PENINGKATAN KEAMANAN DATA MELALUI TEKNIK SUPER ENKRIPSI MENGGUNAKAN ALGORITMA VIGENERE DAN CAESAR

Eko Nur Wahyudi[1], Eka Ardhianto[2], Widiyanto Tri Handoko[3], Hari Murti[4], Edy Supriyanto[5], Endang Lestariningsih[6], Rara Sriartati Redjeki[7]

[1] Program Studi Manajemen Informatika, Fakultas Vokasi, Universitas Stikubank,
[2 3 6] Program Studi Teknik Informatika, Fakultas Teknologi Informasi dan Industri, Universitas Stikubank,
[4 5 7] Program Studi Sistem Informasi, Fakultas Teknologi Informasi dan Industri, Universitas Stikubank,
[1]eko@edu.unisbank.ac.id, [2]ekaardhianto@edu.unisbank.ac.id, [3]wthandoko@edu.unisbank.ac.id,
[4]harimurti@edu.unisbank.ac.id, [5] edy_supriyanto@edu.unisbank.ac.id,
[6]endanglestariningsih@edu.unisbank.ac.id, [7]rara_artati@edu.unisbank.ac.id

Abstrak

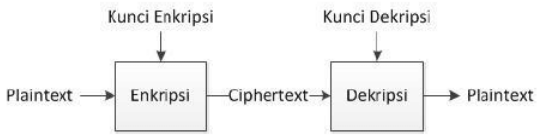
Keamanan data penting untuk dijaga, terutama di era digital ini. Salah satu cara untuk menjaga keamanan data adalah enkripsi. Teknik enkripsi digunakan untuk melindungi data. Penggunaan konsep super-enkripsi memberikan efek peningkatan keamanan informasi. Tujuan dari penelitian ini adalah untuk memperkuat algoritma Caesar Cipher Standard dengan konsep super-enkripsi, dimana teknik yang diterapkan adalah kombinasi algoritma Caesar Cipher Standard dengan Vigenere Autokey sebagai ukuran kinerja menggunakan perhitungan entropi. Sebagai metrik performansi digunakan nilai entropi yang menyatakan Tingkat keamanan data. Berdasarkan hasil yang diperoleh, nilai entropi usulan metode super enkripsi lebih baik yaitu 4,972, lebih baik dari sebelumnya yaitu 4,689. Nilai yang diperoleh menunjukkan peningkatan yang signifikan dengan capaian tingkat keamanan hingga 62,15% dibanding sebelumnya 58,62%. Ukuran file cipherteks dan ukuran file plainteks pada eksperimen ini tidak mengalami perubahan, sehingga menghemat sumberdaya media penyimpanan. Selain itu berdasarkan eksperimen yang dilakukan nilai ukuran file optimal untuk melakukan ekripsi adalah 16 kilobyte dengan nilai entropi tertinggi adalah 5,095. Dengan demikian, penggunaan teknik super enkripsi untuk melindungi data mampu memberikan keamanan yang lebih baik.

Kata kunci : vigenere autokey, caesar cipher, super enkripsi, entropi, keamanan data.

1. Pendahuluan

Data dianggap sebagai aset vital perusahaan di era teknologi saat ini. Menjaga keamanan informasi merupakan suatu hal yang penting. Salah satu cara untuk menjaga keamanan informasi adalah enkripsi (Muhammad Fadlan et al., 2021). Kriptografi adalah ilmu menjaga kerahasiaan pesan. Kriptografi memiliki dua proses yaitu enkripsi dan dekripsi. Enkripsi berarti mengubah pesan asli plainteks (*plaintext*) menjadi pesan acak cipherteks (*ciphertext*). Dekripsi adalah konversi pesan acak menjadi pesan asli. Kriptografi berasal dari bahasa Yunani yaitu "*cryptos*" yang merujuk pada bidang matematika karena berhubungan dengan angka dan huruf (Maulana et al., 2023; Ridho et al., 2023). Teknik kriptografi digunakan untuk menyelesaikan masalah kebocoran informasi atau informasi karena menggunakan rumus matematika dari yang paling sederhana hingga yang paling rumit (Hidayah et al., 2023).

Proses kriptografi secara umum ditunjukkan pada gambar 1. Pada proses ini plainteks digunakan sebagai input pesan yang akan dirahasiakan. Kunci enkripsi digunakan sebagai kunci dalam proses enkripsi. Proses enkripsi melakukan penyandian dan mengubah plainteks yang dapat dipahami menjadi cipherteks yang tidak memiliki makna. Proses dekripsi menggunakan kunci dekripsi untuk membuat cipherteks. Dalam konteks ini pesan menjadi tidak bermakna dan aman selama menajdi cipherteks.



Gambar 1. Proses Kriptografi secara Umum.

Caesar cipher merupakan salah satu algoritma enkripsi tertua dan paling terkenal dalam perkembangan kriptografi. Sandi Caesar adalah jenis sandi substitusi yang membentuk sandi dengan mengganti karakter teks biasa dengan tepat satu karakter sandi. Teknik seperti ini disebut juga enkripsi satu huruf (Ardhianto et al., 2021). *Caesar Cipher Standard* adalah salah satu metode enkripsi

paling sederhana, yang termasuk dalam kelas sandi substitusi dan digunakan untuk mengenkripsi dan mendekripsi teks (Febrianingsih & Hafiz, 2019). *Caesar Cipher* adalah teknik enkripsi yang banyak digunakan di mana setiap huruf dari teks biasa diganti dengan huruf lain dengan transfer nilai kunci (Mesran & Nasution, 2020).

Selain *Caesar Cipher*, algoritma berbasis teks lain adalah Algoritma Vigenere atau sandi Vigenere. Sandi Vigenere diterbitkan oleh *Blaise de Vigenere* pada tahun 1586 dan digunakan untuk memproses informasi yang dilindungi dalam bentuk teks pada saat itu (Ardhianto et al., 2021). Vigenere Cipher adalah metode enkripsi yang menggunakan kunci yang terdiri dari kata atau frase. Setiap huruf dienkripsi menggunakan algoritma Caesar cipher dengan offset yang berbeda-beda sesuai dengan huruf kunci yang bersangkutan. Metode ini menawarkan tingkat keamanan yang lebih tinggi dibandingkan dengan *cipher Caesar* karena menggunakan varian offset (Irawan, 2017).

Vigenere telah dilakukan pengembangan menjadi beberapa varian, salah satunya adalah *Vigener Autokey* atau *Cipher Autokey*. *Vigenere Autokey* merupakan varian dari cipher Vigenere yang menggunakan teks biasa sebagai bagian dari kuncinya. Hal ini memperbaiki kelemahan sandi Vigenere dalam analisis frekuensi, di mana kunci diulang secara berkala. Dengan menggunakan plaintext sebagai kuncinya, enkripsi kunci otomatis menghasilkan kunci yang lebih sulit diprediksi (Fadlan et al., 2021). *Vigenere Autokey* adalah metode enkripsi yang secara otomatis menggunakan teks biasa sebagai kuncinya. Prosesnya dimulai dengan menggunakan plaintext untuk mengenkripsi karakter pertama pesan sebagai kunci, setelah itu ciphertext yang dihasilkan digunakan sebagai kunci untuk karakter berikutnya (Irawan, 2017).

Kombinasi vigenere dengan Caesar dilakukan secara umum untuk meningkatkan keamanan pesan teks. Penelitian terhadap pengamanan pesan teks dan simbol dilakukan dengan mengkombinasi vigenere standar dan cipher Caesar untuk memberikan keamanan ganda terhadap pesan (Hardita & Sholeha, 2021). Pada penelitian ini, bentuk cipherteks yang digunakan adalah berupa simbol bukan karakter. dengan demikian proses enkripsi yang dilakukan adalah mensubstitusi karakter pesan kedalam bentuk simbol, sehingga lebih sulit di maknai oleh pihak yang tidak berwenang.

Penggunaan kombinasi Caesar dan vigenere juga dilakukan pada penelitian (Setyawati, 2021). Penelitian ini melakukan perhitungan secara manual dan komputerisasi antara proses kombinasi Caesar dan Vigenere. Hasil yang diperoleh pada penelitian ini adalah bahwa percobaan yang dilakukan menghasilkan nilai yang sama. Bentuk cipherteks yang dihasilkan dari penggabungan model Caesar dan vigenere tidak terdapat perubahan.

Penelilian terhadap algoritma enkripsi dan dekripsi hybrid yang menggabungkan konsep algoritma Caesar Cipher dan Vigenere Cipher. Hal ini dilakukan dengan membandingkan desain yang diusulkan dengan beberapa cipher terkenal seperti Hill Cipher, Caesar Cipher dan Vigenere Cipher melalui simulasi MATLAB. Parameter seperti frekuensi huruf dan perilaku grafik dievaluasi pada penelitian ini. Hasil menunjukkan bahwa algoritma yang diusulkan mempunyai kinerja yang sangat baik. Hasil penelitian ini memiliki grafik yang terdistribusi paling merata diantara cipher-cipher lain dibandingkan dalam hal frekuensi ciphertextnya (Tan et al., 2021).

Pada penelitian sebelumnya, permasalahan yang ada adalah bahwa penggunaan sample tidak merepresentasikan kondisi nyata dalam komunikasi pesan antara pengirim dan penerima. Selain itu, bentuk keamanan yang disajikan tidak pernah dinyatakan dalan notasi kuantitatif, sehingga secara kualitatif hanya disajikan dalam bentuk penjelasan deskriptif.

Pada eksperimen ini, sebagai penelitian eksperimen awal, ukuran file sampel dataset adalah berbeda-beda, mulai dari 1 KB sampai dengan 128 KB. Penggunaan ukuran yang berbeda ini dimaksudkan untuk mengakomodasi kemungkinan variasi file yang terdapat dalam transaksi data sebenarnya. Jumlah percobaan yang dilakukan dalam eksperimen awal adalah 20 kali untuk setiap sampel dan diambil nilai rata-rata entropi untuk setiap sampel. Dalam eksperimen awal adalah 4,838 pada ukuran sampel 16 KB. Untuk rata-rata entropi pada eksperimen awal adalah 4,689 dengan tingkat keamanan 58,62%. Jika dilihat ukuran file plainteks dan file cipherteks, algoritma Caesar Cipher tidak terdapat perubahan.

Penelitian ini bertujuan meningkatkan tingkat keamanan *Caesar Cipher* menggunakan metode super enkripsi. Metode super enkripsi adalah teknik mengamankan data menggunakan lebih dari satu algoritma (Bahri et al., 2023; Falensky & Pakereng, 2022). Pada penelitian ini, eksperimen dilakukan menggunakan algoritma *Caesar Cipher* digabungkan dengan Algoritma *Vigenere Autokey*.

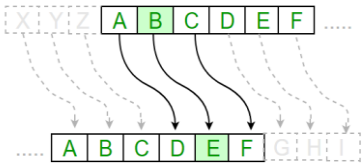
2. Metode

2.1 Caesar Cipher

Caesar cipher merupakan salah satu algoritma enkripsi tertua dan paling terkenal dalam perkembangan kriptografi. Sandi Caesar adalah jenis sandi substitusi yang membentuk sandi dengan mengganti karakter teks biasa dengan tepat satu karakter sandi. Teknik seperti ini juga disebut enkripsi *monoalphabetic* (Asiani & Yanti, 2022). Gambar 2 menunjukkan piringan Caesar yang digunakan untuk melindungi data. *Caesar Cipher Standard* adalah salah satu metode enkripsi paling sederhana, yang termasuk dalam kelas sandi

substitusi dan digunakan untuk mengenkripsi dan mendekripsi teks (Febrianingsih & Hafiz, 2019). Caesar Cipher adalah teknik enkripsi yang banyak digunakan di mana setiap huruf dari teks biasa diganti dengan huruf lain dengan transfer nilai kunci (Mesran & Nasution, 2020). Gambar 3 menunjukkan proses transisi karakter pada *Caesar Cipher*.

Gambar 2. Cakram *Caesar Cipher*.



Gambar 3. Pergeseran Karakter dalam Caesar Cipher

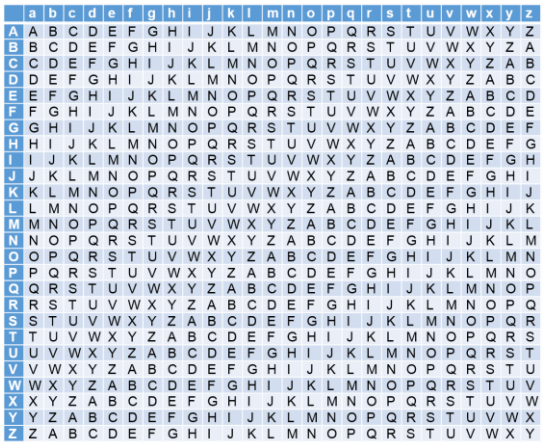
Enkripsi *Caesar Cipher* menggunakan persamaan 1. Sedangkan proses dekripsi dilakukan menggunakan persamaan (2). Simbol *Ci* adalah nilai desimal karakter *ciphertext* ke-*i*, *Pi* adalah nilai desimal karakter *plaintext* ke-*i*, *Ki* dan *Ci* adalah nilai desimal karakter kunci ke-*i* dan mod 26 merupakan jumlah dari keseluruhan abjad yang digunakan (Pratiwi et al., 2022).

$$Ci=(Pi+Ki) \bmod 26 \quad (1)$$

$$Pi=(Ci+Ki) \bmod 26 \quad (2)$$

2.2 Vigenere Autokey

Vigenere juga digolongkan sebagai algoritma substitusi polialfabet yang menggunakan pemetaan posisi karakter, dimana setiap karakter ditransformasikan oleh salah satu dari beberapa *cipher-shift* yang ditentukan dengan kunci (*key*) (Ardhianto et al., 2024). Vigenere pada secara umum digunakan untuk memproses informasi teks, baik dalam pesan yang akan dirahasiakan juga penggunaan kuncinya. Kunci dalam vigenere jika memiliki panjang kurang dari pesan yang akan dirposes, maka kunci tersebut akan digunakan secara berulang sampai teks pesan terproses seluruhnya. Dalam penggunaannya Vigenere mirip seperti penggunaan Caesar dengan mengikuti pergeseran kunci yang disesuaikan untuk mendapatkan karakter cipher. Gambar 4 memperlihatkan tabel Vigenere versi 26 x 26 karakter. Sebagai contoh plainteks: ILIKEGOOGLE, dan kunci: ZFLT. cipherteks yang terbentuk adalah: HQTDDLZHFQP, proses ini diperlihatkan pada tabel 1.



Gambar 4. Tabel Vigenere.

Tabel 1. Contoh Proses Enkripsi Vigenere.

	Urutan Karakter										
	1	2	3	4	5	6	7	8	9	10	11
Plainteks	I	L	I	K	E	G	O	O	G	L	E
Kunci	Z	F	L	Z	F	L	Z	F	L	Z	F
Ciperteks	H	Q	T	D	D	L	Z	H	F	Q	P

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 (Fadlan et al., 2021). 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 (Irawan, 2017).

Vigenere Autokey dienkripsi dengan menggunakan menggunakan persamaan pada persamaan (3). Persamaan (4) adalah proses dekripsi algoritma *Vigenere Autokey*. Simbol *Ci* adalah nilai desimal karakter *ciphertext* ke- *i*, *Pi* adalah nilai desimal karakter p*laintext* ke- *i*, *Ki* dan *Ci* adalah nilai desimal karakter kunci ke- *i* dan *m* merupakan jumlah dari keseluruhan karakter yang digunakan (Priyono, 2017).

$$Ci=(Pi+Ki) \bmod m \quad (3)$$

$$Pi=(Ci-Ki) \bmod m \quad (4)$$

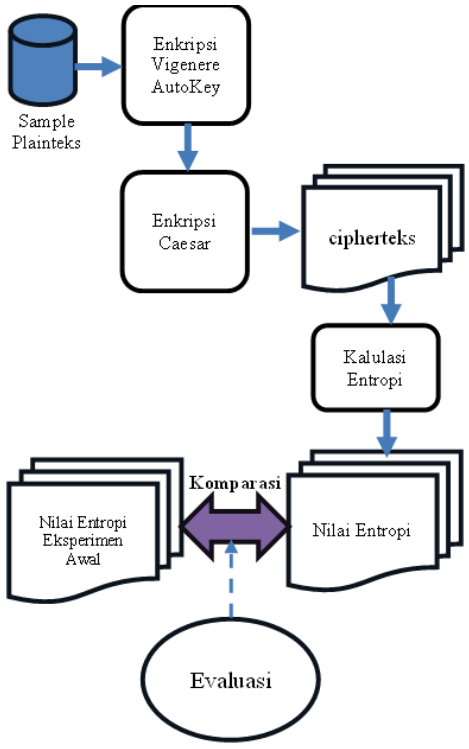
2.3 Desain Penelitian

Penelitian ini bersifat eksperimental. Sebagai sampel digunakan dataset astronomer telegram yang berisi laporan singkat pengamatan astronomi yang dikirimkan melalui aplikasi telegram. Pelaksanaan

penelitian ini digambarkan dalam desain penelitian yang terlihat pada gambar 5.

Dari gambar 5 dapat dijelaskan bahwa, penelitian ini melakukan eksperimen awal untuk mendapatkan nilai pembanding sebagai bentuk metrik performansi. Nilai metrik yang digunakan adalah nilai entropi yang dihitung menggunakan persamaan (5).

Eksperimen lanjutan dilakukan dengan menerapkan konsep super enkripsi menggunakan dua algoritma. Algoritma yang digunakan adalah algoritma *vigenere autokey* yang digabung dengan algoritma *Caesar cipher*. Pada gambar 3, terlihat susunan desain penelitian berupa eksperimen pengamanan data menggunakan dua algoritma. Pada eksperimen ini penggunaan algoritma pertama adalah *vigenere autokey* yang kemudian dilanjutkan dengan algoritma *Caesar cipher*. Hasil yang diperoleh dalam eksperimen adalah bentuk cipherteks dari sample plainteks. cipherteks yang diperoleh dari hasil eksperimen selanjutnya dihitung nilai entropi menggunakan persamaan (5).



Gambar 5. Desain Penelitian

Pada bagian evaluasi, proses komparasi dilakukan dengan cara membandingkan nilai entropi eksperimen awal dan nilai entropi pada eksperimen penerapan super enkripsi. Hasil yang diperoleh selanjutnya dihitung nilai siginfikasninya menggunakan kalkulator *mannwhitney*. Perhitungan siginfikasni menggunakan kalkulator online yang dapat diakses pada laman website https://www.socscistatistics.com/tests/mannwhitney/default3.aspx.

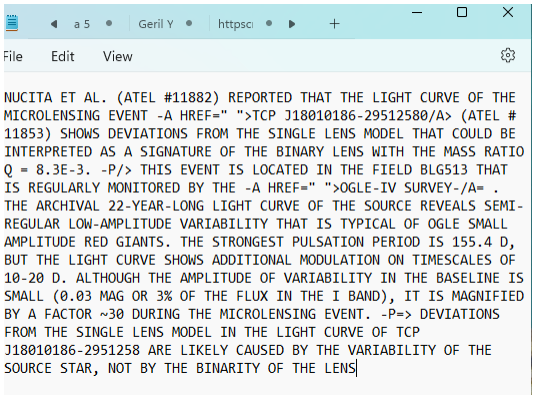
2.4 Evaluasi

Dalam bidang teori informasi, nilai entropi yang tinggi mewakili keacakan yang sebenarnya. Masalah keamanan informasi yang timbul dari pengaruh entropi yang tidak mencukupi menunjukkan bahwa keacakan yang cukup penting dari sudut pandang keamanan. Entropi digunakan untuk mengukur keacakan data, yang mencerminkan kekuatan algoritma enkripsi (Ardhianto et al., 2024). Semakin tinggi nilai entropinya, semakin acak datanya. Sehingga dapat mempengaruhi ketahanan algoritma terhadap serangan hacker. Persamaan (5) digunakan untuk menghitung entropi.

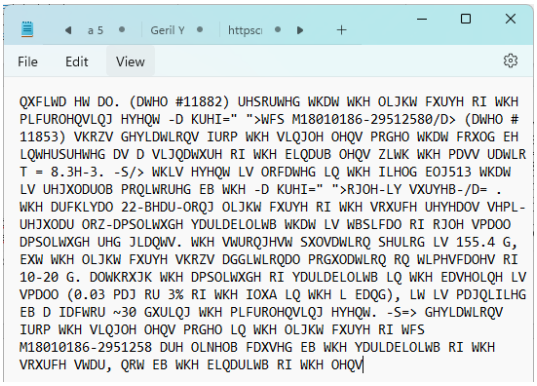
$$H_m = \sum_{i=0}^{2^n} P(m_i) \log_2 \frac{1}{P(m_i)} \qquad (5)$$

3. Hasil dan Pembahasan

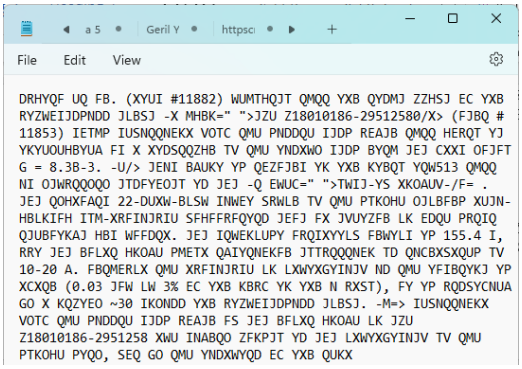
Pada eksperimen ini digunakan sampel dengan beberapa ukuran seperti pada tabel 2. Eksperimen dilakukan dengan memproses sampel dengan enkripsi Vigenere Autokey dan dilanjutkan dengan enkripsi Caesar. Bentuk perubahan plainteks menjadi cipherteks akhir digambarkan pada gambar 6, 7, dan 8. Gambar 6 adalah contoh bentuk plainteks pesan, gambar 7 adalah bentuk karakter cipherteks pada eksperimen awal, dan gambar 8 memperlihatkan hasil cipherteks akhir hasil eksperimen.



Gambar 6. Sampel Karakter Plainteks



Gambar 7. Bentuk Karakter Ciupherteks pada Eksperimen Awal



Gambar 8. Bentuk Cipherteks Akhir Hasil Eksperimen

Pada eksperimen awal, digunakan *dataset* dari telegram astronomer yang berisi informasi hasil pengamatan astronomi yang dikirim melalui telegram. Tabel 2 memperlihatkan nilai entropi dari dataset yang dienkripsi menggunakan *Caesar Cipher*.

Tabel 2. Hasil Eksperimen Awal

Ukuran Plainteks (KB)	Ukuran Cipherteks (KB)	Nilai Entropi Rata-rata
1	1	4,577
2	2	4,639
3	3	4,577
4	4	4,576
5	5	4,591
6	6	4,689
7	7	4,663
8	8	4,746
9	9	4,727
10	10	4,735
16	16	**4,838**
32	32	4,758
64	64	4,753
128	128	4,783
Rata-rata entropi		4,689

Pada eksperimen awal, ukuran file sampel dataset adalah berbeda-beda, mulai dari 1 KB sampai dengan 128 KB. Penggunaan ukuran yang berbeda ini dimaksudkan untuk mengakomodasi kemungkinan variasi file yang terdapat dalam transaksi data sebenarnya. Jumlah percobaan yang dilakukan dalam eksperimen awal adalah 20 kali untuk setiap sampel dan diambil nilai rata-rata entropi untuk setiap sampel.

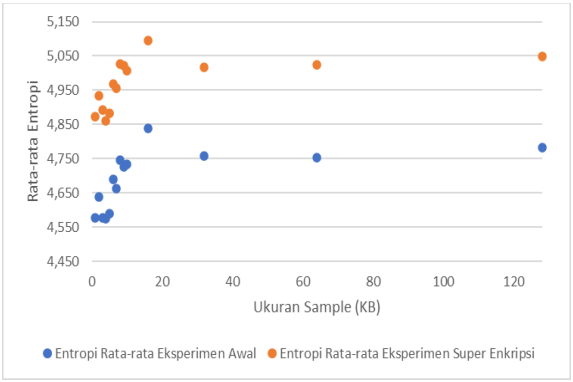
Dari tabel 2, dapat dilihat bahwa nilai entropi tertinggi dalam eksperimen awal adalah 4,838 pada ukuran sampel 16 KB. Untuk rata-rata entropi pada eksperimen awal adalah 4,689 dengan tingkat keamanan 58,62%. Jika dilihat ukuran file plainteks dan file cipherteks, algoritma Caesar Cipher tidak terdapat perubahan.

Ekeperimen penerapan super enkripsi menggunakan algoritma *Vigenere Autokey* dan *Caesar cipher* menunjukkan hasil seperti terlihat pada tabel 3. Pada tabel 3 terlihat perbedaan nilai entropi rata-rata setiap sampel. Penggunaan ukuran sampel yang berbeda-beda diperlukan untuk merepresentasikan beberapa ukuran file yang mungkin terdapat dalam pengiriman data pada keadaan sebenarnya. Pada eksperimen ini, ukuran sampel yang digunakan adalah 1 kilobyte hingga 128 kilobytes. Visualisasi dari tabel 3 diperlihatkan pada gambar 9.

Tabel 3. Nilai Entropi Rata-Rata Hasil Eksperimen

Ukuran Plainteks (KB)	Ukuran Cipherteks (KB)	Nilai Entropi Rata-rata Eksperimen Awal	Nilai Entropi Rata-rata hasil Eksperimen
1	1	4,577	4,873
2	2	4,639	4,934
3	3	4,577	4,893
4	4	4,576	4,860
5	5	4,591	4,883
6	6	4,689	4,969
7	7	4,663	4,956
8	8	4,746	5,026
9	9	4,727	5,021
10	10	4,735	5,008
16	16	**4,838**	**5,095**
32	32	4,758	5,016
64	64	4,753	5,023
128	128	4,783	5,049
Rata-rata entropi		4,689	**4,972**

Dari tabel 3, dapat dilihat bahwa terdapat peningkatan nilai entropi dari eksperimen sebelumnya. Pada eksperimen penerapan super enkripsi nilai entropi lebih tinggi dari nilai entropi eksperimen awal. Rata-rata nilai entropi pada eksperimen penerapan super enkripsi menunjukkan nilai 4,972 yang lebih tinggi dari eksperimen awal yaitu 4,689. Jika dibandingkan dengan nilai entropi optimum, maka nilai rata-rata entropi pada eksperimen awal adalah 58,62%, sedangkan nilai enrtopi rata-rata pada eksperimen super enkripsi adalah 62,15%. Nilai rata-rata entropi eksperimen super eknkripsi meningkat 6% dari rata-rata eksperimen awal. Gambar 9 memperlihatkan perbandingan nilai entropi rata-rata setiap sampel yang digunakan. Terlihat bahwa nilai entropi rata-rata lebih tinggi dari nilai entropi rata-rata pada eksperimen awal.



Gambar 9. Grafik Perbandingan Nilai Entropi Rata-Rata

Dari tabel 3 dan gambar 7, terlihat bahwa nilai rata-rata entropi pada ekperimen awal dan eksperimen super enkripsi yang paling tinggi adalah pada sample dengan ukuran 16 kilobyte yaitu 4,838 meningkat menjadi 5.095. Dengan demikian dapat disarankan untuk mengoptimalkan penggunaan teknik super enkripsi *Vigenere Autokey* dan *Caesar Cipher* adalah pada ukuran data 16 kilobytes.

Perhitungan perbandingan ukuran file cipherteks dan plainteks juga dilakukan untuk melihat kapasitas file yang dihasilkan dari penerapan teknik super enkripsi. Pada eksperimen ini terlihat pada tabel 3 bahwa antara ukuran file plainteks dan file cipherteks tidak mengalami perubahan. Hal ini dapat diartikan bahwa penggunaan teknik super enkripsi *Vigenre Autokey* dan *Caesar Cipher* tidak memerlukan ukuran media penyimpanan yang lebih besar untuk menampung hasil proses enkripsi.

Untuk melihat tingkat signifikansi peningkatan nilai entropi digunakan perhitungan *U-Test Mann-Whitney* menggunakan kalkulator online pada laman https://www.socscistatistics.com/tests/mannwhitney/default3.aspx. pada perhitungan ini digunakan nilai rata-rata entropi pada setiap ukuran file sampel. Tabel 4 memperlihatkan hasil perhitungan *U-Test Mann-Whitney*.

Tabel 4. Perhitungan Siginifkansi Hasil

	Eksperimen Awal	**Eksperimen Super Enkripsi**	**Kombinasi**
Jumlah Rangking	105	301	406
Rata-rata Rangking	7,5	21,5	14,5
Nilai Harapan	203	203	
Rata rata	14,5	14,5	14,5
Nilai U	196	0	
Nilai Harapan	98	98	
Standard Deviasi			**21, 7639**
Nilai Z			**4,4799**

Dari tabel 4, terlihat bahwa nilai U eksperimen super enkripsi lebih rendah dari nilai kritis yaitu 42. Dengan tingkat signifikasi 0.01. Nilai Z yang diperoleh adalah 4,4799, dan nilai P adalah dibawah 0.0001 dengan tingkat signifikasn 0.01. dengan demikian dapat disimpulkan bahwa nilai rata-rata entropi eksperiman super enkripsi memiliki perbdaan signifikansi. Sehingga cipherteks yang dihasilkan menjadi lebih sulit dipecahkan oleh pihak yang tidak berwenang.

4. Kesimpulan dan Saran

Dari eksperimen yang dilakukan dapat ditarik simpulan bahwa dengan menggunakan teknik super enkripsi terdapat peningkatan nilai entropi dari 4,689 menjadi 4,972. Dengan demikian terdapat peningkatan keamanan data yang dienkripsi menggunakan teknik super enkripsi gabungan Vigenere Autokey dan Caesar Cipher. Dari eksperimen juga di peroleh bahwa ukuran file plainteks dan ukuran file cipherteks tidak terdapat perbedaan. Hal ini dapat diartikan bahwa untuk mengamankan data menggunakan teknik super enkripsi Vigenere Autokey dan Caesar Cipher tidak perlu mempersiapkan media penyimpanan yang lebih besar dari ukuran plainteks, sehingga menghemat sumber daya yang dimiliki. Berdasar perhitungan nilai signifikasni, terdapat perbedaan antara hasil ekperimen awal dan eksperimen super enkripsi. Hal ini juga terlihat bahwa terdapat peningkatan sebesar 6% dari nilai capaian entropinya. Hal ini dapat diartiken bahwa peningkatan yang terjadi berpengaruh pada kekuatan data yang diamankan menggunakan teknik super enkripsi. Dengan adanya peningkatan yang siginifikan maka data yang diamankan akan menjadi lebih sulit ditebak dan dipecahakn oleh pihak yang tidak berhak.

Dari sisi percobaan yang dilakukan pada setiap sample terlihat bahwa ukuran file plainteks yang memiliki nilai entropi paling tinggi adalah file berukuran 16 kilobyte. Dengan demikian, sebagai saran pengoptimaslisasian penggunan tekni super enkripsi *Vigenere Autokey* dengan *Caesar Cipher* adalah pada file dengan ukuran 16 kilobyte.

Daftar Pustaka:

Ardhianto, E., Handoko, W. T., Supriyanto, E., & Murti, H. (2021). Evolusi Cipher Vigenere dalam Peningkatan Pengamanan Informasi. *Jurnal Informatika Upgris*, *7*(2), 23–27.

Ardhianto, E., Redjeki, R. S., Supriyanto, E., Murti, H., & Wahyudi, E. N. (2024). Adopsi Generator Kunci Euler Number dan Pembangkit Kunci Blum Blum Shub untuk Meningkatkan Confidentiality Level pada Extended Vigenere. *Infotek : Jurnal Informatika Dan Teknologi*, *7*(1), 1–11. https://doi.org/10.29408/jit.v7i1.21512

Asiani, R. W., & Yanti, I. (2022). Penerapan Kriptografi Caesar Cipher Dan Hill Cipher dalam Pengiriman Pesan Rahasia Sebagai Media Pembelajaran Matematika Realistik Pada Materi Modulo. *Baitul 'Ulum: Jurnal Ilmu Perpustakaan Dan Informasi*, *6*(1), 79–97.

Bahri, S., Jihan, F., & Rudianto, B. (2023). IMPLEMENTASI ALGORITMA SUPER ENKRIPSI VIGENERE CIPHER DAN ROUTE CIPHER PADA PENYANDIAN PESAN TEKS. *Jurnal Matematika UNAND*, *12*(2), 168–175.

Fadlan, M., Rosmini, R., & Haryansyah, H. (2021). Perpaduan Algoritma Kriptografi Atbash dan Autokey Cipher dalam Mengamankan Data. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, *5*(3), 806. https://doi.org/10.30865/mib.v5i3.3019

Falensky, L. V., & Pakereng, M. A. I. (2022). PENGAMANAN DATA PASIEN DI UPT. PUSKESMAS PUJON KALIMANTAN TENGAH MENGGUNAKAN KRIPTOGRAFI SUPER ENKRIPSI. *J-SAKTI (Jurnal Sains Komputer & Informatika)*, *6*(2), 711–725.

Febrianingsih, R., & Hafiz, A. (2019). IMPLEMENTASI KRIPTOGRAFI BERBASIS CAESAR CHIPER UNTUK KEAMANAN DATA. *Jurnal Informasi Dan Komputer*, *7*(2), 81–86. https://doi.org/10.35959/jik.v7i2.163

Hardita, V. C., & Sholeha, E. W. (2021). PENERAPAN KOMBINASI METODE VIGENERE CIPHER, CAESAR CIPHER DAN SIMBOL BACA DALAM MENGAMANKAN PESAN. *Jurnal SAINTEKOM*, *11*(1). https://doi.org/10.33020/saintekom.v11i1.202

Hidayah, V. M., Mulyana, D. I., & Bachtiar, Y. (2023). Algoritma Caesar Cipher atau Vigenere Cipher pada Pengenkripsian Pesan Teks. *Journal on Education*, *5*(3), 8563–8573. https://doi.org/10.31004/joe.v5i3.1647

Irawan, M. D. (2017). IMPLEMENTASI KRIPTOGRAFI VIGENERE CIPHER DENGAN PHP. *JURNAL TEKNOLOGI INFORMASI (JurTI)*, *1*(1), 11–21.

Maulana, D. K., Tanjung, S. M., Ritonga, R. S., & Ikhwan, A. (2023). Penerapan Kriptografi Vigenere Cipher Pada Kekuatan Kata Sandi. *Jurnal Sains Dan Teknologi (JSIT)*, *3*(1), 47–52. https://doi.org/10.47233/jsit.v3i1.483

Mesran, M., & Nasution, S. D. (2020). Peningkatan Keamanan Kriptografi Caesar Cipher dengan Menerapkan Algoritma Kompresi Stout Codes. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *4*(6). https://doi.org/10.29207/resti.v4i6.2730

Muhammad Fadlan, Haryansyah, & Rosmini. (2021). Pengamanan Data melalui Model Super Enkripsi Autokey Cipher dan Transposisi Kolom. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *5*(6), 1113–1119. https://doi.org/10.29207/resti.v5i6.3566

Pratiwi, R., Utami, L. C., Bima Sakti, R., & Triase. (2022). Perancangan Keamanan Data Pesan Dengan Menggunakan Metode Kriptografi Caesar Cipher. *Bulletin of Information Technology (BIT)*, *3*(4), 367–373. https://doi.org/10.47065/bit.v3i4.420

Priyono, P. (2017). PENERAPAN ALGORITMA CAESAR CIPHER DAN ALGORITMA VIGENERE CIPHER DALAM PENGAMANAN PESAN TEKS. *JURIKOM (Jurnal Riset Komputer)*, *3*(5), 351–356.

Ridho, A., Mutia, C., & Putri, A. (2023). Konsep Three-Pass Protocol Pengamanan Teks Menggunakan Metode Playfair Cipher Dengan Gronsfeld Cipher. *Technologia : Jurnal Ilmiah*, *14*(1), 27. https://doi.org/10.31602/tji.v14i1.9236

Setyawati, N. Y. (2021). Modifikasi Kriptografi Klasik Kombinasi Metode Vigenere Cipher dan Caesar Cipher. *Journal of Smart System*, *1*(1), 1–8. https://doi.org/10.36728/jss.v1i1.1601

Tan, C. M. S., Arada, G. P., Abad, A. C., & Magsino, E. R. (2021). A Hybrid Encryption and Decryption Algorithm using Caesar and Vigenere Cipher. *Journal of Physics: Conference Series*, *1997*(1), 012021. https://doi.org/10.1088/1742-6596/1997/1/012021