STUDI LITERATURE

Analisis Keamanan Vigenère Cipher terhadap serangan Kriptografi klasik dan modern

Mata Kuliah : Kriptografi

Dosen Pengampu : JEFRY SUNUPURWA ASRI , S.kom., M.kom.

Nama :

Fitra Candra Ramadhani (20230801202)

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS ESA UNGGUL

2025

1. Pendahuluan

Dalam era digital, keamanan data menjadi kebutuhan utama dalam sistem informasi. Pertukaran data antarjaringan dan komunikasi daring menuntut adanya mekanisme perlindungan agar informasi tidak disalahgunakan. Kriptografi merupakan fondasi utama dalam menjaga kerahasiaan data dan komunikasi digital. Sebelum munculnya algoritma modern seperti AES dan RSA, metode enkripsi klasik telah digunakan secara luas, salah satunya adalah Vigenère Cipher.

Vigenère Cipher merupakan algoritma klasik yang menggunakan teknik substitusi polialfabetik dengan kunci berulang untuk menyandikan pesan. Walaupun tergolong sederhana, algoritma ini memiliki nilai historis penting dan sering menjadi dasar pemahaman konsep kriptografi simetris. Namun, dengan berkembangnya teknologi dan meningkatnya kemampuan komputasi, berbagai penelitian berusaha untuk memperkuat algoritma ini melalui modifikasi dan penggabungan dengan algoritma modern.

Tujuan dari studi literatur ini adalah untuk menganalisis tingkat keamanan Vigenère Cipher, mengidentifikasi serangan yang efektif, serta mengeksplorasi potensi penguatan algoritma melalui pendekatan modern seperti dynamic key dan hybrid encryption.

2. Konsep Dasar Kriptografi

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara mengubah informasi asli (plaintext) menjadi bentuk tidak bermakna (ciphertext). Tujuan utama kriptografi meliputi kerahasiaan (confidentiality), integritas (integrity), autentikasi (authentication), dan non-repudiation.

Jenis-jenis kriptografi:
- Symmetric key: AES, DES, Blowfish, ChaCha20
- Asymmetric key: RSA, ECC
- Hash function: SHA, MD5
- Hybrid cryptosystem: kombinasi antara simetris dan asimetris
- Protokol kriptografi: SSL/TLS, PGP

Tabel berikut menunjukkan perbandingan singkat beberapa jenis algoritma kriptografi:

Jenis Algoritma	**Kunci**	**Keamanan**	**Contoh Aplikasi**
Vigenère	Simetris	Lemah (klasik)	Edukasi, latihan dasar
AES	Simetris	Kuat (modern)	Enkripsi data
RSA	Asimetris	Kuat, lambat	Pertukaran kunci

ECC	Asimetris	Sangat kuat	IoT, mobile security

Vigenère Cipher menggunakan kunci berulang dalam proses enkripsi dan dekripsi. Rumus enkripsi: $C_i = (P_i + K_i) \bmod 26$ dan dekripsi: $P_i = (C_i - K_i) \bmod 26$. Walaupun lebih kompleks dibandingkan Caesar Cipher, pola kunci berulang tetap menjadi celah yang dapat dieksploitasi dengan metode analisis frekuensi dan serangan Kasiski.

3. Tinjauan Penelitian Terdahulu

Bagian ini memaparkan hasil penelitian terdahulu yang berfokus pada penguatan algoritma Vigenère Cipher melalui berbagai pendekatan.

Peneliti & Tahun	**Sumber / Jurnal**	**Metode / Fokus**	**Hasil & Temuan**	**Kelemahan / Keterbatasan**
(Neri et al., 2019)	WCSE Proceedings	Evaluasi keamanan modifikasi Vigenère	Meningkatkan resistensi terhadap serangan klasik	Dataset kecil
(Hameed & Sadeeq, 2022)	IJEECS	Pembangkitan kunci baru	Meningkatkan entropi dan keamanan cipher	Belum diuji pada cipher modern
(Hananto et al., 2019)	Semantic Scholar	Analisis efektivitas metode Kasiski	Efektif untuk kunci pendek	Tidak mencakup modifikasi modern
(Labady et al., 2024)	QJOEST Journal	Enhanced Vigenère Cipher untuk IoT	Lebih tahan terhadap serangan klasik	Belum diuji pada sistem besar
Pratama (Studi et al., 2007)	Neliti	Modifikasi menggunakan Catalan Number	Ciphertext lebih acak dan kuat	Belum diuji secara matematis mendalam

4. Analisis dan Sintesis

Berdasarkan hasil penelitian, tren utama peningkatan keamanan Vigenère Cipher terletak pada pengembangan metode pembangkitan kunci dinamis dan penggabungan algoritma klasik dengan algoritma modern. Pendekatan hybrid encryption dinilai mampu meningkatkan entropi kunci dan mengurangi pola berulang yang menjadi titik lemah cipher klasik. Selain itu, beberapa penelitian mulai mengarah pada penerapan Vigenère Cipher di bidang IoT dan sistem mobile dengan penyesuaian agar lebih efisien.

5. Arah dan Peluang Penelitian

1. Pengembangan adaptive key generation berbasis waktu atau hash.
2. Implementasi hybrid encryption berbasis Vigenère dan AES untuk sistem komunikasi sederhana.
3. Pengembangan lightweight encryption berbasis Vigenère untuk perangkat IoT.
4. Penggunaan machine learning untuk mendeteksi pola serangan terhadap cipher klasik.

6. Kesimpulan

Berdasarkan literatur yang dikaji, Vigenère Cipher masih relevan untuk konteks edukatif dan riset dasar. Meskipun tergolong lemah terhadap serangan klasik seperti frequency analysis dan Kasiski, berbagai modifikasi dan pendekatan hybrid terbukti mampu meningkatkan tingkat keamanannya. Penelitian selanjutnya dapat difokuskan pada integrasi algoritma ini dalam lingkungan komputasi terbatas seperti IoT, dengan perhatian khusus pada efisiensi daya dan kecepatan proses enkripsi.

7. Daftar Pustaka (APA 7th Edition)

Hameed, T. H., & Sadeeq, H. T. (2022). *Modified Vigenère cipher algorithm based on new key generation method*. *28*(2), 954–961. https://doi.org/10.11591/ijeecs.v28.i2.pp954-961

Hananto, A. L., Solehudin, A., Susilo, A., Irawan, Y., & Priyatna, B. (2019). *Analyzing the Kasiki Method Against Vigenere Cipher Abstract : November*. https://doi.org/10.29126/23942231/IJCT-V6I6P2

Labady, A., Hawkat, S. A. S., & Drees, T. F. A. (2024). *ENHANCED VIGENERE CIPHER ALGORITHM FOR IMPROVED CRYPTOGRAPHIC SECURITY*. *6*(1), 1–12.

Neri, D. A., Sison, A. M., & Medina, R. P. (2019). *Performance Analysis of the Modified Vigenere Algorithm to Secure Data*. *794*, 15–17. https://doi.org/10.18178/wcse.2019.06.117

Studi, P., Informatika, T., Tinggi, S., & Adisutjipto, T. (2007). *METODE CATALAN NUMBER DAN DOUBLE COLUMNAR*. 31–40.