pesan teks PESAN INI SANGAT RAHASIA dan key ARMADA. Hasil dari prosedur enkripsi tersebut yaitu PVEAQ INZ EAQGAK DAKASZM.

Prosedur Dekripsi:

Rumus : $P_i = (C_i - K_i) \; mod \; 26$ (3)

C : Ciphertext

K : Kunci

Tabel 2. Proses Deskripsi

Ciphertext	Urutan Alfabet	Key	Urutan Alfabet		Plainteks
P	15	A	0	15	P
V	4	R	17	4	E
E	18	M	12	18	S
A	0	A	0	0	A
Q	13	D	3	13	N
I	8	A	0	8	I
N	13	A	0	13	N
Z	8	R	17	8	I
E	18	M	12	18	S
A	0	A	0	0	A
Q	13	D	3	13	N
G	6	A	0	6	G
A	0	A	0	0	A
K	13	R	17	13	T
D	17	M	12	17	R
A	0	A	0	0	A
K	7	D	3	7	H
A	0	A	0	0	A
S	18	A	0	18	S
Z	8	R	17	8	I
M	0	M	12	0	A

Tabel diatas merupakan tabel prosedur enkripsi pesan teks PVEAQ INZ EAQGAK DAKASZM dengan kunci ARMADA. Hasil dari prosedur enkripsi tersebut yaitu PESAN INI SANGAT RAHASIA.

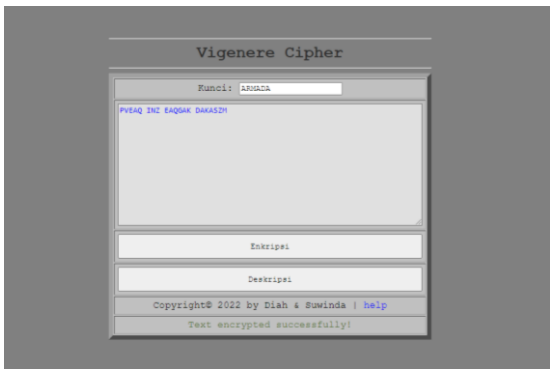
a. Halaman Utama

Halaman ini ialah tampilan utama yang muncul didalam program. Gambar 4 dibawah ini menunjukkan tampilan dari halaman utama pada aplikasi kriptografi Vigenere cipher.

Gambar 4. Tampilan Halaman Utama

b. Halaman Enkripsi

Halaman tersebut merupakan tampilan halaman yang digunakan saat proses enkripsi. Kita harus memasukkan plaintext dan key di halaman ini. Gambar 5 di bawah ini menunjukkan bagaimana prosedur enkripsi bekerja.

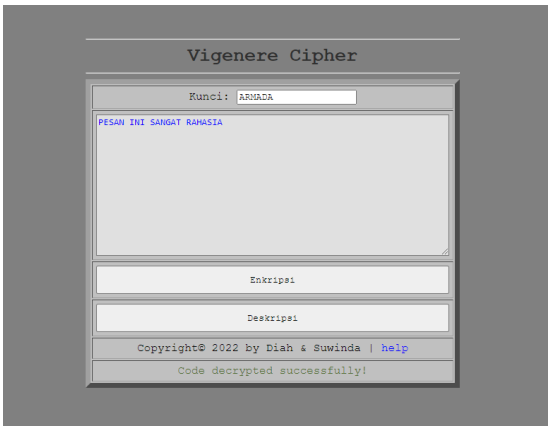


Gambar 5. Tampilan Proses Enkripsi

c. Halaman Dekripsi

Halaman ini berfungsi sebagai halaman tampilan untuk prosedur deskripsi. Kita harus memasukkan ciphertext dan key di halaman ini. Gambar 6 di bawah ini merupakan tampilan pada prosedur deskripsi.

 ISSN 2686-3359 (Online)



Gambar 6. Tampilan Proses Deskripsi

KESIMPULAN DAN SARAN

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 PUSTAKA

[1] 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.

[2] M. I. Afandi and N. Nurhayati, "Implementasi Algoritma Vigenere Cipher Dan Atbash Cipher Untuk Keamanan Teks Pada Aplikasi Catatan Berbasis Android," *It (Informatic Tech. J.*, vol. 8, no. 1, p. 30, 2021, doi: 10.22303/it.8.1.2020.30-41.

[3] 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.

[4] A. A. Permana, "Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode Vigenere Cipher Berbasis Android," *J. Al-AZHAR Indones. SERI SAINS DAN Teknol.*, vol. 4, no. 3, p. 110, 2018, doi: 10.36722/sst.v4i3.280.

[5] V. S. Ginting, "Penerapan Algoritma Vigenere Cipher dan Hill Cipher Menggunakan Satuan Massa," *J. Teknol. Inf.*, vol. 4, no. 2, pp. 241–246, 2020, doi: 10.36294/jurti.v4i2.1365.

[6] A. Z. Hasibuan, M. S. Asih, and H. Harahap, "Penerapan QR Code dan Vigenere Cipher Dalam Sistem Pelaporan Juru Parkir Ilegal," *Query J. Sist. Inf.*, vol. 3, no. 1, pp. 2579–5341, 2019.

[7] L. D. Simatupang and K. Khairil, "Pengamanan Dokumen Teks Dengan Menerapkan Kombinasi Algoritma Kriptografi Klasik," *J. Tek. Inform. UNIKA St. Thomas*, vol. 07, pp. 133–140, 2022, doi: 10.54367/jtiust.v7i1.1998.

[8] G. B. Minarto and M. Q. Khairuzzaman, "Penerapan Kriptografi Menggunakan Caesar Cipher Dan Vigenere Cipher," *Enter*, vol. 1, pp. 1–12, 2018, [Online]. Available: http://www.sisfotenika.stmikpontianak.ac.id/index.php/enter/article/view/787.

[9] A. Junikhah, "Implementasi Vigenere Cipher Pada Aplikasi Myprichat End-To-End Encrypted Sms Berbasis Android," *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 7, no. 3, pp. 680–691, 2022, doi: 10.29100/jipi.v7i3.3012.

[10] N. Laila and A. S. R. Sinaga, "Implementasi Steganografi LSB Dengan Enkripsi Vigenere Cipher Pada Citra," *Sci. Comput. Sci. Informatics J.*, vol. 1, no. 2, p. 47, 2019, doi: 10.22487/j26204118.2018.v1.i2.11221.

[11] M. Suhartanto, "Kata kunci : Pembuatan Website Sekolah, PHP, 1.1," *J. Speed-Sentra Penelit. Enginerring dan Edukasi*, vol. 4, no. 1, pp. 1–8, 2012.

[12] Sardiarinto, "Aplikasi Sms Gateway Untuk Keamanan Sistem Informasi Berbasis Web," *Bianglala Inform.*, vol. II, no. 1, pp. 1–10, 2014, [Online]. Available: http://ejournal.bsi.ac.id/jurnal/index.php/Bianglala/article/view/556/448.

[13] T. Wahyuni and M. T. Susanto, "Perancangan Website Periklanan Dengan Fasilitas Reviewer Iklan Menggunakan Php Dan Mysql," *INFOTECH J.*, vol. 4, no. 2, pp. 1–5, 2018, [Online]. Available:

 ISSN 2686-3359 (Online)

https://jurnal.unma.ac.id/index.php/infotech/article/view/907/844.

[14] Kurniawan and Ropianto, "Perancangan Sistem Informasi Berbasis Website Dengan PHP dan SQL Sekolah Nurul Yaqin," *Academia.Edu*, pp. 1–21, 2020.

[15] Ismai, "Perancangan Website Sebagai Media Promosi Dan Informasi," *J. Inform. Pelita Nusant.*, vol. 3, no. 1, pp. 82–86, 2018.

[16] Y. Trimarsiah and M. Arafat, "Analisis dan Perancangan Website Sebagai Sarana," *J. Ilm. MATRIK*, vol. Vol. 19 No, pp. 1–10, 2017.

[17] Z. K. Mudztaba, "(Ppdb) Di Ra Nurul Hijrah Berbasis Website," *IKRA-ITH Inform. J. Komput. dan Inform.*, vol. 6, no. 1, pp. 109–124, 2022.

[18] A. Y. Molan, "Perancangan Sistem Informasi Akuntansi Penjualan Kredit Dan Penerimaan Kas Berbasis Web," *Inf. Technol. Control Audit*, vol. 1, no. 3, pp. 14–24, 2021.

[19] I. Kanedi, Yupianti, and F. Hari Utami, "Media Sarana Promosi Makanan Khas Bengkulu Berbasis Website Menggunakan Script Php," *J. Media Infotama*, vol. 9, no. 2, pp. 206–225, 2013, [Online]. Available: http://jurnal.unived.ac.id/index.php/jmi/article/viewFile/71/63.

[20] E. Gunadhi and A. P. Nugraha, "Penerapan Kriptografi Base64 Untuk Keamanan URL (Uniform Resource Locator) Website Dari Serangan SQL Injection," *J. Algoritm.*, vol. 13, no. 2, pp. 391–398, 2017, doi: 10.33364/algoritma/v.13-2.391.