

ANALISIS KEAMANAN DATA PELANGGAN MENGGUNAKAN ALGORITMA VIGENERE CIPHER DAN PLAYFAIR CIPHER

Erika Tangsi Rante¹, Muhammad Alnando², Mistu Heru³, Kevin Junior⁴

Institut Teknologi Batam

erikatangsi04@gmail.com

Abstrak

Teknologi yang berkembang pesat menjadi salah satu alasan mengapa keamanan informasi harus dijaga dengan ketat. Khusus untuk data pelanggan yang berisi data pribadi dan transaksi yang sensitif. Pengamanan data melalui enkripsi merupakan cara untuk melindungi data dari hal-hal yang tidak diinginkan seperti kebocoran data. Enkripsi dan dekripsi menggunakan kombinasi algoritme enkripsi Vigenere dan algoritme enkripsi Playfair mempersulit orang luar untuk memecahkan data pelanggan. Hasil analisis ini menghasilkan ciphertext yang kuat.

Key Words: Keamanan data, Vigenere Cipher, Playfair Cipher, Enkripsi, Data pelanggan

1. PENDAHULUAN

Perkembangan dunia teknologi dan komunikasi yang begitu pesat memungkinkan terjadinya pertukaran informasi yang cepat dengan pihak lain. Teknologi informasi juga mempermudah penyimpanan file dalam bentuk data, yang secara fisik mengurangi konsumsi kertas yang memakan banyak ruang. Di dunia informasi terdapat dua jenis informasi, yakni informasi publik yang dapat diakses oleh siapa saja, bahkan kadang berubah-ubah, dan informasi rahasia yang hanya dapat diakses oleh pihak tertentu.

Dunia teknologi informasi yang terus berkembang membuat tantangan keamanan data juga menjadi sangat kompleks. Organisasi atau bisnis menyimpan data pelanggan seperti identitas pribadi dan data transaksi pelanggan. Melindungi data pelanggan penting dalam menghadapi ancaman seperti pencurian identitas, serangan dunia maya dan pelanggaran data. Algoritma perlindungan data pelanggan adalah sekumpulan metode dan teknik untuk melindungi kerahasiaan data pelanggan. Tujuan dari algoritma ini adalah untuk mencegah

akses tidak sah, manipulasi data dan pengungkapan informasi sensitif. Suatu teknik keamanan yang sering diterapkan secara luas adalah enkripsi.

Enkripsi adalah proses mengubah teks atau data menjadi bentuk yang hanya dapat dibaca oleh pihak yang memiliki kunci dekripsi yang tepat. Ketika data pelanggan dienkripsi, mereka tidak dapat membaca atau mengakses data bahkan jika orang yang tidak berhak menyita data tersebut. Identifikasi pengguna merupakan langkah penting dalam algoritma keamanan data pelanggan. Artinya, identitas pengguna diverifikasi menggunakan kata sandi, autentikasi dua faktor atau metode verifikasi lainnya mewajibkan pengguna untuk membuktikan identitas mereka yang dapat mengurangi risiko penggunaan yang tidak sah. Beberapa penelitian tentang enkripsi Vigenere telah dilakukan dengan menggabungkan enkripsi Vigenere dengan teknologi lainnya. Karena itu muncul ide menggabungkan sandi Vigenere dengan sandi Playfair. Hasil kombinasi ini menghasilkan ciphertext yang sulit untuk diprediksi, bahkan ketika menggunakan metode penyerangan Klasik, Hal ini terjadi karena set karakter yang dihasilkan berbeda dengan karakter yang digunakan pada teks asli (plaintext).

2. METODELOGI PENELITIAN

Metodologi penelitian yang digunakan yaitu metode analisis deskriptif, yang mengumpulkan informasi melalui penelitian, observasi dan studi literatur dan didukung oleh algoritma Vigenere Cipher dan Playfair Cipher, yang digunakan untuk menguji dan mengawasi keamanan data sebagai implementasi proses keamanan pada sisi enkripsi sehingga keamanan data dikatakan lebih aman.

a. Vigenere Cipher

Vigenere Cipher merupakan teknik enkripsi sederhana yang memiliki tingkat keamanan lebih tinggi daripada Caesar Cipher. Metode ini memanfaatkan karakter dari kata kunci untuk melakukan pengkodean pada teks abjad. Cipher Vigenere termasuk dalam kelas cipher substitusi multihuruf, yang berarti bahwa setiap huruf dalam plaintext dapat dienkripsi dengan beberapa huruf berbeda dalam ciphertext. Rumus enkripsi sandi Vigenere adalah sebagai berikut:

$C_i = (P_i + K_i) \bmod 26$, dimana C_i adalah nilai desimal dari karakter ciphertext ke- i , P_i adalah nilai desimal dari karakter plaintext ke- i , K_i adalah karakter kunci ke- i , dan mod adalah operasi modulus.

Rumus dekripsi untuk sandi Vigenere adalah sebagai berikut:

$P_i = (C_i - K_i + 26) \bmod 26$, dimana P_i adalah nilai desimal dari karakter plaintext ke- i , C_i adalah nilai desimal ke- i dari karakter ciphertext, K_i adalah nilai desimal ke- i dari karakter kunci, dan mod adalah operasi modular. Untuk mengenkripsi teks biasa menggunakan enkripsi Vigenere, setiap huruf dari teks biasa dienkripsi dengan huruf dari kunci yang sesuai.

b. Playfair Cipher

Metode enkripsi Playfair merupakan salah satu metode enkripsi klasik yang sudah dikenal sejak lama dan masih banyak digunakan serta diteliti. Playfair Cipher terdapat dalam kelas Polygram Cipher, dimana metode ini mengenkripsi pasangan huruf menjadi teks yang jelas. Dengan Playfair Cipher, plaintext dipecah menjadi pasangan huruf (bigram) yang kemudian dienkripsi sesuai dengan aturan dan ketentuan tertentu. Skema enkripsi Playfair Cipher menggunakan tabel sandi yang menggantikan huruf-huruf dalam teks biasa dengan huruf yang sesuai dalam teks sandi. Tabel penyandian ini sering disebut tabel Playfair atau Matriks Playfair.

3. ANALISA DAN PERANCANGAN

Di bawah ini, kami akan menunjukkan penggunaan Vigenere cipher dengan menggunakan urutan abjad seperti pada tabel 1.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Algoritma Vigenere dengan teknik bilangan menggunakan tabel translasi huruf ke angka dimana huruf yang dimulai dengan A diubah menjadi 0, sedangkan B menjadi 1 dan seterusnya kemudian berakhir dengan angka 25.

Plaintext : TANJIROU KAMADO

Key : ITEBA JAYA

Rumus : $C_i \equiv (P_i + K_i) \bmod 26$

Kemudian untuk mendapatkan ciphertext, plaintext diubah menjadi format sesuai tabel

berikut:

Plain Text	T	A	N	J	I	R	O	U	K	A	M	A	D	O
Konversi	19	0	13	9	8	17	14	20	10	0	12	0	3	14
Key	I	T	E	B	A	J	A	Y	A	I	T	E	B	A
Konversi	8	19	4	1	0	9	0	24	0	8	19	4	1	0

Lalu hasil konversi dari plaintext dan key dijumlahkan

Hasil	27	19	17	10	8	26	14	44	10	8	31	4	4	14
-------	----	----	----	----	---	----	----	----	----	---	----	---	---	----

Hasil penjumlahan konversi diubah sesuai dengan Mod 26, apabila jika jumlahnya lebih dari 26 maka akan diulang dari huruf A. Setelah jumlahnya ditemukan, angka-angka tersebut diubah kembali menjadi huruf untuk mendapatkan ciphertext-nya:

Modulo 26	1	19	17	10	8	0	14	18	10	8	5	4	4	14
Cipher Text	A	T	R	K	I	A	O	S	K	I	F	D	D	O

4. KESIMPULAN

Berdasarkan hasil analisis, kombinasi metode enkripsi dengan Algoritma Vigenere Cipher dan Playfair Cipher dapat digunakan sebagai alat untuk mengamankan data pelanggan, sehingga data dan transaksi pelanggan tetap aman meskipun terjadi gangguan yang disebabkan oleh berbagai tindakan yang tidak diinginkan.

Melindungi data pelanggan dengan menggabungkan algoritma enkripsi Vigenere dan metode enkripsi Playfair menjadi sulit untuk dipecahkan oleh pihak lain. Hal ini disebabkan karena analisis frekuensi menjadi sangat rumit, mengingat frekuensi kemunculan huruf dalam teks sandi menjadi seragam dan proses enkripsi serta dekripsi data melibatkan kombinasi dua huruf. Oleh karena itu, menganalisis frekuensi untuk teknik enkripsi ini menjadi sangat sulit.

REFERENSI

- Aisyiah, J., Priyambodo, Bambang, Faridah, Bilqis, Yanuarima, Arisa, & Sudi, Galih Gumelar. (2023, June). Penerapan Algoritma Vigenere Cipher Untuk Keamanan Data. *Jurnal Informatika - COMPUTING*, X(1), 1-6.
- Kehista, A. P., Fauzi, A., Tamara, A., Putri, I., Fauziah, N. A., Klarissa, S., & Damayanti, V. B. (2023). Analisis Keamanan Data Pribadi pada Pengguna E-Commerce: An-

- caman, Risiko, Strategi Keamanan (Literature Review). *Jurnal Ilmu Manajemen Terapan*, 4(5), 625-632.
- Habibie, Alief Fathul, Zahary, Fahmi, Lubis, Muara Nataryda, & Nasution, Mardiah. (2022, December). Penggunaan Algoritma Vigenere Cipher Sebagai Keamanan Sistem Pada Usaha Kecil Menengah. *Journal of Software Engineering, Computer Science and Information Technology*, III(2), 223-231.
- Maynard, Taufan, Sancaka, Prananda, Lusiana, Veronica, Lomba, Jalan Tri, & Semarang, Juang. (2022, December). Penerapan Metode Playfair Cipher Dalam Aplikasi Enkripsi-Dekripsi File Teks. *XV(2)*, 260-270.
- Riadi, imam, Fadlil, Abdul, & Tsani, Fahmi Auliya. (2022, January). Pengamanan Citra Digital Berbasis Kriptografi Menggunakan Algoritma Vigenere Cipher. *JISKA (Jurnal Informatika Sunan Kalijaga)*, 7(1), 33-45.
- Riadi, I., Fadlil, A., & Tsani, F. A. (2022). Pengamanan Citra Digital Berbasis Kriptografi Menggunakan Algoritma Vigenere Cipher. *JISKA (Jurnal Informatika Sunan Kalijaga)*, 7(1), 33-45.
- Sancaka, T. M. P., & Lusiana, V. (2022). Penerapan Metode Playfair Cipher Dalam Aplikasi Enkripsi-Dekripsi File Teks. *Jurnal Elektronika dan Komputer*, 15(2), 260-270.
- Perdana, G. A., & Mayasari, R. (2021). Implementasi Algoritma Kriptografi Playfair Cipher untuk Mengamankan Data Aset. *Jurnal Informatika Polinema*, 7(2), 109-114.
- Suriadi, R., Satra, R., & Fattah, F. (2020). Peningkatan Keamanan Data dengan Menggunakan Equation pada Metode Playfair Cipher. *Buletin Sistem Informasi dan Teknologi Islam (BUSITI)*, 1(4), 266-269.
- Aini, F. N., Amiroch, S., & Chandra, N. E. (2020). Penggunaan Algoritma Vigenere Cipher dan RSA (Rivest-Shamir-Adleman) Untuk Keamanan Data Pembelian di PT Lamongan Marine Industry. *UJMC (Unisda Journal of Mathematics and Computer Science)*, 6(01), 39-46.
- Simbolon, Y. K. B. (2019). Perancangan Aplikasi Pengamanan File PDF Menggunakan Algoritma Playfair Cipher. *Informasi dan Teknologi Ilmiah (INTI)*, 6(3), 346-349.
- Surbakti, S. D. B. (2019). Implementasi Algoritma Playfair Cipher pada Penyandian Data. *Jurnal Teknik Informatika UNIKA Santo Thomas*, 4(2), 125-132.
- Eka, P. S. (2018). Implementasi Keamanan Data Menggunakan Algoritma Vernam Cipher Dan Playfair Cipher. *Pelita Informatika: Informasi dan Informatika*, 7(2), 193-198.

- Susanto, I. A., & Solichin, A. (2018). Enkripsi Data Penggajian Dengan Algoritma Caesar Cipher dan Vigenere Cipher Pada PT. Kemasindo Cepat Nusantara. *SKANIKA: Sistem Komputer dan Teknik Informatika*, 1(1), 399-404.
- Priyono, P. (2016). Penerapan Algoritma Caesar Cipher dan Algoritma Vigenere Cipher Dalam Pengamanan Pesan Teks. *JURIKOM (Jurnal Riset Komputer)*, 3(5).