IMPLEMENTASI KOMBINASI CAESAR CIPHER, VIGENÈRE CIPHER, DAN VIGENÈRE AUTOKEY PADA APLIKASI WEB CATATAN HARIAN UNTUK MENINGKATKAN KEAMANAN PENYIMPANAN DATA

1. Pendahuluan

Dalam lanskap teknologi informasi kontemporer, data telah bertransformasi menjadi aset krusial, baik bagi individu maupun entitas bisnis(Simatupang & Khairil, 2022). Peningkatan signifikan dalam nilai data ini diiringi pula oleh eskalasi ancaman keamanan siber, termasuk insiden peretasan kredensial dan pencurian informasi sensitif yang dapat merusak stabilitas finansial dan reputasi(Simatupang & Khairil, 2022). Kriptografi, sebagai disiplin ilmu yang mendedikasikan diri pada penyembunyian pesan rahasia, memegang peranan vital dalam menjamin **kerahasiaan** (*confidentiality*) dan **integritas** data(Setyawati et al., 2021).

Meskipun standar industri saat ini didominasi oleh kriptografi modern (seperti protokol HTTPS) untuk transmisi data dalam aplikasi web, terdapat kebutuhan berkelanjutan untuk mengeksplorasi mekanisme keamanan *lightweight* atau lapisan pertahanan sekunder pada titik-titik kritis sistem(Menggunakan et al., 2021).

Kriptografi klasik, seperti Caesar Cipher dan Vigenère Cipher, secara individual rentan terhadap kriptanalisis, terutama analisis frekuensi(Sutoyo & Murhaban, 2016). Fenomena ini memicu penelitian yang mengkombinasikan ketiganya (melalui varian Vigenère Autokey) dalam konsep **super enkripsi** atau **product cipher**(Menggunakan et al., 2021). Dengan menggabungkan substitusi monoalfabetik (Caesar) dengan substitusi polialfabetik (Vigenère/Vigenère Autokey), dihipotesiskan mampu meningkatkan *confusion* dan *diffusion* data, menjadikannya lebih tahan terhadap serangan dibandingkan jika diterapkan secara tunggal(Menggunakan et al., 2021). Peningkatan keamanan relatif ini, terutama jika diukur menggunakan metrik kuantitatif seperti **Entropi**, dapat menawarkan solusi yang efisien secara komputasi untuk pengamanan data tekstual, seperti **catatan harian** yang memerlukan **kerahasiaan penyimpanan data**. Justifikasi penerapan kombinasi algoritma klasik dalam studi ini adalah untuk menganalisis pemanfaatan efisiensi komputasi yang tinggi, menjadikannya menarik untuk arsitektur *lightweight* pengamanan penyimpanan data(Menggunakan et al., 2021).

Tujuan utama dari studi literatur ini adalah menganalisis dan menyintesis hasil-hasil penelitian yang mengimplementasikan teknik kombinasi Caesar Cipher, Vigenère Cipher, dan Vigenère Autokey.

2. Konsep Dasar Kriptografi

Dalam kriptografi, perlindungan data diwujudkan melalui pemenuhan beberapa aspek dasar, antara lain: **Kerahasiaan** (*Confidentiality*), **Integritas** (*Integrity*), **Autentikasi** (*Authentication*), dan **Kontrol Akses** (*Access Control*)(Sutoyo & Murhaban, 2016). Kombinasi Caesar Cipher dan Vigenère Cipher dalam penelitian ini terutama berfokus pada peningkatan **Kerahasiaan** data.

Algoritma Kriptografi Klasik

Secara umum, kriptografi klasik menggunakan dua teknik utama:

- **Substitusi (Penggantian):** Proses penggantian karakter pada pesan asli (*plaintext*) dengan karakter berbeda untuk menghasilkan pesan tersandi (*ciphertext*)(Setyawati et al., 2021).
- **Transposisi (Pengubahan Posisi):** Proses penataan ulang atau pengubahan susunan/posisi karakter dalam pesan asli(Setyawati et al., 2021).

Caesar Cipher

Caesar Cipher digolongkan sebagai sandi substitusi **monoalfabetik**(Menggunakan et al., 2021; Simatupang & Khairil, 2022). Mekanismenya sangat sederhana: setiap huruf dari pesan asli diganti dengan huruf lain melalui pergeseran nilai kunci (*shift operation*) yang sama untuk semua karakter(Simatupang & Khairil, 2022).

Vigenère Cipher dan Vigenère Autokey

Vigenère Cipher adalah metode sandi substitusi **polialfabetik** yang lebih maju(Setyawati et al., 2021; Simatupang & Khairil, 2022). Jika pesan melebihi panjang kunci, kunci akan diulang kembali (*key periodicity*)(Simatupang & Khairil, 2022). Vigenère Cipher dianggap lebih aman daripada Caesar Cipher karena menggunakan varian *offset* yang bervariasi(Menggunakan et al., 2021; Simatupang & Khairil, 2022).

- **Varian Vigenère Autokey:** Metode ini menggunakan *plaintext* itu sendiri sebagai bagian dari kunci, yang secara efektif menghilangkan kelemahan utama Vigenère standar, yaitu perulangan kunci secara berkala, sehingga kunci menjadi lebih sulit diprediksi(Menggunakan et al., 2021).

Jenis Kombinasi (Super Enkripsi)

Super Enkripsi (*Product Cipher*) adalah teknik keamanan data yang menggunakan dua atau lebih algoritma kriptografi secara berurutan(Menggunakan et al., 2021; Simatupang & Khairil, 2022).

- **Mekanisme Kombinasi:** Kombinasi ini bertujuan untuk menerapkan dua prinsip keamanan kunci:
    - **Confusion:** Dicapai terutama melalui Vigenère Cipher (atau Vigenère Autokey), yang memperumit hubungan antara kunci dan *ciphertext*(Menggunakan et al., 2021).
    - **Diffusion:** Dicapai melalui aplikasi algoritma kedua (Caesar Cipher), yang menyebarkan pengaruh satu karakter *plaintext* ke banyak karakter *ciphertext*(Menggunakan et al., 2021).
- **Contoh Proses Berurutan:** Proses kombinasi yang umum digunakan adalah **enkripsi beruntun**(Setyawati et al., 2021; Simatupang & Khairil, 2022).
    - *Plainteks* dienkripsi menggunakan *Vigenère Cipher* (menghasilkan *Cipherteks 1*)(Setyawati et al., 2021; Simatupang & Khairil, 2022).
    - *Cipherteks 1* kemudian dijadikan *Plainteks* untuk dienkripsi oleh *Caesar Cipher* (menghasilkan *Cipherteks Akhir*)(Setyawati et al., 2021; Simatupang & Khairil, 2022).

Kombinasi ini diklaim menghasilkan tingkat keamanan yang lebih baik dibandingkan penerapan masing-masing metode secara terpisah(Simatupang & Khairil, 2022).

3. Tinjauan Penelitian Terdahulu

Peneliti & Tahun	**Metode / Algoritma**	**Tujuan Penelitian**	**Hasil Kunci dan Temuan**	**Kelemahan / Keterbatasan**
Wahyudi et al. (2024)	Caesar Cipher Standard + **Vigenère Autokey** (Super	Memperkuat Caesar Cipher dengan *super enkripsi*, diukur menggunakan Entropi[cite: 313].	Peningkatan Entropi signifikan (dari 4,689 menjadi **4,972**), peningkatan keamanan **6%**[25252525]. Ukuran file tidak	Fokus pada peningkatan entropi; tidak mengukur ketahanan terhadap

	Enkripsi) [cite: 313, 377]		berubah, optimal pada data 16 KB[cite: 318, 576, 579].	kriptanalisis frekuensi atau kecepatan transmisi data di lingkungan web secara spesifik.
Setyawati et al. (2021)	Kombinasi Vigenère Cipher (Text Key) dan Caesar Cipher (Geser Angka Key) [cite: 14, 15]	Memberikan prosedur keamanan data teks; membandingkan hasil manual dan program[cite: 16].	Hasil konsisten 100% hingga 5000 karakter [cite: 18, 31], namun **memerlukan input huruf kapital** untuk kesamaan hasil manual dan program[26262626].	Keterbatasan krusial pada penanganan karakter (hanya huruf kapital) yang tidak sesuai untuk implementasi web modern (set karakter penuh)[cite: 263].
Sutoyo & Murhaban (2016)	Kombinasi Caesar Chiper (Tahap 1) dan Vigenère Chiper (Tahap 2) [cite: 682, 691]	Mengkombinasikan algoritma klasik untuk pesan rahasia dan meningkatkan ketahanan terhadap *brute force*[cite: 691, 968].	Kombinasi sulit dipecahkan dengan *brute force* dibandingkan tunggal[cite: 968]. Proses dekripsi terbalik berhasil[cite: 869, 949].	Hanya menyatakan sulit dipecahkan secara kualitatif, tanpa metrik kuantitatif kinerja atau keamanan.
Simatupang & Khairil (2022)	Kombinasi Vigenère Cipher (Tahap 1) dan Caesar Cipher (Tahap 2) [cite: 1243]	Pengamanan dokumen teks dan evaluasi fungsional sistem[cite: 1061].	Hasil enkripsi/dekripsi normal[cite: 1247]. Kriptografi simetris **memerlukan kunci yang sama** untuk dekripsi[cite: 1000, 1248].	Tidak menyajikan metrik performa (kecepatan atau entropi); fokus pada fungsionalitas, bukan pada arsitektur penyimpanan data web.

4. Analisis dan Sintesis

Tren Evolusi Algoritma

Analisis dari penelitian terdahulu menunjukkan adanya pergeseran dari algoritma klasik tunggal yang rentan (seperti Caesar Cipher) menuju solusi **super enkripsi** (kombinasi) sebagai upaya untuk meningkatkan keamanan(Menggunakan et al., 2021).

- **Peningkatan Kuantitatif:** Penelitian terbaru (Wahyudi et al.) telah berpindah dari klaim keamanan kualitatif (sulit dipecahkan) menjadi pembuktian keamanan **kuantitatif** melalui metrik Entropi(Menggunakan et al., 2021).

- **Fokus pada Varian Kunci:** Penggunaan **Vigenère Autokey** dalam kombinasi menunjukkan tren upaya mengatasi kelemahan klasik, di mana *plaintext* dijadikan bagian dari kunci untuk menghilangkan perulangan kunci yang periodik(Menggunakan et al., 2021).

Perbandingan Performa (Kecepatan vs Keamanan)

- **Keamanan (Entropi):** Tingkat keamanan kombinasi ini (Entropi rata-rata **4,972**) lebih tinggi **6%** daripada Caesar Cipher tunggal (4,689)(Menggunakan et al., 2021).
- **Kecepatan dan Sumber Daya:** Ukuran *ciphertext* tidak berubah dibandingkan *plaintext*[31313131]. Hal ini berarti C+V **menghemat sumber daya media penyimpanan** dan *bandwidth* transmisi data(Menggunakan et al., 2021).

Celah Penelitian (*Research Gap*)

Analisis literatur mengidentifikasi celah utama yang membatasi penerapan C+V secara luas:

1. **Keterbatasan Lingkup Karakter Set:** Beberapa studi terdahulu (Setyawati et al. 2021) menemukan bahwa algoritma kombinasi hanya berfungsi optimal atau konsisten jika **input plaintext menggunakan huruf kapital** (*mod 26*)(Setyawati et al., 2021). Hal ini menjadi **celah krusial** karena data **catatan harian** umumnya mencakup set karakter penuh (huruf besar, huruf kecil, angka, simbol).
2. **Tantangan Manajemen Kunci Simetris untuk Penyimpanan Data:** Sifat simetris C+V mengharuskan kunci yang sama untuk enkripsi dan dekripsi(Simatupang & Khairil, 2022; Sutoyo & Murhaban, 2016). Analisis menegaskan bahwa dekripsi tidak akan berhasil jika kunci berbeda(Simatupang & Khairil, 2022).

5. Arah dan Peluang Penelitian

- **Analisis Komparatif Algoritma C+V *Extended***: Melakukan studi komparatif dan validasi teoritis terhadap kecepatan komputasi C+V (yang dimodifikasi untuk mendukung set karakter penuh) dibandingkan dengan algoritma *lightweight* modern yang sudah mapan(Menggunakan et al., 2021).
- **Studi Kelayakan Arsitektur Kriptografi Hibrida:** Merancang dan menganalisis secara teoritis model arsitektur keamanan *hybrid* yang secara eksplisit mengatasi kelemahan distribusi kunci simetris C+V. Studi ini akan berfokus pada potensi penggunaan C+V sebagai mesin enkripsi data masal yang cepat, dengan pertukaran kunci yang dijamin oleh algoritma asimetris (seperti RSA atau ECC)(Sutoyo & Murhaban, 2016).
- **Kriptanalisis Lanjutan terhadap C+V Autokey:** Melakukan studi teoritis mendalam untuk mengukur batas keamanan praktis dari **super enkripsi** C+V (terutama varian Autokey) terhadap serangan kriptanalisis frekuensi yang lebih canggih.

6. Kesimpulan

Studi literatur ini mengkonfirmasi bahwa penerapan teknik **Super Enkripsi** yang menggabungkan Caesar Cipher dan Vigenère Cipher, terutama varian Autokey, berhasil meningkatkan keamanan secara terukur dibandingkan dengan penggunaan *cipher* klasik tunggal(Menggunakan et al., 2021). Temuan kuantitatif kunci dari penelitian acuan menunjukkan peningkatan nilai Entropi rata-rata, dari 4,689 (Caesar Cipher Standard) menjadi **4,972** (Super Enkripsi C+V Autokey), yang merefleksikan peningkatan tingkat keamanan relatif sebesar **6%**(Menggunakan et al., 2021). Peningkatan ini

mendukung analisis C+V sebagai solusi **kriptografi ringan yang efisien untuk meningkatkan keamanan penyimpanan data teks** seperti **catatan harian**.

Justifikasi utama pemilihan jurnal acuan terletak pada fokus mereka pada **kuantifikasi dan pembuktian empiris** dari *super enkripsi* klasik(Menggunakan et al., 2021). Studi yang mengungkap kelemahan praktis implementasi klasik, yaitu keterbatasan pada **huruf kapital** saja, menciptakan **celah penelitian** yang harus diatasi(Setyawati et al., 2021). Selain itu, penegasan sifat simetris C+V **menyoroti perlunya studi teoritis tentang tantangan manajemen kunci**(Simatupang & Khairil, 2022; Sutoyo & Murhaban, 2016).

7. Daftar Pustaka

Menggunakan, E., Vigenere, A., & Caesar, D. A. N. (2021). *Peningkatan Keamanan Data Melalui Teknik Super*. 315–322. https://doi.org/10.33795/jip.v10i3.5131

Setyawati, N. Y., Khofid, A. N., Rund, A. U. ., & Wati, V. (2021). Modifikasi Kriptografi Klasik Kombinasi Metode Vigenere Cipher dan Caesar Cipher (Modification of Classical Cryptography Combination of the Vigenere Cipher and Caesar Cipher Methods). *Journal of Smart System*, *1*(1), 1–8. https://ejournal.utp.ac.id/index.php/JSS/article/download/1601/520521268/

Simatupang, L. D., & Khairil, K. (2022). Pengamanan Dokumen Teks Dengan Menerapkan Kombinasi Algoritma Kriptografi Klasik. *Jurnal Teknik Informatika UNIKA Santo Thomas*, *07*, 133–140. https://doi.org/10.54367/jtiust.v7i1.1998

Sutoyo, M. N., & Murhaban, M. (2016). Kombinasi Algoritma Kriptografi Caesar Chiper dan Vigenere Chiper Untuk Keamanan Data. *Jurnal Mekanova*, *2*(2), 58–66. http://download.garuda.kemdikbud.go.id/article.php?article=1101128&val=16540&title=Kombinasi%20Algoritma%20Kriptografi%20Caesar%20Chiper%20dan%20Vigenere%20Chiper%20Untuk%20Keamanan%20Data