PENINGKATAN KEAMANAN ALGORITMA VIGENÈRE DENGAN PROTOKOL TIGA LANGKAH TANPA PENDISTRIBUSIAN KUNCI

Andysah Putera Utama Siahaan
Program Studi Sistem Komputer, Universitas pembangunan Panca Budi
Email: andiesiahaan@gmail.com

ABSTRACT
In computer networks, information exchange is common. The information transmitted can be confidential or ordinary. However, when sending confidential information, there are often concerns about its security. Senders tend to worry that the information sent will be stolen, especially if it contains confidential data. In order for the information to be read correctly, the sender and receiver must know the key or password. However, sending keys is also an important concern because if it falls into the wrong hands, the data and information contained in the file can be read easily. Therefore, key exchanges should be avoided and one of the techniques that can be used to avoid them is the Three Step Protocol scheme. This scheme allows the sender and receiver to encrypt and decrypt using their respective keys without having to exchange keys. The Three-Step Protocol is a mechanism that involves two algorithms in the cryptographic process, the Vigenère Algorithm. By implementing the Three-Step Protocol scheme, it can improve data security.
***Keywords**: Vigenère, TPP, encryption, decryption, protocol*

PENDAHULUAN

Pertukaran informasi adalah kegiatan yang sangat penting dalam kehidupan modern. Seiring dengan perkembangan teknologi, pertukaran informasi semakin sering dilakukan melalui jaringan komputer, seperti internet dan intranet. Meskipun demikian, pertukaran informasi melalui jaringan komputer juga memiliki risiko keamanan yang tinggi [1].

Untuk menghindari risiko keamanan, diperlukan upaya untuk mengenkripsi data yang akan dikirimkan. Enkripsi adalah proses mengubah data asli menjadi bentuk yang tidak dapat dibaca oleh pihak yang tidak berwenang [2]. Dalam melakukan enkripsi, digunakan suatu kunci rahasia yang hanya diketahui oleh pengirim dan penerima data. Dengan begitu, hanya penerima data yang dapat membaca pesan yang dikirimkan.

Algoritma Vigenère merupakan salah satu jenis sandi substitusi polialfabetik yang menggunakan kunci yang sama panjang dengan teks terenkripsi untuk menghasilkan sandi yang sulit dipecahkan [3]. Namun, distribusi kunci pada algoritma Vigenère menjadi tantangan karena kunci harus disebarkan secara aman kepada pihak yang berwenang untuk membuka pesan terenkripsi. Masalah utama dalam penggunaan Algoritma Vigenère adalah distribusi kunci enkripsi yang tidak aman [4]. Saat ini, banyak cara untuk mendistribusikan kunci enkripsi, seperti pengiriman kunci melalui email atau pesan teks, namun metode ini dapat rentan terhadap serangan cyber.

Untuk mengatasi masalah ini, telah dikembangkan Protokol Tiga Langkah pada algoritma Vigenère untuk menghindari distribusi kunci. Protokol ini bertujuan untuk meningkatkan keamanan algoritma Vigenère dengan menggunakan tiga tahap komunikasi antara pengirim dan penerima tanpa harus mengirimkan kunci secara langsung [5].

Protokol Tiga Langkah pada algoritma Vigenère melibatkan penggunaan operasi XOR dan operasi modulo dalam proses pengiriman dan penerimaan pesan [6]. Dalam protokol ini, pengirim mengenkripsi pesan dengan kunci acak yang dikirim ke penerima pada tahap pertama. Pada tahap kedua, penerima mengirimkan pesan kembali ke pengirim setelah melakukan operasi XOR dengan pesan yang diterima dan kunci acak tersebut.

Penulis menjelaskan secara rinci tentang Protokol Tiga Langkah pada Algoritma Vigenère yang telah mereka rancang. Mereka juga melakukan analisis keamanan terhadap protokol tersebut dan menguji keefektifannya dalam mengamankan pesan yang dikirim melalui jaringan komunikasi.

TINJAUAN PUSTAKA

2.1 Algoritma Vigenère

Algoritma Vigenère adalah salah satu teknik enkripsi yang ditemukan pada abad ke-16 oleh Blaise de Vigenère, seorang diplomat dan kriptografer Prancis. Sandi ini tergolong sebagai jenis sandi substitusi polialfabetik, yang berarti satu huruf pada plaintext dapat dienkripsi menjadi huruf yang berbeda pada ciphertext dengan menggunakan kunci enkripsi tertentu. Pada awalnya, Algoritma Vigenère dianggap sangat sulit untuk dipecahkan karena kunci enkripsi yang digunakan berubah secara periodik. Namun, pada abad ke-19, seorang kriptologis asal Prancis bernama Charles Babbage menemukan celah kelemahan dalam sandi ini. Sejak saat itu, banyak penelitian telah dilakukan untuk meningkatkan keamanan Algoritma Vigenère dan menemukan metode untuk mendekripsi pesan yang dienkripsi dengan sandi ini. Salah satu metode yang paling umum digunakan adalah analisis frekuensi huruf dalam teks terenkripsi [7].

Beberapa penelitian terbaru mengusulkan penggunaan metode kriptografi modern, seperti teknik enkripsi kunci publik, untuk meningkatkan keamanan Algoritma Vigenère. Selain itu, Protokol Tiga Langkah juga diusulkan sebagai cara untuk meningkatkan keamanan Algoritma Vigenère dengan meminimalkan distribusi kunci enkripsi yang rentan terhadap serangan cyber. Dalam tinjauan pustaka tentang Algoritma Vigenère, peneliti juga membahas tentang aplikasi sandi ini dalam berbagai bidang, seperti keamanan komunikasi, kriptografi teori, dan analisis bahasa [8].

2.2 Protokol Tiga Langkah

Protokol Tiga Langkah merupakan salah satu metode dalam kriptografi untuk meningkatkan keamanan komunikasi. Protokol ini dirancang untuk memastikan bahwa pesan hanya dapat diakses oleh pihak yang sah dan tidak dapat diakses oleh pihak yang tidak berwenang [9].

Salah satu contoh penggunaan Protokol Tiga Langkah adalah dalam kriptografi kunci publik, di mana kunci enkripsi dan dekripsi berbeda. Dalam protokol ini, tiga pesan pertukaran disertakan untuk memastikan bahwa kunci enkripsi yang dikirimkan aman dan tidak dapat diakses oleh pihak yang tidak berwenang.

Banyak penelitian telah dilakukan untuk meningkatkan Protokol Tiga Langkah dan menerapkannya dalam berbagai aplikasi kriptografi, seperti pertukaran kunci, autentikasi, dan enkripsi data. Beberapa penelitian terbaru juga mengusulkan Protokol Tiga Langkah untuk meningkatkan keamanan dalam berbagai sistem, seperti jaringan sensor nirkabel, pengiriman pesan instan, dan pembayaran elektronik [10].

METODOLOGI

Metodologi kriptografi algoritma Vigenère menggunakan Protokol Tiga Langkah terdiri dari langkah-langkah berikut:

1. Langkah Pertama: Pembangkitan Kunci
   Pembangkitan kunci dilakukan terhadap pengirim dan penerima untuk mendapatkan kunci rahasia yang berbeda dan dipegang oleh masing-masing pengirim dan penerima. Kunci rahasia ini akan digunakan untuk mengenkripsi dan mendekripsi pesan. Kunci tidak perlu dipertukarkan kepada pengirim atau penerima.
2. Langkah Kedua: Enkripsi Pesan oleh Pengirim
   Setelah kunci rahasia telah disepakati, pengirim mengenkripsi pesan yang ingin dikirim dengan menggunakan algoritma Vigenère. Algoritma Vigenère adalah metode enkripsi yang menggunakan kunci rahasia berupa string karakter untuk mengubah pesan asli menjadi pesan terenkripsi. Setelah pesan dienkripsi, pengirim mengirimkan pesan terenkripsi ke penerima.

e-ISSN: 2775 - 4049

3. Langkah Ketiga: Enkripsi Pesan oleh Penerima
   Setelah menerima pesan terenkripsi, penerima menggunakan kunci rahasia miliknya untuk mengenkripsi pesan tahap kedua. Penerima mengembalikan pesan terenkripsi ke penerima untuk selanjutnya diproses.
4. Langkah Ketiga: Dekripsi Pesan oleh Pengirim
   Setelah menerima pesan terenkripsi tahap kedua dari penerima, pengirim menggunakan kunci rahasia miliknya untuk mendekripsikan pesan tersebut. Penerima mengembalikan pesan terenkripsi ke penerima untuk selanjutnya diproses.
5. Langkah Ketiga: Dekripsi Pesan oleh Penerima
   Setelah menerima pesan terenkripsi yang sudah dilakukan proses dekripsi oleh pengirim, penerima menggunakan kunci rahasia miliknya untuk mengenkripsi pesan untuk terakhir kalinya agar mendapatkan pesan asli. Setelah berhasil, penerima dapat membaca pesan tersebut dengan sempurna.

HASIL DAN PEMBAHASAN

4.1 Hasil Penelitian

Dalam tes yang dilakukan, tabel-tabel dapat digunakan untuk menjelaskan bagaimana proses transformasi teks biasa menjadi teks sandi dan teks sandi menjadi teks biasa. Tabel pertama dan kedua dapat menunjukkan langkah-langkah yang dilakukan pada saat enkripsi dan tabel ketiga dan keempat dapat menunjukkan langkah-langkah yang dilakukan pada saat dekripsi. Dengan adanya tabel-tabel ini, diharapkan tes dapat dilakukan dengan lebih mudah dan jelas, serta memudahkan dalam mengevaluasi keamanan skema Protokol Tiga Langkah yang digunakan. Berikut tabel-tabel yang digunakan untuk menjelaskan proses enkripsi dan dekripsi pada hasil ujicoba.

Table 1. Enkripsi pertama dilakukan oleh pengirim

Karakter Plaintext	ASCII Plaintext	Kunci Pengirim	ASCII Kunci	Hasil Enkripsi	Karakter Ciphertext
R	82	I	73	155	›
A	65	N	78	143	•
I	73	D	68	141	•
N	78	O	79	157	•
N	78	N	78	156	œ
B	66	E	69	135	‡
O	79	S	83	162	¢
W	87	I	73	160	
	32	A	65	97	a
S	83	I	73	156	œ
I	73	N	78	151	—
X	88	D	68	156	œ

Table 2. Enkripsi kedua dilakukan oleh penerima

Karakter Ciphertext	ASCII Ciphertext	Kunci Penerima	ASCII Kunci	Hasil Enkripsi	Karakter Ciphertext

e-ISSN: 2775 - 4049

›	155	F	70	225	á
•	143	R	82	225	á
•	141	E	69	210	Ò
•	157	E	69	226	â
œ	156	D	68	224	à
‡	135	O	79	214	Ö
¢	162	M	77	239	ï
	160	F	70	230	æ
a	97	R	82	179	³
œ	156	E	69	225	á
—	151	E	69	220	Ü
œ	156	E	69	225	á

Table 3. Dekripsi pertama dilakukan oleh pengirim

Karakter Ciphertext	ASCII Ciphertext	Kunci Pengirim	ASCII Kunci	Hasil Dekripsi	Karakter Ciphertext
á	225	I	73	152	˜
á	225	N	78	147	“
Ò	210	D	68	142	Ž
â	226	O	79	147	“
à	224	N	78	146	’
Ö	214	E	69	145	‘
ï	239	S	83	156	œ
æ	230	I	73	157	•
³	179	A	65	114	r
á	225	I	73	152	˜
Ü	220	N	78	142	Ž
á	225	D	68	157	•

Table 4. Dekripsi pertama dilakukan oleh penerima

Karakter Ciphertext	ASCII Ciphertext	Kunci Penerima	ASCII Kunci	Hasil Dekripsi	Karakter Plaintext
˜	152	F	70	82	R
“	147	R	82	65	A
Ž	142	E	69	73	I
“	147	E	69	78	N
’	146	D	68	78	N
‘	145	O	79	66	B
œ	156	M	77	79	O

•	157	F	70	87	W
r	114	R	82	32	
˜	152	E	69	83	S
Ž	142	E	69	73	I
•	157	E	69	88	X

Dari hasil penelitian yang dilakukan, dapat disimpulkan bahwa skema Protokol Tiga Langkah menggunakan algoritma Vigenère mampu menghasilkan hasil enkripsi dan dekripsi yang berhasil. Tabel 1 dan 2 menunjukkan hasil enkripsi teks "RAINBOW SIX" dengan menggunakan dua kunci yang berbeda yang dilakukan oleh penerima dan pengirim. Sedangkan tabel 3 dan 4 menunjukkan hasil dekripsi dari pengirim dan penerima. Hasil akhir yang diterima oleh pengirim sama dengan pesan asli yang dikirimkan, membuktikan bahwa skema Protokol Tiga Langkah berfungsi dengan baik dan berhasil melakukan enkripsi dan dekripsi secara efektif tanpa perlu menukar kunci antara pengirim dan penerima. Dengan demikian, skema Protokol Tiga Langkah dengan algoritma Vigenère dapat dianggap sebagai metode yang aman dan efisien untuk menjaga keamanan pesan dalam komunikasi digital.

4.2 Pembahasan Penelitian

Protokol Tiga Langkah menggunakan algoritma Vigenère dapat digunakan untuk mengamankan pesan. Dalam eksperimen ini, plaintext yang digunakan adalah "RAINBOW SIX". Proses enkripsi dilakukan dengan menggunakan dua kunci yang berbeda, yaitu kunci pertama dan kunci kedua. Kunci pertama digunakan untuk menghasilkan ciphertext 1, sedangkan kunci kedua digunakan untuk menghasilkan ciphertext 2 dan ciphertext 3.

Dalam proses enkripsi, setiap karakter plaintext ditransformasi menjadi nilai ASCII. Kemudian, nilai ASCII tersebut ditambahkan dengan nilai ASCII dari karakter kunci pertama. Jika panjang plaintext melebihi panjang kunci, maka kunci akan diulang untuk menyesuaikan panjang plaintext.

Setelah ciphertext 1 berhasil dihasilkan, proses enkripsi dilanjutkan dengan menggunakan ciphertext 1 sebagai plaintext dan kunci kedua sebagai kunci. Proses ini menghasilkan ciphertext 2 dan ciphertext 3. Nilai ASCII dari ciphertext 2 dan ciphertext 3 dihitung dengan mengurangi nilai ASCII dari ciphertext 1 dengan nilai ASCII dari karakter kunci kedua. Seperti halnya dengan proses sebelumnya, jika panjang ciphertext 1 melebihi panjang kunci kedua, maka kunci kedua akan diulang.

Hasil dari proses enkripsi tersebut adalah ciphertext yang terdiri dari tiga bagian, yaitu ciphertext 1, ciphertext 2, dan ciphertext 3. Ciphertext ini kemudian dapat dikirimkan ke penerima pesan.

Untuk proses dekripsi, penerima pesan menggunakan dua kunci yang sama dengan pengirim pesan, yaitu kunci pertama dan kunci kedua. Penerima pesan pertama-tama melakukan proses dekripsi pada ciphertext 3 dengan menghitung nilai ASCII dari karakter plaintext menggunakan rumus yang sama dengan proses enkripsi sebelumnya, namun dengan mengurangi nilai ASCII dari ciphertext 3 dengan nilai ASCII dari karakter kunci kedua.

Kemudian, penerima pesan melakukan proses dekripsi pada ciphertext 2 dengan menggunakan nilai ASCII dari hasil proses dekripsi ciphertext 3 sebagai plaintext dan kunci kedua sebagai kunci. Nilai ASCII dari plaintext dihitung dengan menambahkan nilai ASCII dari ciphertext 2 dengan nilai ASCII dari karakter kunci kedua.

Proses dekripsi terakhir dilakukan pada ciphertext 1 dengan menggunakan nilai ASCII dari hasil proses dekripsi ciphertext 2 sebagai plaintext dan kunci pertama sebagai kunci. Nilai ASCII dari plaintext dihitung dengan mengurangi nilai ASCII dari ciphertext 1 dengan nilai ASCII dari karakter kunci pertama.

Setelah proses dekripsi selesai dilakukan, hasil akhirnya adalah plaintext yang sesuai dengan pesan asli yang dikirimkan, yaitu "RAINBOW SIX". Hal ini menunjukkan keberhasilan dari penggunaan Protokol Tiga Langkah menggunakan algoritma Vigenère untuk mengamankan pesan.

KESIMPULAN

Hasil penelitian dengan skema Protokol Tiga Langkah dapat memberikan banyak informasi. Dalam penelitian ini, penulis mengambil beberapa kesimpulan berdasarkan desain dan implementasi yang telah dilakukan. Dalam skema Protokol Tiga Langkah, dua kunci yang berbeda digunakan dalam proses enkripsi dan dekripsi. Salah satu keuntungan dari skema ini adalah bahwa pengirim dan penerima tidak perlu menukar atau memberikan kunci untuk menggunakan algoritma Algoritma Vigenère. Proses enkripsi dilakukan dengan menambahkan nilai ASCII dari teks biasa dengan nilai sandi yang dihasilkan dari kunci pertama. Sedangkan dalam proses dekripsi, nilai ASCII dari sandi dihitung dengan mengurangi nilai sandi dengan kunci kedua. Agar lebih mudah menghitung skema Protokol Tiga Langkah, algoritma yang digunakan pada pengirim dan penerima adalah algoritma Vigenère.

DAFTAR PUSTAKA

[1] S. Supiyandi, H. Hermansyah, and K. A. P. Sembiring, "Implementasi dan Penggunaan Algoritma Base64 dalam Pengamanan File Video," *J. MEDIA Inform. BUDIDARMA*, vol. 4, no. 2, p. 340, Apr. 2020, doi: 10.30865/mib.v4i2.2042.

[2] I. Sumartono, A. P. U. Siahaan, and Arpan, "Base64 Character Encoding and Decoding Modeling," *Int. J. Recent Trends Eng. Res.*, vol. 2, no. 12, pp. 63–68, 2016.

[3] A. I. Permana, *Kombinasi Algoritma Kriptografi One Time Pad dengan Generate Random Keys dan Vigenere Cipher dengan Kunci EM2B*. Medan: Universitas Sumatera Utara, 2019.

[4] A. Hidayat, "Algoritma Kriptografi Vigenere Cipher," *Web Programmer*, 2018. [Online]. Available: https://arfianhidayat.com/algoritma-kriptografi-vigenere-cipher. [Accessed: 07-Nov-2021].

[5] D. Rachmawati and M. A. Budiman, "An implementation of the H-rabin algorithm in the shamir three-pass protocol," in *2017 2nd International Conference on Automation, Cognitive Science, Optics, Micro Electro--Mechanical System, and Information Technology (ICACOMIT)*, 2017, pp. 28–33, doi: 10.1109/ICACOMIT.2017.8253381.

[6] A. Subandi, R. Meiyanti, C. L. M. Sandy, and R. W. Sembiring, "Three-Pass Protocol Implementation in Vigenere Cipher Classic Cryptography Algorithm with Keystream Generator Modification," *Adv. Sci. Technol. Eng. Syst. J.*, vol. 2, no. 5, pp. 1–5, Jun. 2017, doi: 10.25046/aj020501.

[7] A. Amrulloh and E. I. H. Ujianto, "Kriptografi Simetris Menggunakan Algoritma Vigenere Cipher," vol. 5, no. 2, pp. 71–77, 2019.

[8] 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.

[9] B. Oktaviana and A. P. U. Siahaan, "Three-Pass Protocol Implementation on Caesar Cipher in Classic Cryptography," *IOSR J. Comput. Eng.*, vol. 18, no. 4, pp. 26–29, 2016.

[10] A. P. U. Siahaan, "Three-Pass Protocol Concept in Hill Cipher Encryption Technique," *Int. J. Sci. Res.*, vol. 5, no. 7, pp. 1149–1152, 2016.