

Implementasi vigenere cipher dalam keamanan email untuk keamanan pada pesan teks

Implementation of Vigenere cipher in email security for security in text messages

Nafal Mumtaz¹, Daffa Gibran², Wahyu Firhansyah³, Hamim Muhana⁴

¹Informatika, Teknik, Universitas Pelita Bangsa

²Informatika, Teknik, Universitas Pelita Bangsa

³Informatika, Teknik, Universitas Pelita Bangsa

⁴Informatika, Teknik, Universitas Pelita Bangsa

¹nafalmumtaz93@gmail.com, ²daffa3966@gmail.com,

³wahyu21@mhs.pelitabangsa.ac.id, ⁴hamim.man@gmail.com

Abstract

In the current digital era, information security is becoming increasingly crucial. Email, as one of the most commonly used forms of digital communication, often contains confidential or sensitive information. Therefore, email security is of utmost importance to safeguard the confidentiality of text messages. One technique that can be employed to enhance email security is the Vigenère Cipher, a classical encryption method that has been utilized for centuries. This research discusses the implementation of the Vigenère Cipher in the context of email security with the goal of protecting text messages. In the current digital era where sensitive information is frequently transmitted via email, email security is becoming more critical. The Vigenère Cipher, as a classical encryption method, is utilized in this study to enhance email security by encrypting text before it is sent via email. The study also explores the challenges and benefits of using the Vigenère Cipher in the realm of email security. By applying the Vigenère Cipher in email security, this research aims to contribute to a practical understanding of the implementation of classical encryption techniques in the modern digital communication environment.

Keywords: Vigenère Cipher, email security, text message encryption, communication confidentiality, information security.

Abstrak

Keamanan email dan pesan teks menjadi perhatian utama dalam konteks komunikasi digital. Salah satu metode yang digunakan untuk meningkatkan keamanan dalam hal ini adalah Vigenère Cipher. Penelitian ini bertujuan untuk mengeksplorasi implementasi Vigenère Cipher dalam konteks keamanan email untuk melindungi pesan teks. Dengan memanfaatkan metode ini, diharapkan dapat memberikan kontribusi dalam pemahaman praktis tentang penerapan teknik enkripsi klasik dalam lingkungan komunikasi digital yang modern. Beberapa penelitian telah berhasil membangun aplikasi berbasis web dan Android yang menggunakan Vigenère Cipher untuk mengamankan data yang dikirimkan melalui email dan aplikasi pesan. Temuan dari penelitian ini diharapkan dapat memberikan panduan berharga bagi profesional keamanan informasi dan peneliti yang tertarik dalam mengamankan komunikasi melalui email.

Dalam konteks komunikasi digital, keamanan email dan pesan teks menjadi perhatian utama. Salah satu cara untuk meningkatkan keamanan adalah menggunakan metode enkripsi klasik, seperti Vigenère Cipher. Penelitian ini bertujuan untuk mengeksplorasi penerapan Vigenère Cipher dalam konteks keamanan email untuk melindungi pesan teks. Dengan memanfaatkan metode ini, diharapkan dapat memberikan kontribusi dalam pemahaman praktis tentang penerapan teknik enkripsi klasik dalam lingkungan komunikasi digital yang modern. Beberapa penelitian telah berhasil membangun aplikasi berbasis web dan Android yang menggunakan Vigenère Cipher untuk mengamankan data yang dikirimkan melalui email dan aplikasi pesan. Temuan dari penelitian ini diharapkan dapat memberikan panduan berharga bagi profesional keamanan informasi dan peneliti yang tertarik dalam mengamankan komunikasi melalui email.

Kata kunci: Vigenère Cipher, keamanan email, enkripsi pesan teks, kerahasiaan komunikasi, keamanan informasi.

Pendahuluan

Dalam era berkembangnya teknologi digital, perlindungan keamanan informasi menjadi hal yang sangat penting, terutama ketika berbicara tentang pertukaran pesan melalui email. Keamanan pesan teks menjadi prioritas utama untuk mencegah akses yang tidak sah dan menjaga kerahasiaan komunikasi. Dalam konteks ini, penerapan algoritma kriptografi seperti Vigenere Cipher dapat dianggap sebagai langkah kritis dalam memperkuat keamanan email.

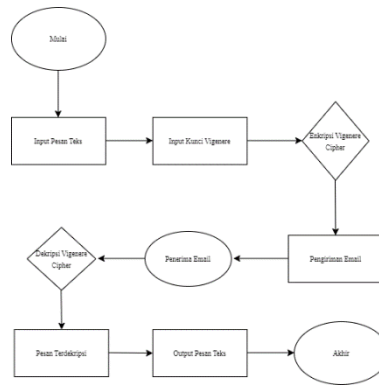
Vigenere Cipher, sebuah metode enkripsi klasik yang menggunakan pola kunci untuk melindungi pesan, telah menjadi opsi yang relevan dalam menjaga kerahasiaan pesan teks. Keunggulan dari Vigenere Cipher terletak pada kemampuannya untuk memberikan lapisan keamanan tambahan melalui penggunaan kunci yang dapat diubah secara dinamis. Dengan demikian, metode ini dapat memberikan perlindungan yang efektif terhadap ancaman keamanan terhadap pesan teks tanpa mengorbankan efisiensi dalam pertukaran informasi.

Dalam konteks penggunaan Vigenere Cipher untuk keamanan email, implementasi yang cermat akan memainkan peran penting dalam memastikan bahwa setiap pesan yang dikirim dan diterima dapat dienkripsi dan didekripsi dengan aman. Tindakan perlindungan ini menjadi sangat penting mengingat adanya serangan siber yang semakin meningkat dan upaya peretasan terhadap komunikasi online.

Penelitian ini bertujuan untuk mengeksplorasi penerapan Vigenere Cipher sebagai solusi untuk meningkatkan keamanan pesan teks pada platform email, dengan melakukan analisis mendalam terhadap kelebihan dan kelemahan algoritma ini. Diharapkan hasilnya dapat menghasilkan rekomendasi praktis untuk meningkatkan keamanan dan privasi dalam pertukaran pesan elektronik. Implementasi Vigenere Cipher pada keamanan email tidak hanya akan meningkatkan keamanan pesan teks, tetapi juga memberikan kontribusi positif terhadap upaya menjaga integritas dan kerahasiaan informasi dalam lingkungan digital yang penuh tantangan ini.

Metode Penelitian

Penelitian ini memiliki tujuan utama untuk menerapkan Vigenere Cipher dalam konteks keamanan email dengan fokus pada melindungi pesan teks. Melalui telaah literatur, kami akan mengeksplorasi kelebihan dan kelemahan Vigenere Cipher, sekaligus mengidentifikasi potensi risiko keamanan yang mungkin muncul dalam penggunaannya pada email. Selanjutnya, perancangan dan implementasi sistem akan dilakukan, yang mencakup integrasi Vigenere Cipher ke dalam alur keamanan email dan penyesuaian aturan enkripsi serta dekripsinya. Uji keamanan akan dilaksanakan untuk menilai sejauh mana Vigenere Cipher mampu melawan serangan, termasuk brute force atau analisis frekuensi. Selain itu, kinerja sistem akan dievaluasi dengan dan tanpa Vigenere Cipher, dengan perhatian khusus terhadap potensi overhead selama proses enkripsi dan dekripsi. Hasil analisis akan digunakan untuk mendalami efektivitas dan efisiensi penggunaan Vigenere Cipher dalam konteks keamanan email. Dalam konteks perbandingan, kami juga akan membandingkan hasil dengan metode enkripsi lain yang umum digunakan, dengan menguraikan kelebihan dan kekurangannya masing-masing. Harapannya, penelitian ini akan memberikan kontribusi yang signifikan dalam pemahaman praktis terkait penerapan Vigenere Cipher untuk meningkatkan keamanan email khususnya dalam melindungi pesan teks.



Gambar 1 Flowchart

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Gambar 2 Tabel Vegenere Cipher

Metode penelitian menjelaskan desain penelitian, rancangan kegiatan, ruang lingkup atau objek penelitian, tempat penelitian, teknik pengumpulan data, dan teknik analisis penelitian. **Hindari menulis konsep keilmuan yang sudah umum, tinjauan pustakan dan definisi-definisi umum.**

Hasil dan Pembahasan

Fungsi generateKey: Fungsi ini digunakan untuk menghasilkan kunci yang digunakan untuk enkripsi dan dekripsi. Jika panjang kunci sama dengan panjang pesan, maka kunci tersebut digunakan secara langsung. Jika tidak, kuncinya akan diulang secara dinamis. Diskusi: Pendekatan ini memastikan bahwa panjang kunci Vigenere cocok dengan panjang pesan. fungsi enkripsi: Fungsi ini mengenkripsi pesan menggunakan enkripsi Vigenere Cipher. Pembahasan: Enkripsi dilakukan dengan mengubah karakter pesan sesuai dengan karakter kunci yang bersangkutan. Fungsi ctype_alpha digunakan untuk memastikan bahwa hanya karakter alfabet yang dikodekan. Fungsi dekripsi: Fungsi ini mendekripsi pesan terenkripsi menggunakan Vigenere Cipher. Pembahasan: Dekripsi dilakukan dengan mengubah karakter terenkripsi sesuai dengan karakter kunci yang bersangkutan. Seperti halnya fungsi enkripsi, ctype_alpha digunakan untuk karakter alfabet. Penanganan formulir: Formulir HTML mengumpulkan informasi seperti email pengirim, penerima, subjek, pesan, dan kunci. Informasi ini digunakan untuk mengenkripsi pesan, menyimpan informasi dalam database, dan menampilkan pesan terenkripsi dan terenkripsi. Diskusi: Data sensitif seperti kunci tidak boleh disimpan di klien dan harus dilindungi oleh praktik keamanan yang baik. Koneksi ke database: Menggunakan koneksi MySQL untuk menyimpan data dalam database. Diskusi: Kebutuhan untuk memastikan bahwa koneksi ke database aman dan terlindungi dari serangan injeksi SQL. Tampilan HTML: Formulir HTML disertakan untuk menerima masukan pengguna. Menampilkan pesan terenkripsi dan terenkripsi saat pengguna mengirimkan formulir. Diskusi: Antarmuka yang sederhana dan bersih, namun Anda perlu memperhatikan keamanan klien, seperti validasi input. Gaya CSS: Gunakan CSS untuk menambah gaya dan membuat

bentuknya lebih menarik. Diskusi: Menggunakan CSS meningkatkan pengalaman pengguna. Ikon email: Ikon email telah ditambahkan ke formulir. Diskusi: Menambahkan elemen visual dapat memperkaya layar dan membantu pengguna memahami cara kerja formulir.

	Keterangan
id	Kolom "id" secara otomatis meningkat nilainya dan dijadikan sebagai kunci utama.
timestamp	Kolom yang mencatat waktu untuk menandai kapan pesan telah dikirim.
sender_email	Kolom yang digunakan untuk menyimpan alamat email pengirim.
recipient_email	Kolom yang digunakan untuk menyimpan alamat email penerima.
subject	Kolom yang digunakan untuk menyimpan subjek dari pesan email.
message	Kolom yang digunakan untuk menyimpan teks asli dari pesan.
key_used	Kolom yang digunakan untuk menyimpan kunci yang digunakan dalam proses enkripsi dan dekripsi.
encrypted_message	Kolom yang digunakan untuk menyimpan teks pesan yang telah dienkripsi.
decrypted_message	Kolom yang digunakan untuk menyimpan teks pesan yang telah didekripsi.

Tabel 1 enkripsi pengamanan pengiriman pesan teks pada keamanan email

Gambar ini menggambarkan sebuah formulir email yang ada di aplikasi atau website. Formulir tersebut dilengkapi dengan bidang untuk memasukkan 'Email Pengirim', 'Email Penerima', 'Subjek', dan 'Pesan'. Terdapat juga bidang 'Kunci' yang kemungkinan digunakan dalam proses enkripsi dan dekripsi. Kehadiran tombol 'Enkripsi & Dekripsi' menandakan bahwa aplikasi atau website ini menawarkan fitur untuk melakukan enkripsi dan dekripsi pesan.

Gambar 3 Tabel Vegenera Cipher

Hasil pengujian dari penelitian ini dapat dipaparkan sebagai berikut:

No	Enkripsi	Deskripsi	Keterangan
1	Pesan : Ayo kerjakan tugas Kunci : Siaplaksanakan Hasil : Sgo vebbaxax gmoah	Pesan Enkrip : Sgo vebbaxax gmoah Kunci : Siaplaksanakan Pesan : Ayo kerjakan tugas	sesuai

2	Pesan :	Pesan Enkrip :	sesuai
	Kerjain bareng ayo	nycdavn bdlphg aho	
	Kunci:	Kunci:	
	Duluanaja	Duluanaja	
	Hasil:	Pesan :	
	nycdavn bdlphg aho	Kerjain bareng ayo	

Tabel 1 pengujian dari penelitian

Kesimpulan

Menerapkan enkripsi Vigenere untuk keamanan email Anda merupakan langkah efektif untuk meningkatkan keamanan pesan teks Anda. Cipher Vigenere adalah metode enkripsi klasik yang menggunakan tabel rektor tabular untuk menggabungkan teks asli dengan kunci, sehingga menghasilkan teks sandi yang sulit diuraikan tanpa kunci yang sesuai. Dari perspektif keamanan email, Vigenere Cipher menawarkan manfaat melindungi pesan teks dari akses tidak sah. Kunci enkripsi yang digunakan dikelola dengan baik dan disepakati antara pihak-pihak yang terlibat dalam komunikasi. Peningkatan keamanan pesan teks: Vigenere Cipher memberikan lapisan keamanan tambahan untuk pesan teks di email menggunakan kunci enkripsi yang dapat dikonfigurasi sesuai kebutuhan, Perlindungan terhadap pencurian informasi: Enkripsi Vigenere Cipher mencegah pihak yang tidak berkepentingan mencuri informasi sensitif dalam email karena pesan tidak dapat didekripsi dengan mudah tanpa kunci yang benar, Fleksibilitas Kunci: Penerapan enkripsi Vigenere memungkinkan penggunaan kunci yang berbeda untuk setiap sesi pesan atau komunikasi, sehingga meningkatkan fleksibilitas dan tingkat keamanan, Pertukaran Kunci Aman: Memungkinkan pengguna menukar kunci enkripsi dengan aman menggunakan saluran lain atau metode keamanan tambahan, tanpa risiko kunci dicegat oleh pihak yang tidak berwenang, Pentingnya Manajemen Kunci: Keamanan enkripsi Vigenere sangat bergantung pada manajemen kunci yang tepat. Oleh karena itu, penting untuk menjaga kerahasiaan kunci dan menggantinya secara berkala untuk meminimalkan risiko keamanan. Menerapkan Vigenere Cipher untuk keamanan email memungkinkan pengguna meningkatkan kerahasiaan dan integritas pesan teks mereka, menjadikannya pilihan yang baik untuk melindungi komunikasi email dari ancaman keamanan.

Ucapan Terima Kasih

Kami ingin mengungkapkan rasa terima kasih sebesar-besarnya kepada semua pihak yang turut serta dalam memberikan dukungan dan kontribusi pada penelitian ini. Keberhasilan yang kami capai tidak lepas dari sinergi dan bantuan berharga yang telah diberikan.

Terima kasih kepada seluruh anggota tim penelitian yang telah menunjukkan dedikasi dan kerja keras, kepada para pemberi dana yang telah memberikan dukungan finansial yang sangat diperlukan, serta kepada semua individu yang telah berkontribusi dengan wawasan dan masukan berarti. Peran masing-masing dari Anda telah menjadi pilar utama dalam pencapaian hasil positif ini.

Tak lupa, terima kasih kepada keluarga dan teman-teman yang telah memberikan dukungan moral dan semangat selama proses penelitian. Keberhasilan ini tidak hanya milik kami sebagai peneliti, tetapi juga milik semua yang turut serta dalam memberikan dukungan.

Semoga hasil penelitian ini dapat memberikan manfaat yang signifikan dan memberikan kontribusi positif pada pengembangan ilmu pengetahuan. Sekali lagi, terima kasih atas dedikasi dan kerjasama yang luar biasa.

Hormat kami,

Daftar Rujukan

- [1] Imam Riadi, Abdul Fadlil, and Fahmi Auliya Tsani, "Pengamanan Citra Digital Berbasis Kriptografi Menggunakan Algoritma Vigenere Cipher," *JISKA (Jurnal Informatika Sunan Kalijaga)*, vol. 7, no. 1, pp. 33–45, 2022, doi: 10.14421/jiska.2022.7.1.33-45.
- [2] A. Junikhah, "Implementasi Vigenere Cipher Pada Aplikasi Myprichat End-To-End Encrypted Sms Berbasis Android," *JUPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 7, no. 3, pp. 680–691, 2022, doi: 10.29100/jipi.v7i3.3012.
- [3] A. Arfriandi, "Pengamanan Teks Pada Dokumen Email Menggunakan Enkripsi Rotor," *Edu Komputika Journal*, vol. 5, no. 1, pp. 23–32, 2018.
- [4] Marchandi and Ferdiansyah, "Implementasi Algoritma Vigenere Cipher Dalam Aplikasi Chatting Untuk Pengamanan Informasi Berbasis Desktop," *Skamika*, vol. 1, no. 1, pp. 340–345, 2018.
- [5] I. Murni, A. S. Br pa, B. R. Lubis, and A. Ikhwan, "Pengamanan Pesan Rahasia dengan Algoritma Vigenere Cipher Menggunakan PHP," *Journal on Education*, vol. 5, no. 2, pp. 3466–3476, 2023, doi: 10.31004/joe.v5i2.1027.
- [6] E. Irianti, D. F. Surianto, Ainun Zahra Adistia, Muh. Juharman, and Jumadil Ahmad Safi'i, "Implementasi Kriptografi Vigenere Cipher untuk Keamanan Data Informasi Desa," *Progressive Information, Security, Computer, and Embedded System*, vol. 1, no. 1, pp. 8–15, 2023, doi: 10.61255/pisces.v1i1.24.
- [7] M. Rivaldi, I. Z. Harahap, H. Isdianto, and R. A. Putri, "Implementasi Algoritma Kriptografi Vigenere Cipher Pada Pengamanan Pesan Text Berbasis Web," *Positif: Jurnal Sistem dan Teknologi Informasi*, 2023.
- [8] N. B. Putra, B. C. Andika, A. D. P. Bagas, and M. Ridwan, "Implementasi Sandi Vigenere Cipher Dalam," vol. 1, no. 1, pp. 42–50, 2023.
- [9] A. A. Permana, "Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode Vigenere Cipher Berbasis Android," *JURNAL AL-AZHAR INDONESIA SERI SAINS DAN TEKNOLOGI*, vol. 4, no. 3, p. 110, 2018, doi: 10.36722/sst.v4i3.280.
- [10] A. Rachmadsyah, A. Perdana, and A. Budiman, "Kombinasi Algoritma Beaufort Cipher dan Vigenere Cipher untuk Pengamanan Pesan Teks Berbasis Mobile Application," *Jurnal Minfo Polgan*, vol. 9, no. 2, pp. 12–17, 2020.
- [11] S. Aulansari, D. Sawitri, and A. Ikhwan, "Penerapan Kriptografi Vigenere Cipher Pada Keamanan Data Pesan Teks Berbasis Website," *Jurnal Informatika Teknologi dan Sains*, vol. 4, no. 4, pp. 421–426, 2022, doi: 10.51401/jinteks.v4i4.2155.
- [12] D. Arfandy, M. Simanjuntak, and T. Pasaribu, "Penerapan Metode Vigenere Cipher Untuk Mengamankan Data Text," *JUKI : Jurnal Komputer dan Informatika*, vol. 4, no. 1, pp. 48–54, 2022.
- [13] V. C. Hardita and E. W. Sholeha, "Penerapan Kombinasi Metode Vigenere Cipher, Caesar Cipher Dan Simbol Baca Dalam Mengamankan Pesan," *Jurnal SAINTEKOM*, vol. 11, no. 1, pp. 34–43, 2021, doi: 10.33020/saintekom.v11i1.202.
- [14] B. - and F. Syahputra, "Perancangan Aplikasi Penyandian Pesan Teks Menggunakan Vigenere Chiper Dan Algoritma Elgamal," *MEANS (Media Informasi Analisa dan Sistem)*, vol. 2, no. 2, pp. 80–87, 2018, doi: 10.54367/means.v2i2.142.

- [15] M. R. Darmawan and Windarto, "Implementasi Algoritma Kriptografi Vigenere Cipher dan Affine Cipher untuk Mengamankan Pesan pada Aplikasi Chatting Berbasis Android," *Skanika*, vol. 1, no. 2, pp. 583–590, 2018.