Peningkatan Keamanan Pesan Teks Menggunakan Super Enkripsi Algoritma *Caesar Cipher Standard* dan *Vigenere Autokey*

Alfaruq Marsalsani Supriyatno dan Eka Ardhianto

Program Studi Teknik Informatika, Fakultas Teknologi Informasi dan Industri,
Universitas Stikubank, Semarang Jl. Tri Lomba Juang No. 1, Semarang
E-mail : fmarsalsani05@gmail.com, ekaardhianto@edu.unisbank.ac.id

Abstrak

Keamanan data merupakan hal yang penting untuk dijaga, terutama di era digital saat ini. Berbagai macam cara untuk menjaga keamanan dari sebuah data, Kriptografi adalah salah satu metode untuk menjaga keamanan data. Teknik enkripsi sendiri digunakan untuk menjaga data agar tetap terjaga keamanannya. Namun penggunaan konsep super enkripsi memberikan dampak terhadap peningkatan keamanan data. Tujuan dari penelitian ini adalah untuk meningkatkan algoritma Caesar Cipher Standar dengan gagasan tentang pendekatan super enkripsi. Untuk mencapai tujuan ini, metode yang digunakan adalah menggabungkan algoritma Caesar Cipher Standard dengan Vigenere Autokey sebagai metric performance digunakan perhitungan nilai entropi. Hasilnya menunjukkan peningkatan nilai entropi metode super enkripsi paling tinggi sebesar 63,2% dibandingkan dengan algoritma tunggal Caesar Cipher Standard sebelumnya yang hanya mendapatkan nilai paling tinggi sebesar 59,3%. Dengan demikian penggunaan teknik super enkripsi terbukti lebih efektif untuk mengamankan data dengan bukti memberikan dampak peningkatan persentase keamanan yang berarti data akan menjadi lebih aman dari serangan.

Kata kunci :Kriptografi, Super Enkripsi, Caesar Cipher Standard, Vigenere Autokey, Keamanan Pesan Teks.

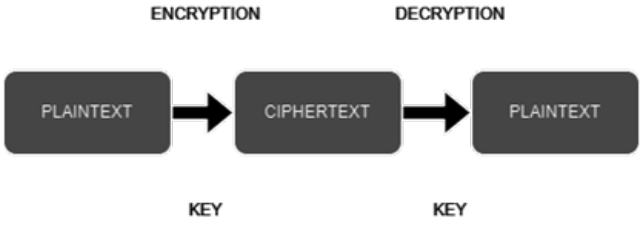
Pendahuluan

Salah satu instrumen penting di era digital saat ini adalah data. Menjaga keamanan data merupakan hal yang penting untuk dilakukan. Salah satu cara yang dapat dilakukan untuk menjaga keamanan data adalah melalui kriptografi [1]. Kriptografi merupakan ilmu yang mempelajari tentang cara menjaga kerahasiaan pesan. Terdapat dua proses dalam kriptografi yaitu enkripsi dan dekripsi. Enkripsi yaitu merubah pesan asli (plaintext) menjadi pesan acak (ciphertext). Dekripsi merupakan proses merubah pesan acak menjadi pesan asli. Penelitian ini menggunakan metode super enkripsi yang mana merupakan gabungan dari dua metode yang terdiri dari metode caesar cipher dan metode vigenere autokey [2].

Salah satu model kriptografi yang cukup bertahan lama adalah algoritma Vigenere atau dikenal sebagai Vigenere Cipher. Vigenere Cipher dipublikasikan pada tahun 1586 oleh Blaise de Vigenere yang pada saat itu digunakan untuk memproses pengamanan informasi dalam bentuk teks [3]. Menurut Widya Teffani Putri Caesar cipher merupakan salah satu algoritma cipher tertua dan paling diketahui dalam perkembangan ilmu kriptografi. Caesar cipher merupakan salah satu jenis cipher substitusi yang membentuk cipher dengan cara melakukan penukaran karakter pada plaintext menjadi tepat satu karakter pada ciphertext. Teknik seperti ini disebut juga sebagai cipher abjad tunggal [4].

Kriptografi berasal dari Yunani yaitu "cryptos" yang berhubungan dengan bidang matematika karena ada pengolahan angka dan huruf [5]. Teknik kriptografi digunakan untuk menangani masalah kebocoran data atau informasi karena menggunakan rumus matematika dari yang paling sederhana hingga paling kompleks [6]. Caesar Cipher Standard merupakan salah satu metode kriptografi paling sederhana yang termasuk dalam kategori cipher substitusi dan digunakan untuk mengenkripsi dan mendeskripsi teks [7]. Caesar Cipher adalah salah satu teknik kriptografi yang banyak digunakan, dimana setiap huruf pada plainteks digantikan dengan huruf lain dengan pergeseran sebanyak nilai kunci [8].

DOI : http://dx.doi.org/10.32409/jikstik.23.2.3602



Gambar 1: Proses Kriptografi Secara Umum. [Diadopsi dari : [9]]

Vigenere Cipher merupakan metode penyandian yang menggunakan kunci yang terdiri dari kata atau frase. Setiap huruf dienkripsi menggunakan algoritma Caesar Cipher dengan pergeseran yang berbeda sesuai dengan huruf kunci yang bersesuaian. Metode ini memberikan tingkat keamanan yang lebih tinggi dibandingkan dengan Caesar Cipher karena menggunakan variasi pergeseran [10].

Autokey Cipher adalah variasi dari Vigenere Cipher yang menggunakan teks terbuka sebagai bagian dari kunci. Hal ini memperbaiki kelemahan Vigenere Cipher terhadap analisis frekuensi, di mana kunci diulang secara periodik. Dengan menggunakan teks terbuka sebagai kunci, Auto Key Cipher menghasilkan kunci yang lebih sulit diprediksi [11]. Vigenere Autokey merupakan metode enkripsi yang memanfaatkan teks terbuka sebagai kunci secara otomatis. Prosesnya dimulai dengan menggunakan karakter teks terbuka sebagai kunci untuk menyandikan karakter pertama pesan, kemudian teks sandi yang dihasilkan digunakan sebagai kunci untuk karakter berikutnya [12].

Sebagai eksperimen awal dilakukan percobaan usulan sample data dengan ukuran 8 Byte, 16 Byte, 32 Byte, dan 64 Byte. Pada eksperimen awal diperoleh nilai entropi Algoritma Caesar Cipher Standard diperoleh bahwa nilai paling tinggi adalah 4,83806 atau 60,4757% serta rata-rata nilai entropi yang didapatkan adalah 4,77365 atau 59,6706% seperti yang tertera pada Tabel 1.

Tabel 1: Hasil Nilai Entropi Eksperimen Awal Menggunakan Caesar Cipher Standard

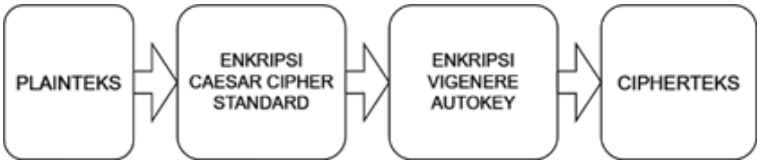
Ukuran Plainteks	Ukuran Cipherteks	Nilai Entropi
8 Byte	8 Byte	4,74584
16 Byte	16 Byte	4,83806
32 Byte	32 Byte	4,75762
64 Byte	64 Byte	4,75310
Rata-Rata Nilai Entropi		4,77365

Tujuan penelitian ini adalah untuk memperkuat algoritma Caesar Cipher Standard dengan konsep pendekatan super enkripsi. Sehingga data menjadi lebih sulit untuk diretas.

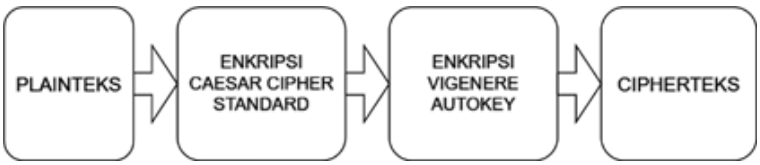
Metode Penelitian

Dari data eksperimen awal, maka diusulkanlah pengembangan eksperiman yang menggunakan gabungan dari dua algoritma yaitu penggabungan antara Caesar Cipher Standard dengan Vigenere Autokey. Dalam penelitian ini model yang diusulkan dibagi menjadi dua bagian yaitu model enkripsi dan deskripsi melalui perpaduan algoritma caesar cipher dan vigenere autokey.

Pada Gambar 2 proses mengubah plaintext menjadi ciphertext dilakukan melalui dua lapis proses enkripsi, yaitu enkripsi caesar cipher standard dan vigenere autokey. Terdapat beberapa komponen utama yang diperlukan dalam model enkripsi ini, yakni data awal dan kunci yang akan digunakan pada setiap lapisan proses enkripsi.



Gambar 2: Proses Enkripsi Algoritma Gabungan.



Gambar 3: Proses Dekripsi Algoritma Gabungan..

Model dekripsi merupakan kebalikan dari model proses enkripsi. Model ini bertujuan untuk mengembalikan data tersandi menjadi bentuk semula. Model dekripsi yang diusulkan dapat dilihat pada Gambar 3.

Pada Gambar 2 merupakan proses mengubah data plaintext menjadi data ciphertext melalui dua lapis proses enkripsi, yaitu Caesar Cipher Standard dan Vigenere Autokey. Komponen utama yang akan digunakan pada setiap lapisan enkripsi berupa plaintext dan kunci yang ditentukan oleh pengguna [1]. Tahap enkripsi pertama dengan Caesar Cipher, data akan dienkripsi dengan menggunakan algoritma Caesar Cipher Standard dengan menggunakan persamaan 1.

$$Ci = (Pi + Ki)\ mod\ 26 \tag{1}$$

dengan Ci adalah nilai desimal karakter ciphertext ke- i, Pi adalah nilai desimal karakter plaintext ke- i, Ki dan Ci adalah nilai desimal karakter kunci ke- i dan mod 26 merupakan jumlah dari keseluruhan abjad yang digunakan [14].

Tahap enkripsi kedua dengan Vigenere Autokey, data akan dienkripsi dengan menggunakan algoritma Vigenere Autokey dengan menggunakan persamaan pada Persamaan 2.

$$Ci = (Pi + Ki)\ mod\ m \tag{2}$$

dengan Ci adalah nilai desimal karakter ciphertext ke- i, Pi adalah nilai desimal karakter plaintext ke- i, Ki dan Ci adalah nilai desimal karakter kunci ke- i dan m merupakan jumlah dari keseluruhan karakter yang digunakan [13].

Pada Gambar 3 proses mengubah data ciphertext menjadi data plaintext melalui dua lapis proses dekripsi, yaitu Caesar Cipher Standard dan Vigenere Autokey. Komponen utama yang akan digunakan pada setiap lapisan dekripsi berupa ciphertext dan kunci yang ditentukan.

Tahap dekripsi pertama dengan Vigenere Autokey, berkebalikan dengan Persamaan (2) data akan didekripsi dengan menggunakan algoritma Vigenere Autokey dengan persamaan 3.

$$Pi = (Ci - Ki)\ mod\ m \tag{3}$$

dengan Pi adalah nilai desimal karakter Plaintext ke- i, Pi adalah nilai desimal karakter plaintext ke- i, Ki dan Ci adalah nilai desimal karakter kunci ke- i dan m merupakan jumlah dari keseluruhan karakter yang digunakan.

Tahap dekripsi kedua dengan Caesar Cipher Standard, berkebalikan dengan Persamaan (1) data akan didekripsi dengan menggunakan algoritma Caesar Cipher Standard dengan persamaan 4.

$$Pi = (Ci - Ki)\ mod\ 26 \tag{4}$$

dengan Pi adalah nilai desimal karakter Plaintext ke- i, Pi adalah nilai desimal karakter plaintext ke- i, Ki dan Ci adalah nilai desimal karakter kunci ke- i dan mod 26 merupakan jumlah dari keseluruhan karakter abjad yang ada.

Hasil dan Pembahasan

Penelitian ini melakukan eksperimen awal dan eksperimen pengembangan. Eksperimen awal dilakukan untuk melihat performa algoritma Caesar Cipher Standard yang telah ada. Nilai yang diperoleh seperti pada Tabel 1 digunakan sebagai pembanding pada nilai eksperimen pengembangan. Eksperimen dilakukan dengan menambahkan enkripsi Vigenere Autokey setelah proses enkripsi Caesar Cipher Standard selesai dilakukan.

Perhitungan nilai entropi informasi dilakukan dengan menggunakan Persamaan 5, dimana X adalah pesan, Si adalah simbol ke-i dalam pesan, $p(Si)$ adalah peluang kemunculan Si dan ai adalah jumlah kemunculan Si.

$$H(x) = \sum_{i=1}^{n} ai^2 log(p(S_i) \tag{5}$$

Berdasarkan Tabel 1 diambil beberapa sampel eksperimen untuk dijadikan tolak ukur sebagai hasil eksperimen awal, melihat dari ukuran plainteks dan cipherteks tidak ada perubahan ukuran file, maka dari itu dapat disimpulkan setelah penggunaan algoritma Caesar Cipher Standard ukuran file tidak berubah.

Tabel 2: Hasil Nilai Entropi Eksperimen Pengembangan Algoritma Kombinasi.

Ukuran Plainteks	Ukuran Cipherteks	Nilai Entropi
8 Byte	8 Byte	4,98248
16 Byte	16 Byte	5,06284
32 Byte	32 Byte	4,98589
64 Byte	64 Byte	4,97148
Rata-Rata Nilai Entropi		5,00067

Berdasarkan Tabel 2 ada beberapa sampel eksperimen yang berbeda hasilnya dari tolak ukur pada eksperimen awal, terlihat dari data bahwa nilai entropi yang dihasilkan pada setiap kali percobaan nilainya berbeda. Dalam eksperimen pengembangan ini menghasilkan nilai tertinggi sebesar 5,06284 atau 63,28% dan juga rata-rata nilai entropi sebesar 5,00067 atau jika dalam persentase 62,50%.

Dalam eksperimen ini, telah dijelaskan penerapan dua metode enkripsi, yaitu Caesar Cipher dan Vigenere Autokey, untuk meningkatkan keamanan data. Melalui uji coba dan analisis, dapat disimpulkan beberapa hal yang dapat membentuk dasar bagi penggunaan kedua teknik ini.

Dilihat dari nilai entropinya, algoritma Caesar Cipher Standard sudah termasuk dalam kategori aman meskipun konsepnya sederhana. Algoritma ini juga ternyata dapat memberikan lapisan keamanan yang memadai terhadap ancaman-ancaman dasar. Namun, keterbatasan metode ini terletak pada kerentanannya terhadap serangan, akibatnya memerlukan upaya lebih lanjut untuk mengatasi kelemahan tersebut.

Sementara itu, jika digabungkan dengan algoritma Vigenere Autokey memberikan tingkat keamanan yang lebih tinggi dengan bukti nilai entropi yang lebih besar dari sekedar algoritma Caesar Cipher Standard saja. Hal ini membuatnya lebih tahan terhadap serangan dibandingkan dengan Caesar Cipher Standard. Keunggulan Vigenere Auto-Key terutama terlihat dalam pengamanan data dengan panjang teks yang lebih besar.

Tabel 3: Perbandingan Nilai Entropi.

Ukuran Plainteks	Ukuran Cipherteks	Caesar Cipher Standard	Caesar Cipher Standard Dengan Vigenere Autokey
8 Byte	8 Byte	4,74584	4,98248
16 Byte	16 Byte	4,83806	5,06284
32 Byte	32 Byte	4,75762	4,98589
64 Byte	64 Byte	4,75310	4,97148
Rata-Rata Nilai Entropi		4, 77365	5, 00067

Tabel 4: Perbandingan Capaian Level Keamanan Informasi.

Ukuran Plainteks	Ukuran Cipherteks	Caesar Cipher Standard (%)	Caesar Cipher Standard Dengan Vigenere Autokey (%)
8 Byte	8 Byte	59,323	62,281
16 Byte	16 Byte	60,4757	63,2855
32 Byte	32 Byte	59,47025	62,323625
64 Byte	64 Byte	59,41375	62,1435
Rata-Rata Capaian Keamanan		59,6706	62,5084

Tabel 4 memperlihatkan nilai capaian level keamanan informasi dalam bentuk persentase (%) yang diperoleh pada eksperimen, capaian persentase keamanan data ini sendiri tidak bergantung pada ukuran dari suatu plainteks dalam percobaan kali ini. Dalam tabel 4 juga terlihat bahwa hasil percobaan pengembangan memiliki hasil rata-rata persentase capaian keamanan yang lebih tinggi dibandingkan hanya menggunakan satu algoritma Caesar Cipher saja. Lalu, capaian keamanan paling tinggi dihasilkan pada plainteks dengan ukuran 16 Byte dikarenakan nilai entropi pada sampel data tersebut merupakan yang paling tinggi sehingga lebih mendekati nilai ideal entropi yaitu 8, ini berarti informasi yang diamankan dapat dinilai aman. Jika nilai entropi pada eksperimen dibandingkan dengan nilai entropi maksimal, maka akan didapatkan nilai capaian dalam bentuk persentase. Rumus untuk menghitung persentase nilai entropi menggunakan persamaan pada Persamaan 6.

$$Presentase = \frac{S}{8} X\ 100\% \tag{6}$$

dengan S adalah nilai entropi yang akan akan dihitung sebagai persentase dari total nilai ideal entropi, sedangkan 8 adalah nilai entropi ideal. Sehingga jika ingin menghitung persentase capaian keamanan dibutuhkan nilai entropi dari hasil percobaan dibagi dengan nilai ideal entropi yaitu 8.

Nilai ini dapat dimaknai sebagai nilai capaian level keamanan informasi. Dengan capaian yang semakin mendekati 100% maka dapat dianggap bahwa metode yang diusulkan memiliki tingkat keamanan yang lebih kuat sehingga produk cipherteks yang dihasilkan akan lebih sulit untuk ditebak. Peningkatan nilai entropi ini memberikan makna bahwa plainteks dan cipherteks semakin berbeda dan tidak memiliki hubungan yang berarti. Pada eksperimen yang dilakukan, diperoleh nilai capaian level kea-

manan informasi tertinggi dalam algoritma kombinasi Caesar Cipher Standard dengan Vigenere Autokey sesuai dengan Persamaan (5) ialah 63,29 %. Hal ini dapat dikatakan bahwa kombinasi dua algoritma dapat mempengaruhi capaian tingkat keamanan yang lebih baik sehingga cipherteks yang dihasilkan akan semakin sulit ditebak oleh kriptanalis serta cipherteks memiliki ketidakterkaitan dengan plainteks yang lebih tinggi.

Penutup

Dari hasil eksperimen, Enkripsi Caesar Cipher Standard menunjukkan keandalan yang cukup, meskipun sederhana. Enkripsi ini dapat memberikan tingkat keamanan yang memadai, terutama jika diimplementasikan sebagai bagian dari sistem enkripsi yang lebih kompleks. Meskipun memiliki kerentanan terhadap serangan, keamanannya dapat diperkuat melalui penambahan lapisan keamanan tambahan.

Di lain sisi algoritma kombinasi, yang menggabungkan Caesar Cipher Standard dengan Vigenere Autokey, membuktikan peningkatan signifikan dalam tingkat keamanan dengan nilai entropi keseluruhan yang lebih tinggi. Kombinasi ini, terutama efektif dalam mengamankan data dengan panjang teks yang lebih besar, menawarkan keunggulan dibandingkan dengan penggunaan hanya Caesar Cipher Standard. Oleh karena itu, kombinasi dua algoritma ini dapat menjadi pilihan yang bagus untuk melindungi data dengan tingkat keamanan yang lebih tinggi. Dalam memilih metode enkripsi, perlu diperhatikan konteks penggunaan dan kebutuhan keamanan spesifik. Enkripsi Caesar Cipher Standard dapat memberikan solusi yang memadai dalam beberapa skenario, sementara kombinasi dengan Vigenere Auto Key menjadi opsi yang lebih baik dalam meningkatkan keamanan data secara keseluruhan.Dengan peningkatan nilai entropi yang diperoleh maka informasi atau pesan yang dienkripsi akan semakin acak sehingga akan semakin sulit ditebak dan dipecahkan.

Meskipun temuan dalam eksperimen ini menjadi lebih baik dari versi sebelumnya, namun eksperimen ini masih terbatas pada bentuk informasi berbasis teks. Sebagai bahan pertimbangan kelanjutan riset perlu pengembangan dengan menggunakan bentuk informasi berbasis piksel, suara, gelombang radio serta melakukan kombinasi dengan algoritma lain untuk pencapaian keamanan informasi maksimal.

Daftar Pustaka

[1] Muhammad Fadlan, Haryansyah dan Rosmini, “Pengamanan Data melalui Model Super Enkripsi Autokey Cipher dan Transposisi Kolom”, Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), vol. 5, no. 6, pp. 1113–1119, doi: 10.29207/resti.v5i6.3566, Dec. 2021.

[2] A.Zulfatul, “Enkripsi dan deskripsi pesan menggunakan metode vigenere cipher dan route cipher”, Disertasi Universitas Islam Negeri Maulana Malik Ibrahim, 2021.

[3] E. Ardhianto, W. T. Handoko, E. Supriyanto dan D. H. (n.d.) Murti, "Evolusi Cipher Vigenere dalam Peningkatan Pengamanan Informasi”, Jurnal Informatika UPGRISVol. 7, No .2, 2021.

[4] R. Widia Asiani dan I. Yanti, “Penerapan Kriptografi Caesar Cipher Dan Hill Cipher dalam Pengiriman Pesan Rahasia Sebagai Media Pembelajaran Matematika Realistik Pada Materi Modulo”, Jurnal Ilmu Perpustakaan dan Informasi, vol. 6, no. 1, 2022.

[5] S. P. Peniel Sam, “Analisis Vigenere Cipher Dalam Tulisan Nama Mahasiswa Di Hasil Ujian Akhir Semester Ganjil T.A 2023/2024”, Journal of Social Science Research, vol. 3, no. 5, 2023.

[6] V. M. Hidayah, D. Iskandar Mulyana dan Y. Bachtiar, “Algoritma Caesar Cipher atau Vigenere Cipher pada Pengenkripsian Pesan Teks”, Journal on Education, vol. 05, no. 03, pp. 8563–8573, 2023.

[7] Febrianingsih, R.dan Hafiz, A. (n.d., “Implementasi Kriptografi Berbasis Caesar Chiper untuk Keamanan Data” , In Jurnal Informasi Dan Komputer, Vol. 7, 2019.

[8] Mesran dan N. Surya Darma “Peningkatan Keamanan Kriptografi Caesar Cipher dengan Menerapkan Algoritma Kompresi “Stout Codes””, Jurnal Rekayasa sistem dan Teknologi Informasi, vol. 4, no. 6, 2020.

[9] GN Salmi dan F Siagian. "Implementation of the data encryption using caesar cipher and vernam cipher methods based on CrypTool2”, Journal of Soft Computing Exploration, Vol. 3, No.2, pp: 99-104, 2022.

[10] M.D. Irawan, "Implementasi Kriptografi Vigenere Cipher Dengan Php”, (JurTI) Jurnal Teknologi Informasi, Vol. 1, No.1, pp: 11-21, 2017.

[11] M. Fadlan, R. Rosmini dan H. Haryansyah, “Perpaduan Algoritma Kriptografi Atbash dan Autokey Cipher dalam Mengamankan Data”, Jurnal Media Informatika Budidarma, vol. 5, no. 3, p. 806, doi: 10.30865/mib.v5i3.3019, Jul. 2021.

[12] C. Irawan dan D. R. I. Moses Setiadi, "Implementasi ALgoritma Autokey Cipher dan AES-128 Pada Enkripsi File”, Prosiding SENDI_U, ISBN: 978-979-3649-99-3, 2019.

[13] P. Priyono, "Penerapan Algoritma Caesar Cipher dan Algoritma Vigenere Cipher Dalam Pengamanan Pesan Teks", JURIKOM (Jurnal Riset Komputer), Vol. 3, No.5, 2016.

[14] R. Pratiwi, L. C. Utami dan R. B. Sakti, "Perancangan Keamanan Data Pesan Dengan Menggunakan Metode Kriptografi Caesar Cipher", Bulletin of Information Technology (BIT), vol. 3, no. 4, pp. 367–373, doi: 10.47065/bit.v3i1, 2022.