SNESTIK

Seminar Nasional Teknik Elektro, Sistem Informasi, dan Teknik Informatika

https://ejurnal.itats.ac.id/snestik dan https://snestik.itats.ac.id

Informasi Pelaksanaan :
SNESTIK IV - Surabaya, 27 April 2024
Ruang Seminar Gedung A, Kampus Institut Teknologi Adhi Tama Surabaya

Informasi Artikel:
DOI : 10.31284/p.snestik.2024.5844

Prosiding ISSN 2775-5126

Fakultas Teknik Elektro dan Teknologi Informasi-Institut Teknologi Adhi Tama Surabaya
Gedung A-ITATS, Jl. Arief Rachman Hakim 100 Surabaya 60117 Telp. (031) 5945043
Email : snestik@itats.ac.id

Sistem Pengamanan Pesan *Chatting* Menggunakan Algoritma *Vigenere Cipher* Berbasis Web

Citra Nurina Prabiantissa, Gusti Eka Yuliastuti, Ilham Habib Azizi

Institut Teknologi Adhi Tama Surabaya
e-mail: citranurina@itats.ac.id

ABSTRACT

The rapid growth in online communications has led to the development of security methods to protect the privacy and confidentiality of messages between users. One approach used is the use of cryptographic algorithms, such as the Vigenère Cipher algorithm, in web-based applications to secure chat messages. This research aims to implement the Vigenère Cipher algorithm in securing web-based chat messages. This method involves applying the Vigenère Cipher algorithm to the message text to be sent via a web-based chat application. The Vigenère Cipher algorithm works by encrypting messages using a key chosen by the user. This key will convert every character in the original message into an encrypted character. Implementation is done by integrating this algorithm into the web application user interface, allowing the user to enter messages and encryption keys. The results of the implementation by applying the Vigenère Cipher algorithm obtained an average avalanche effect value of 35%, while the results of testing showed that the proposed algorithm was not able to secure message text data effectively but was able to encrypt long messages in a short time. However, keep in mind that Vigenère Cipher has some vulnerabilities to certain cryptanalysis attacks, so monitoring and maintaining security remains important.

Keywords: *Encryption, Vigenère Cipher, chatting, website.*

ABSTRAK

Pertumbuhan pesat dalam komunikasi daring telah mendorong pengembangan metode pengamanan untuk melindungi privasi dan kerahasiaan pesan antara pengguna. Salah satu pendekatan yang digunakan adalah penggunaan algoritma kriptografi, seperti algoritma Vigenere Cipher, dalam aplikasi berbasis web untuk mengamankan pesan chatting. Penelitian ini bertujuan untuk mengimplementasikan algoritma Vigenere Cipher dalam pengamanan pesan chatting berbasis web. Metode ini melibatkan penerapan algoritma

Vigenere Cipher pada teks pesan yang akan dikirimkan melalui aplikasi chatting berbasis web. Algoritma Vigenere Cipher bekerja dengan mengenkripsi pesan menggunakan kunci yang dipilih oleh pengguna. Kunci ini akan mengubah setiap karakter dalam pesan asli menjadi karakter yang terenkripsi. Implementasi dilakukan dengan mengintegrasikan algoritma ini ke dalam antarmuka pengguna aplikasi web, yang memungkinkan pengguna untuk memasukkan pesan dan kunci enkripsi. Hasil implementasi dengan menerapkan Algoritma Vigenere Cipher didapatkan nilai avalanche effect rata-rata sebesar 35% sedangkan hasil dari pengujian yang menunjukkan bahwa algoritma yang diusulkan belum mampu mengamankan data teks pesan secara efektif tetapi mampu mengenkripsi pesan yang panjang dengan waktu yang singkat. Namun, perlu diingat bahwa Vigenere Cipher memiliki beberapa kerentanan terhadap serangan kriptanalisis tertentu, sehingga pemantauan dan pemeliharaan keamanan tetap penting.

Kata kunci: enkripsi; Vigenere Cipher; chatting, website.

PENDAHULUAN

Teknologi komunikasi dan informasi berkembang dengan pesat dan memberikan pengaruh besar bagi kehidupan manusia. Banyaknya kebutuhan akan teknologi ini, mengakibatkan kebutuhan akan keamanan data yang disimpan di dalam komputer juga semakin meningkat. Terdapat beberapa usaha untuk menjaga keamanan data yang dikirimkan melalui media internet, salah satu metodenya adalah menggunakan teknik kriptografi [1]. Dengan perkembangan ini juga muncul beberapa permasalahan akan keamanan dan privasi pesan yang dikirimkan antar pengguna[2]. Pesan-pesan ini dapat menjadi rentan terhadap peretasan atau intersepsi oleh pihak-pihak yang tidak berwenang.

Algoritma kriptografi merupakan solusi yang umum digunakan untuk melindungi pesan dan data pribadi dalam komunikasi daring. Salah satu algoritma yang banyak digunakan adalah algoritma Vigenere Cipher. Algoritma ini telah digunakan sejak lama untuk mengenkripsi pesan dengan menggunakan kunci sebagai mekanisme enkripsi. *Vigenere cipher* adalah huruf yang sama pada plainteks tidak selalu dienkripsi menjadi huruf yang sama pada cipherteks. Hal ini disebabkan karena pada *Vigenere cipher*, pergeseran karakternya ditentukan pada karakter kunci dan kata ini selalu di ulang [3].

Penggunaan algoritma Vigenere Cipher memiliki potensi untuk menjadi solusi efektif dalam mengamankan pesan chatting berbasis web. Dalam algoritma ini, pesan dienkripsi dengan menggeser setiap karakter dalam pesan asli berdasarkan karakter dalam kunci. Kunci yang digunakan dapat diberikan oleh pengguna untuk memastikan bahwa hanya penerima yang memiliki kunci yang dapat membaca pesan yang terenkripsi.

Pada penelitian ini, penulis membuat simulasi dari sistem keamanan yang nantinya dapat diterapkan pada pemrograman berbasis web dengan menggunakan metode enkripsi *Vigenere cipher* sebagai pengamanan data pesan chatting. Metode *Vigenere cipher* dipilih karena dapat memberikan tingkat keamanan yang cukup tinggi untuk mengamankan pesan chatting.

METODE

Pada tahapan ini, membahas mengenai proses penelitian dimana ada 3 proses yang dilakukan. Proses pertama adalah melakukan enkripsi dan dekripsi, melakukan pengujian *avalanche effect*, dan pengujian waktu komputasi pada beberapa skenario teks yang berbeda.

Enkripsi dan Dekripsi Menggunakan Vigenere Cipher

Pada penelitian ini, algoritma Vigenere Cipher digunakan untuk mengamankan chat berbasis web menggunakan teknik kriptografi. Algoritma ini menerapkan enkripsi untuk menyembunyikan informasi data pesan chat dalam database dari ancaman hacker dan tidak dapat dibaca atau dimodifikasi. Sandi Vigenere adalah salah satu jenis sandi alfabet majemuk sederhana. Enkripsi Vigenere menerapkan metode substitusi polialfabetik dan termasuk dalam kategori kunci simetris, dimana kunci yang digunakan untuk proses enkripsi sama dengan kunci yang digunakan untuk proses dekripsi [4]. Pada algoritma *Vigenere Cipher* memiliki key yang

akan digunakan sebagai sandi untuk enkripsi maupun deskripsi pada informasi tersebut, proses enkripsi ini pertama yaitu dengan menginputkan sebuah pesan chat yang akan dienkripsikan [5]. Kemudian pesan chat tersebut sebagai *plaintext*, untuk itu diharuskan setiap alfabet diubah menjadi index. Kemudian dilakukan proses enkripsi. Proses enkripsi dilakukan menggunakan rumus aritmatika [6] sebagai berikut :

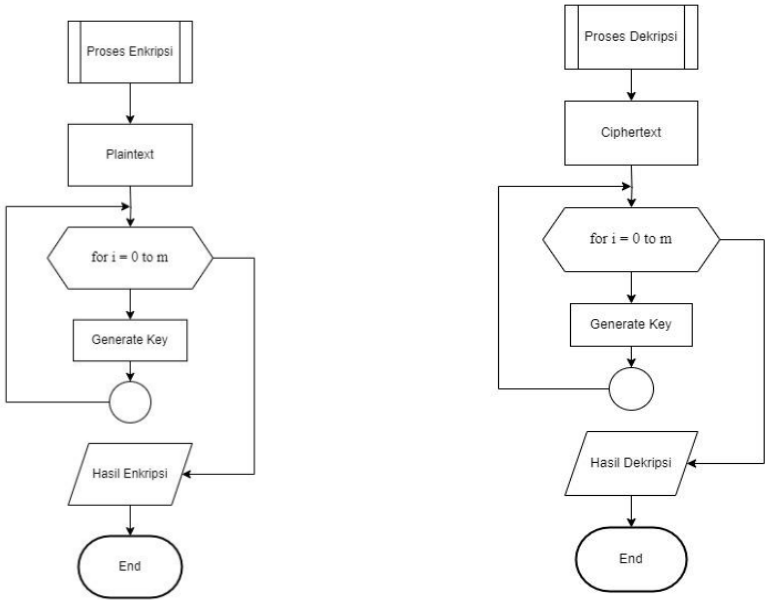
$$C_i = (P_i + K_i) - 26$$

Untuk rumus dekripsi sebagai berikut :

$$C_i = \left(K_i - P_i\right) + 26$$

Ci = karakter dari *ciphertext* ke i
Pi = karakter *plaintext* ke i
Ki = karakter dari *key phase* (jika *key phase* lebih pendek dari *plaintext*, dari *key phase* maka akan diiterasi sesuai dengan panjang dari *plaintext*).

Dekripsi pada *Vigenere Cipher* mempunyai proses yang hampir sama dengan enkripsi, kecuali hasil *plaintext* didapatkan dengan mengurangi huruf dari key yang terduplikasi dari huruf *chipertext*. Jika hasil pengurangan adalah negatif, tambahkan m (jumlah huruf pada alfabet) dengan menentukan P adalah variabel yang mendefinisikan *plaintext*. K digunakan untuk mendefinisikan kunci (Key). C adalah variabel dari *chipertext* [7]. Huruf i adalah variable indeks yang mendefinisikan alamat lokasi dari setiap huruf dalam satu kalimat pesan.



Gambar 1. a) Proses Enkripsi, b) Proses Dekripsi.

Pengujian Menggunakan Avalanche Effect

Skenario pengujian menggunakan *Avalanche Effect* untuk melihat seberapa besar nilai dari kekuatan enkripsi yang dihasilkan saat proses penyandian dengan menggunakan metode Vigenere. Pengujian *Avalanche Effect* bertujuan untuk mengetahui berapa persen perubahan

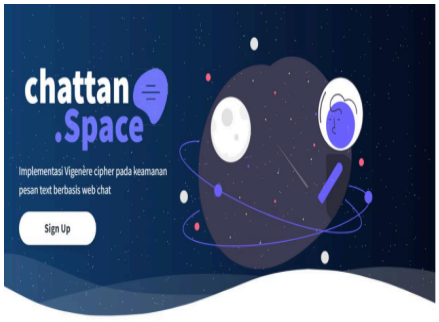
pesan pada saat proses enkripsi dilakukan dengan melihat rasio antar jumlah bit dari *chipertext* yang berubah dan jumlah bit dari *plaintext* sebelum diubah dalam proses enkripsi. Parameter uji coba *Avalanche Effect* dikatakan baik apabila nilai perubahan dari setiap bit dapat menghasilkan lebih dari 50% atau sekitar separuhnya. Untuk menghitung *Avalanche Effect* maka dapat digunakan rumus perhitungannya sebagai berikut :

$$Avalanche\ Effect = \frac{jumlah\ perubaan\ bit}{jumlah\ keseluruhan\ bit} * 100\%$$

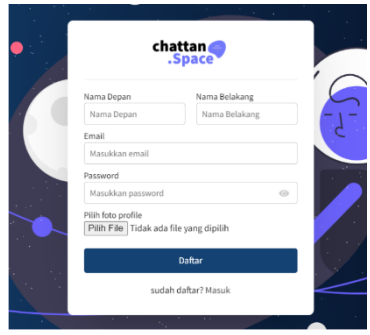
HASIL DAN PEMBAHASAN

Tampilan Antarmuka

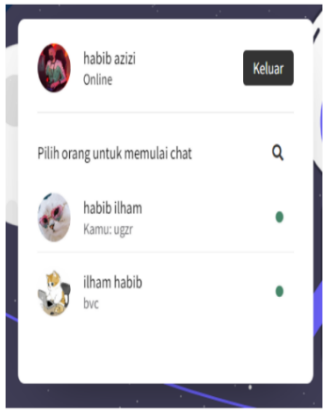
Pada tahap ini akan dijelaskan mengenai implementasi enkripsi pada aplikasi chatting. Tampilan antarmuka dibuat untuk mendukung interaksi antar client pada aplikasi chatting. Pada gambar 2(a) merupakan tampilan awal (*landing page*) dari *website* enkripsi, menunjukkan halaman untuk *sign up.* Gambar 2(b) tampilan ketika pengguna melakukan *Sign up* atau proses di mana pengguna mendaftar atau membuat akun baru dengan inputan nama depan, nama belakang, *email*, *password*, dan upload foto profil. Pada gambar 2(c) adalah halaman dashboard chat, dimana halaman ini berfungsi untuk mengetahui setiap *user* yang ada dengan menunjukkan riwayat *chat* yang terenkripsi, terdapat juga tombol pencarian pengguna, tombol keluar berfungsi untuk *logout* akun, dan setiap ada chat yang masuk maka secara otomatis sistem akan melakukan proses enkripsi dan disimpan di dalam *database* sistem. Gambar 2 (d) halaman tersebut berfungsi untuk mengirim pesan dan menampilkan isi chat dari pengirim dan penerima, menampilkan foto profil dari pengirim pesan serta menunjukkan status *online* dan *offline*. setiap ada chat yang masuk maka secara otomatis system akan melakukan proses *enkripsi* dan disimpan di dalam *database* sistem.



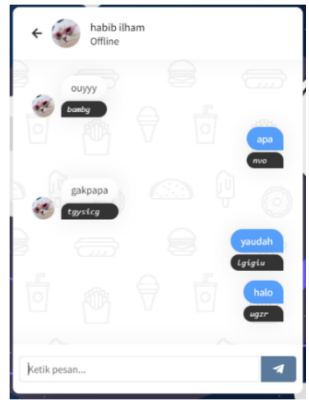
(a)



(b)



(c)



(d)

Gambar 2. a) Tampilan *Dashboard* Aplikasi, b) Tampilan Registrasi, c) Tampilan *Dashboard Chat*, d) Tampilan Halaman *Chatting*

Pengujian Avalanche Effect

Pada pengujian ini akan menggunakan *Avalanche Effect* untuk proses enkripsi dengan *key* yang digunakan adalah "ngoding", untuk mendapatkan data dari keseluruhan prosesnya, dalam pengujian ini akan melakukan pengujian dari 20 data chat, untuk mengetahui tingkat keamanan enkripsi pada pengamanan pesan berbasis web dengan menggunakan algoritma kriptografi metode *Vigenere Cipher.*

Tabel 1. Pengujian *Avalanche Effect*

Data ke-	Jumlah bit terbalik	Jumlah keseluruhan Chipertext	Hasil Avalanche Effect
1	13	32	40%
2	19	48	39%
3	22	64	34%
4	11	32	34,3%
5	23	64	35,9%
6	13	40	32,5%
7	22	72	30,5%
8	21	64	32,8%
9	25	72	34,7%
10	29	88	32,9%
11	26	72	36,1%
12	27	80	33,7%
13	24	64	37,5%
14	28	80	35%
15	18	56	32,1%
Rata -Rata Hasil Avalanche Effect			35%

Hasil pengujian di didapatkan nilai rata - rata *Avalanche Effect* pada tabel 1 adalah 35%, dalam pengujian kali ini metode *Vigenere Cipher* kurang cukup efektif untuk mengamankan data melalui teknik enkripsi dan dekripsi dari pesan chat tersebut karena

persentase kurang dari 50%. Hasil avalanche effect yang paling baik dengan menggunakan jumlah bit terbalik sebanyak 13 dan jumlah ciphertext adalah 32 dengan persentase yang dihasilkan sebanyak 40%.

Pengujian Waktu Komputasi

Pengujian kompleksitas waktu dilakukan untuk mengetahui waktu yang dibutuhkan aplikasi yang digunakan dalam mengamankan data dengan algoritma Vigenere Chiper. Data teks yang digunakan dalam pengujian adalah sebagai berikut:

Aliquam diam velit, fermentum quis posuere eu, venenatis sit amet justo. Aliquam ac nisi felis. Donec quis aliquam sapien. Donec quis efficitur justo. Duis elementum dolor magna, quis sodales diam accumsan nec. In purus urna, auctor at diam at, lobortis sagittis est. Pellentesque et congue nisi. Etiam rutrum vehicula varius. Integer congue finibus sem vel iaculis. Nunc vel mauris est. Ut mollis dolor sed lacinia cursus. Vestibulum eu neque id sem tristique consectetur. Aliquam ut sapien arcu. Sed eu enim ultricies, condimentum dui sit amet, scelerisque nisl. Aliquam pellentesque consectetur purus, in laoreet tortor euismod nec.

Nulla semper enim ac vehicula ultrices. Phasellus molestie neque lectus, quis euismod ex vulputate quis. Morbi dapibus mattis mi, non mattis ex varius in. Phasellus ornare risus in nunc euismod molestie. Vestibulum elit risus, malesuada eget tortor at, tincidunt fermentum augue. Fusce quam lectus, sollicitudin mattis mi ac, tincidunt vulputate mi. Sed id libero tortor. Aenean mauris metus, pellentesque sed ligula quis, vulputate gravida mauris. Maecenas sapien arcu, rutrum eu sollicitudin eu, feugiat eu massa. Aliquam condimentum elit malesuada nisl pretium, id ullamcorper magna tempor. Suspendisse potenti. Maecenas eros magna, iaculis at congue id, cursus ac sapien. Nulla ut consectetur est, non scelerisque ligula.

Duis eleifend at dolor at blandit. Aenean vestibulum felis ut neque hendrerit, sit amet eleifend leo imperdiet. Nam accumsan dui et ultrices gravida. Integer eget odio id erat ultrices mattis ac vitae orci. Integer porta feugiat quam. Vestibulum lectus enim, porta sit amet libero vel, fringilla vulputate massa. Aenean porta dictum felis a fringilla. Duis efficitur vel dolor faucibus scelerisque. In tristique ante non ante scelerisque, at porta ex pretium. Praesent molestie nisi in consectetur fermentum. Ut ex lectus, tincidunt sit amet pellentesque a, placerat aliquam turpis. Aenean accumsan.

Generated 23 paragraphs, 2000 words, 13598 bytes of Lorem Ipsum

Gambar 3. Data teks

Data teks tersebut didapatkan di situs Lorem Ipsum terdapat 23 paragraf dan 2000 kata, dari banyaknya kata tersebut akan dibagi menjadi 20 pengujian setiap pengujian akan menguji berkelipatan 100 kata. Berikut ini hasil dari pengujian waktu komputasi:

Tabel 2. Pengujian Waktu Komputasi

No	Jumlah karakter	Jumlah kata	Hasil Waktu Komputasi
1	705	100	0.0009989738464355469 detik
2	1345	200	0.0019991397857666016 detik
3	2030	300	0.0029983520507812 5 detik
4	2677	400	0.0039966106414794 92 detik
5	3371	500	0.0049972534179687 5 detik
6	4077	600	0.0059974193572998 05 detik
7	4774	700	0.0069959163665771 484 detik
8	5443	800	0.0079925060272216 8 detik
9	6127	900	0.0089952945709228 52 detik
10	6791	1000	0.0099942684173583 98 detik
Rata -Rata Komputasi Waktu			0.0054966 detik

Hasil waktu komputasi pada tabel 2 menunjukkan waktu komputasi tercepat pada saat menggunakan jumlah karakter 705 dan jumlah kata yang digunakan adalah 100 dengan hasil 0.00099 detik. Semakin banyak jumlah karakter yang digunakan, maka waktu komputasi yang

digunakan juga semakin lama seperti pada percobaan ke-10, dengan jumlah karakter 6791 dan menggunakan jumlah kata 1000 dengan hasil 0.0099 detik.

KESIMPULAN

Pengujian aplikasi ini menandakan aplikasi berjalan dengan cukup baik dengan hasil pengujian menggunakan avalanche effect dan pengujian waktu komputasi. Rata – rata hasil pengujian *Avalanche Effect* sebesar 35% dengan 15 kali pengujian untuk skenario yang berbeda. Nilai 40% didapatkan pada data pertama dengan jumlah bit 13 dan jumlah ciphertext 32. Dari hasil ini dapat disimpulkan bahwa algoritma ini tidak terlalu aman dalam menjaga kerahasiaan data, karena seharusnya jumlah prosentase *Avalanche Effect* adalah diatas 50%. Pengujian waktu komputasi yang dilakukan terhitung cukup baik dibandingkan dengan pengujian *Avalanche Effect*. Rata – rata komputasi waktu adalah 0.0054966 detik. Hal ini dinilai cukup cepat untuk sebuah aplikasi dalam melakukan enkripsi pada data teks.

DAFTAR PUSTAKA

[1] D. Astuti and C. Sundari, "IMPLEMENTASI ALGORITMA VIGENERE CIPHER UNTUK ENKRIPSI DAN DEKRIPSI PADA PERESEPAN DATA OBAT DI PUSKESMAS MERTOYUDAN 1 KABUPATEN MAGELANG," *Jurnal Teknik Informasi dan Komputer (Tekinkom)*, vol. 5, no. 2, p. 341, Dec. 2022, doi: 10.37600/tekinkom.v5i2.534.

[2] D. Abdullah, "School of Informatics Management and Computing , STMIK Jayakarta PENGAMANAN EMAIL MENGGUNAKAN METODE VIGENERE CIPHER," *JISAMAR (Journal of Information System, Applied, Management, Accounting and Research*, pp. 2598–8700, 2017, [Online]. Available: http://journal.stmikjayakarta.ac.id/index.php/jisamar

[3] S. Budi, A. B. Purba, and J. Mulyana, "PENGAMANAN FILE DOKUMEN MENGGUNAKAN KOMBINASI METODE SUBTITUSI DAN VIGENERE CIPHER," *ILKOM Jurnal Ilmiah*, vol. 11, no. 3, pp. 222–230, Dec. 2019, doi: 10.33096/ilkom.v11i3.477.222-230.

[4] P. Sumber *et al.*, *SUPER ENCRYPTION APPLICATION OF CRYPTOGRAPHY USING COMBINATION OF COLUMNAR TRANSPOSITION AND VIGENERE CIPHER*.

[5] Megawati, Muhammad Fitra Hamidy, Sasqia Ismi Aulia, Yuhendri Putra, and Mhd Arief Hasan, "Enkripsi dan Deskripsi File Menggunakan Kombinasi Vigenere dan Shift Cipher di Python," *SATIN - Sains dan Teknologi Informasi*, vol. 7, no. 1, pp. 102–111, Jun. 2021, doi: 10.33372/stn.v7i1.686.

[6] M. Hafitz Firmansyah, G. Eka Yuliastuti, and C. Nurina Prabiantissa, "Implementasi Multi Enkripsi Algoritma Vigenere Cipher dan Cipher Block Chaining (CBC) untuk Pengamanan Data Pegawai."

[7] E. Tarigan and D. H. S. Maha, "KOMBINASI VIGENERE CIPHER DAN POLYALPHABETIC CIPHER PADA PENGAMANAN FILE TEXT".