J-ENSISTEC (Journal of Engineering and Sustainable Technology)
Vol. 12|No. 01, December 2025
ISSN : 2477-359X (Online)
ISSN: 2407-6007 (Print)
pp. 10315-10322

IMPLEMENTASI BRUTE FORCE ATTACK TERHADAP VIGENERE CIPHER: PENGARUH PANJANG KUNCI DAN PANJANG TEKS

Yandi Anzari[1], Aulia Rachmawati[2], Muhammad Damas Fatih[3], Pariyadi[4]
[1,2,3,4]Program Studi Sistem Informasi, Fakultas Sains Teknik, Universitas Jambi
Email: yandi.anzari@unja.ac.id

ABSTRACT

The Vigenere Cipher, although historically significant, remains vulnerable to modern brute force attacks. This study aims to empirically measure how key length and text length independently influence the time required to break the cipher using brute force methods. A pure experimental approach was applied through four test scenarios that combined two key lengths (L=3 and L=5) and two plaintext lengths (22 and 420 characters). The experiments were implemented in Python on a controlled computing environment to ensure result consistency. The findings show that key length has an exponential impact on decryption time, where increasing the key from three to five characters extended the execution time by approximately 370 times. In contrast, text length had a linear effect, with a 19-fold increase in characters leading to only about a 20-fold increase in processing time. In conclusion, the study confirms that cryptographic resistance in the Vigenere Cipher is primarily determined by key length, while text length only increases the computational workload proportionally. Future research is suggested to apply similar brute force analyses to other classical ciphers and explore larger key lengths to model performance limits more comprehensively.

Keywords: *Brute Force Attack, Key Length, Time Complexity, Vigenere Cipher.*

Riwayat Artikel :
Tanggal diterima : 03-10-2025
Tanggal revisi : 12-11-2025
Tanggal terbit : 08-12-2025

DOI :
https://doi.org/10.31949/j-ensitec.v12i01.16393

1. PENDAHULUAN

Kriptografi klasik memiliki peran fundamental dalam membangun dasar keamanan informasi modern. Pemahaman terhadap konsep enkripsi, dekripsi, dan kriptanalisis menjadi kunci untuk memahami bagaimana sistem keamanan digital berkembang dari metode konvensional ke sistem modern yang lebih kompleks (Purwanti et al., 2024). Salah satu metode kriptografi klasik yang paling berpengaruh adalah Vigenère Cipher, yang termasuk dalam kategori polyalphabetic substitution cipher (ALABADY et al., 2025). Algoritma ini dikembangkan untuk mengatasi kelemahan cipher monoalfabetik yang rentan terhadap analisis frekuensi huruf tunggal. Dengan pola substitusi yang bergantung pada kunci berulang, Vigenère menghasilkan tingkat kompleksitas enkripsi yang cukup tinggi dan selama beberapa abad dianggap hampir tidak dapat dipecahkan (Gomez et al., 2018).

Selain itu, beberapa studi di Indonesia juga telah membandingkan kinerja algoritma Vigenère dengan algoritma kriptografi modern seperti RSA, menunjukkan perbedaan tingkat keamanan dan efisiensi dalam konteks pengolahan data digital (Sopiandi & Jabbar, n.d.).

Meskipun sederhana dan historis, Vigenère Cipher memiliki kelemahan mendasar terhadap metode kriptanalisis

modern seperti Brute Force Attack (BFA) (Hadi et al., 2024). Serangan brute force dilakukan dengan menguji seluruh kemungkinan kombinasi kunci hingga ditemukan hasil dekripsi yang cocok dengan plaintext asli. Kompleksitas waktu serangan ini dapat dimodelkan sebagai $O(|P|.26^L)$ di mana |P| adalah Panjang teks dan L adalah panjang kunci (Guglani, n.d.-a). Model tersebut menunjukkan bahwa waktu pemecahan cipher sangat dipengaruhi oleh dua faktor utama: panjang kunci dan panjang teks.

Faktor pertama, panjang kunci (L), menentukan ukuran ruang pencarian (keyspace) yang harus dieksplorasi selama proses brute force. Semakin panjang kunci, maka jumlah kombinasi meningkat secara eksponensial, sehingga memperbesar waktu komputasi secara signifikan (Hassan, 2024a). Penelitian terbaru menunjukkan bahwa peningkatan panjang kunci memberikan efek langsung terhadap peningkatan kompleksitas pemecahan (Sebhatu, n.d.-a), sementara beberapa modifikasi algoritmik berusaha memperluas ruang kunci untuk meningkatkan ketahanan enkripsi (Chemlal et al., 2025; Vatshayan et al., 2020).

Faktor kedua, panjang teks (|P|), berpengaruh secara linier terhadap waktu pemrosesan, karena setiap percobaan kunci harus melewati seluruh karakter teks yang diuji. Penelitian oleh G. H. Tuga dan P. Cubero (Tuga et al., n.d.-a) menunjukkan bahwa peningkatan panjang plaintext secara proporsional memperpanjang waktu dekripsi. Temuan ini diperkuat oleh studi lain yang membandingkan waktu eksekusi antara cipher klasik dan modern, di mana peningkatan jumlah karakter berdampak langsung pada total waktu serangan brute force (Adhitya et al., 2024a; Goud et al., n.d.).

Meskipun banyak penelitian yang membahas pengaruh panjang kunci dan panjang teks terhadap keamanan cipher, sebagian besar studi sebelumnya tidak mengisolasi kedua variabel tersebut secara independen dalam konteks Brute Force Attack murni. Celah ini penting, karena tanpa pengujian terpisah, sulit untuk memahami kontribusi empiris masing-masing variabel terhadap kompleksitas waktu pemecahan.

Berdasarkan latar belakang tersebut, penelitian ini dilakukan untuk mengukur secara empiris pengaruh variasi panjang kunci (L) dan panjang teks (|P|) terhadap waktu pemecahan Brute Force Attack pada algoritma Vigenère Cipher. Melalui pendekatan eksperimental, penelitian ini bertujuan untuk memvalidasi model kompleksitas waktu $O(|P|.26^L)$ dan memberikan kontribusi empiris terhadap pemahaman batas keamanan cipher klasik dalam konteks komputasi modern.

Sebagai arah penelitian, rumusan masalah yang dikaji adalah:

1. Bagaimana pengaruh panjang kunci (L) terhadap waktu pemecahan Brute Force Attack pada algoritma Vigenère Cipher?
2. Bagaimana pengaruh panjang teks (|P|) terhadap waktu pemecahan Brute Force Attack pada algoritma Vigenère Cipher?

Struktur artikel ini terdiri dari empat bagian: Pendahuluan, Metode Penelitian, Hasil dan Pembahasan, serta Kesimpulan.

2. METODE PENELITIAN

2.1 Desain Penelitian

Penelitian ini menggunakan pendekatan eksperimental murni (pure experimental research) dengan metode kuantitatif. Tujuannya adalah untuk mengukur secara empiris pengaruh dua variabel independen, yaitu panjang kunci (L) dan panjang teks (|P|), terhadap variabel dependen yaitu waktu pemecahan (T) pada serangan Brute Force Attack (BFA).

Pendekatan eksperimental dipilih karena memungkinkan analisis langsung terhadap performa algoritma kriptografi klasik dalam kondisi yang terkontrol (Budi Handoko, 2022a; Purwanti et al., 2024). Desain penelitian didasarkan pada analisis komparatif berjenjang, di mana hasil empiris dibandingkan dengan model teoritis kompleksitas waktu $T \propto O(|P| \cdot 26^L)$ (Guglani, n.d.-a; Hassan, 2024a). Secara umum, rancangan penelitian mencakup tahapan konseptual mulai dari pemilihan algoritma, perancangan eksperimen, hingga interpretasi hasil pengujian.

ISSN : 2477-359X (Online)
ISSN: 2407-6007 (Print)

2.2 Variabel dan Skenario Pengujian

Penelitian ini melibatkan dua variabel bebas dan satu variabel terikat sebagaimana dijelaskan pada Tabel 1.

Tabel 1. Variabel Penelitian

Jenis Variabel	Nama Variabel	Simbol	Deskripsi
Independen 1	Panjang Kunci	L	Jumlah karakter pada kunci enkripsi yang diuji
Independen 2	Panjang Teks	|P|	Jumlah karakter pada plainteks yang diuji
Dependen	Waktu Pemecahan	T	Waktu total (s) yang dibutuhkan algoritma brute force untuk menemukan kunci yang benar

Empat kombinasi skenario pengujian digunakan untuk menganalisis pengaruh kedua variabel secara lebih mendalam (Adhitya et al., 2024a).

Tabel 2. Skenario Pengujian

No	Panjang Kunci (L)	Panjang Teks (|P|)	Deskripsi Skenario
1	3	22	Kunci Pendek pada Teks Pendek.
2	5	22	Kunci Panjang pada Teks Pendek.
3	3	420	Kunci Pendek pada Teks Panjang
4	5	420	Kunci Panjang pada Teks Panjang

2.3 Alat dan Bahan

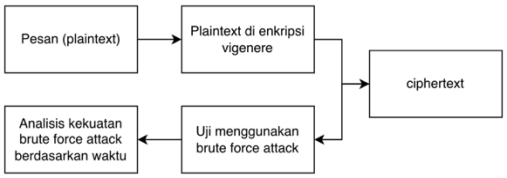
Eksperimen dilaksanakan menggunakan perangkat keras dan perangkat lunak sebagaimana ditunjukkan pada Tabel 3. Spesifikasi sistem dicantumkan untuk mendukung replikabilitas hasil dan konsistensi eksperimen (Hassan, 2024a; Vatshayan et al., 2020).

Tabel 3. Spesifikasi Sistem

Komponen	**Spesifikasi**
Perangkat keras	MacBook Pro (mid-2012), Intel Core i5 (dual-core, ~2.5 GHz) atau i7 tergantung model, RAM 8 GB, penyimpanan SSD/HDD 256–512 GB.
Sistem operasi	MacOS Catalina version 10.15.7
Bahasa pemrograman	Python 3.11
Library pendukung	time, string, dan itertools
Lingkungan pengujian	Jupyter Notebook

2.4 Prosedur Eksperimen

Tahapan pelaksanaan eksperimen terdiri atas empat langkah utama sebagaimana divisualisasikan pada Gambar 1.



Gambar 1. Desain Eksperimen

Langkah 1- Enkripsi Data.

Plaintext dienkripsi menggunakan algoritma Vigenère Cipher berdasarkan formula berikut (Budi Handoko, 2022a):

$$C_i = (P_i . K_i)\ mod\ 26 \qquad \text{(I)}$$

Ci : Huruf pada posisi ke- i dari teks terenkripsi (ciphertext).

ISSN : 2477-359X (Online)
ISSN: 2407-6007 (Print)

Pi : Huruf pada posisi ke- i dari teks asli (plaintext).
Ki : Huruf pada posisi ke- i dari kunci yang diulang-ulang agar sesuai dengan panjang teks.
N : Jumlah huruf dalam alfabet yang digunakan. Untuk alfabet Latin (n=26).
mod n : Operasi modulo yang memastikan hasilnya kembali ke dalam rentang alfabet, misalnya dari 1 hingga 26 untuk alfabet Latin

Contoh proses enkripsi huruf demi huruf ditunjukkan pada Tabel 4, yang menjelaskan proses enkripsi teks "CONTOH" menggunakan kunci "KEY".

Tabel 4. Proses Enkripsi Data (Vigenere Cipher)

Plaintext	Plaintext (P_i)	Key	K_I	(P_i + K_i)(mod n)	C_i	Cipher
C	3	K	11	(3+11) (mod 26)	14	N
O	15	E	5	(15+5) (mod 26)	20	T
N	14	Y	25	(14+25) (mod 26)	39-26 = 13	M
T	20	K	11	(20+11) (mod 26)	31-26 = 5	E
O	15	E	5	(15+5) (mod 26)	20	T
H	8	Y	25	(8+25) (mod 26)	33-26 = 7	G

Tabel 4 menunjukkan proses vigenere dalam enkripsi teks, plainteksnya CONTOH sedangkan yang menjadi keynya KEY. Algoritma vigenere melihat index huruf C di plaintext pada alfabet kemudian index tersebut dicatat oleh algoritma dan algoritma melihat Kembali index huruf K di key, terakhir index di plaintext dan index di key dijumlahkan kemudian algoritma vigenere mencatat ciphertextnya.

Langkah 2 – Pelaksanaan Brute Force Attack.

Ciphertext hasil enkripsi diuji menggunakan metode brute force dengan mencoba seluruh kombinasi kunci dari alfabet (A–Z). Waktu eksekusi diukur mulai dari percobaan pertama hingga kunci yang benar ditemukan (Tuga et al., n.d.-a).

Langkah 3 – Pencatatan Data.

Setiap skenario dijalankan sebanyak lima kali untuk memperoleh nilai rata-rata waktu eksekusi $\overline{T}$, yang dihitung dengan rumus :

$$\overline{T} = \frac{\sum_{i=1}^{n} T_i}{n}, n = 5 \qquad \text{(II)}$$

Langkah 4 – Analisis dan Validasi

Hasil empiris kemudian dibandingkan dengan model teoritis
$O(|P|\cdot 26^{L})$ untuk memvalidasi pola hubungan antara panjang kunci, panjang teks, dan waktu pemecahan (Budi Handoko, 2022b; Guglani, n.d.-b).

2.5 Desain Eksperimen

Bagian ini menjelaskan penerapan praktis desain penelitian dalam bentuk eksperimen terukur.

Desain eksperimen difokuskan pada implementasi empiris untuk mengamati dampak perubahan parameter pada kinerja algoritma.

Tahapan eksperimen ditunjukkan secara visual pada Gambar 1, yang menggambarkan aliran proses mulai dari plaintext hingga analisis hasil.

Gambar 1. Desain Eksperimen Brute Force Attack terhadap Vigenère Cipher. Menunjukkan alur eksperimen: plaintext → enkripsi Vigenère → ciphertext → brute force → analisis hasil berdasarkan waktu.
Desain eksperimen ini berfungsi untuk:

Dengan demikian, desain eksperimen merupakan realisasi teknis dari desain penelitian, yang diterapkan melalui pemrograman Python untuk menghasilkan data empiris terukur.

2.6 Proses Enkripsi Algoritma Vigenere

Vigenere Cipher adalah metode enkripsi klasik yang menggunakan substitusi polyalphabetic dan dikembangkan dari Caesar Cipher. Inti dari Vigenere adalah penggunaan kata kunci yang diulang (repeating key) sepanjang plaintext.

Proses enkripsi Vigenere secara matematis didefinisikan sebagai penambahan nilai numerik plaintext (P_i) dengan nilai numerik kunci (K_i) pada posisi ke-i, dimodulo 26 memakai asumsi alfabet 26 huruf. Tabel 4 menunjukkan proses enkripsi huruf demi huruf antara plaintext "CONTOH" dan key "KEY".

3. HASIL DAN PEMBAHASAN

Bagian ini menyajikan analisis kuantitatif terhadap data empiris yang diperoleh dari empat skenario pengujian implementasi Brute Force Attack (BFA) terhadap Vigenère Cipher. Analisis difokuskan untuk memvalidasi hipotesis penelitian mengenai pengaruh variabel independen, yaitu Panjang Kunci (L) dan Panjang Teks (P), terhadap variabel dependen, yakni Waktu Pemecahan (T).

Penyajian Data Hasil Eksperimen.

Data mentah dari keempat skenario percobaan dikonsolidasi dan distandarisasi ke dalam satuan detik. Langkah ini dilakukan agar perbandingan waktu eksekusi antar skenario dapat dilakukan secara ekuivalen. Data hasil konsolidasi disajikan pada Tabel 4 dan divisualisasikan pada Gambar 2.

Tabel 5. Hasil Rata-rata Waktu Eksekusi Brute Force Attack pada Vigenère Cipher

No	L	P	T	Deskripsi Skenario
1	3	22	0.4469	Kunci Pendek – Teks Pendek
2	5	22	166.2	Kunci Panjang – Teks Pendek
3	3	420	9.2714	Kunci Pendek – Teks Panjang
4	5	420	3427.8	Kunci Panjang – Teks Panjang

Tabel 5 diatas merupakan hasil dari 4 skenario yang telah dilakukan, yaitu waktu rata-rata (T) terhadap Panjang Kunci (L) dan Panjang Teks (P).

Seperti ditunjukkan pada Gambar 2, waktu eksekusi terendah terjadi pada skenario pertama (L=3, |P|=22) yaitu sekitar 0.4 detik, sedangkan waktu tertinggi terjadi pada skenario keempat (L=5, |P|=420) yaitu sekitar 57.13 menit.

Skenario	Panjang Kunci (L)	Panjang Teks (P)	Total Keyspace (Teoritis, 26L)	Iterasi Aktual (Kunci Ditemukan)	Waktu Pemecahan (T) (detik)
Percobaan II	3 (teh)	22 karakter	17,576	12,956	**0.4469**
Percobaan I	5 (MALAM)	22 karakter	11,881,376	5,491,161	**166.2** (2.77 menit)
Percobaan III	3 (teh)	420 karakter	17,576	12,956	**9.2714**
Percobaan IV	5 (MALAM)	420 karakter	11,881,376	5,491,163	**3427.8** (57.13 menit)

Gambar 2. Rangkuman hasil empiris waktu eksekusi Brute Force Attack untuk empat skenario pengujian

Gambar 2 diatas merupakan rangkuman hasil percobaan yang telah dilakukan. Skenario yang dilakukan terdiri dari empat skenario. Waktu paling cepat untuk algoritma brute force attack dalam menyerang algoritma vigenere yaitu selama 0.4 detik dengan panjang kunci 3 karakter dan panjang teks pada plaintext (pesan asli) 22 karakter dan waktu paling lama sebesar 57.13 menit dengan panjang kunci 5 dan panjang teks pada plaintext (pesan asli) 420 karakter.

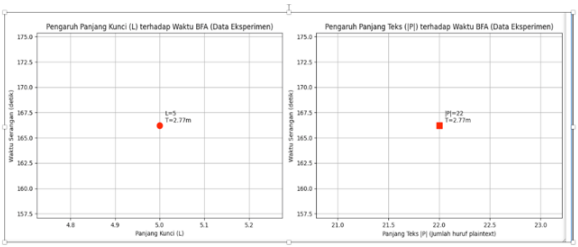
Analisis Pengaruh Variabel Panjang Kunci (L).

Analisis ini bertujuan untuk menguji hipotesis bahwa L memiliki dampak eksponensial terhadap T. Untuk mengisolasi variabel L, digunakan metode komparasi ceteris paribus dengan menjaga variabel P tetap konstan.

Komparasi pada P Konstan (P=22 karakter).

Perbandingan dilakukan antara Percobaan II (L=3, P=22) dan Percobaan I (L=5, P=22).

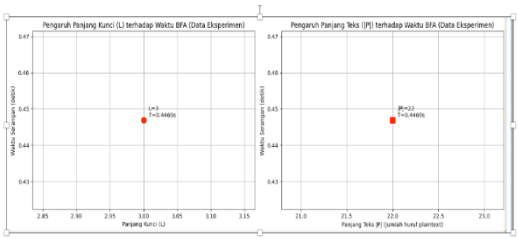
ISSN : 2477-359X (Online)
ISSN: 2407-6007 (Print)



Gambar 3. Hasil Percobaan I

Pada L=3, T = 0.4469 detik.
Pada L=5, T = 166.2 detik.
Analisis Rasio Waktu: $\frac{166.2}{0.4469} = 371.9$ detik kali lipat.

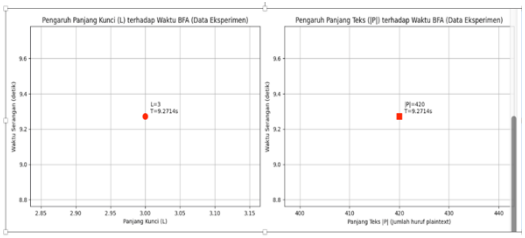
Peningkatan L sebanyak 2 karakter (dari 3 menjadi 5) tidak menghasilkan peningkatan waktu yang aditif, melainkan peningkatan multiplikatif sebesar 371.9 kali lipat. Ini secara empiris mengindikasikan hubungan non-linear yang kuat. Secara teoritis, peningkatan keyspace adalah $\frac{26^5}{26^3} = 26^2 = 676$ kali lipat. Observasi empiris (371.9x) yang berbeda dari rasio teoritis (676x) ini dapat dijelaskan oleh posisi penemuan kunci yang non-uniform dalam keyspace. Pada Percobaan I (L=5), kunci ditemukan setelah 46.2% dari keyspace dijelajahi, sedangkan pada Percobaan II (L=3), kunci ditemukan pada 73.7%. Meskipun demikian, ledakan waktu pemecahan ini secara jelas memvalidasi dampak eksponensial dari L.



Gambar 4. Hasil Percobaan 2

Komparasi pada P Konstan (P=420 karakter).

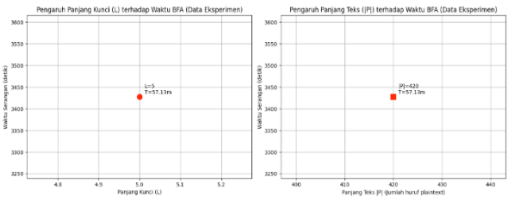
Validasi lebih lanjut dilakukan dengan membandingkan Percobaan III (L=3, P=420) dan Percobaan IV (L=5, P=420).



Gambar 5. Hasil Percobaan 3

Pada L=3, T = 9.2714 detik.
Pada L=5, T = 3427.8 detik.
Analisis Rasio Waktu: $\frac{3427.8}{9.2714} = 369.7$ detik kali lipat.

Konsistensi yang ditemukan sangat tinggi. Rasio peningkatan waktu pada P=420 (369.7x) hampir identik dengan rasio pada P=22 (371.9x). Temuan ini mengonfirmasi bahwa L adalah faktor determinan yang dominan yang berkontribusi secara eksponensial terhadap kompleksitas serangan, dan dampak ini independen terhadap panjang teks yang diproses.



Gambar 6. Hasil Percobaan 4

Perbandingan dengan penelitian terdahulu:
Hasil ini sejalan dengan temuan (Hassan, 2024b; Sebhatu, n.d.-b), yang menyatakan bahwa pertambahan satu karakter kunci pada Vigenère Cipher meningkatkan kompleksitas eksponensial sebesar 26 kali lipat. Dengan demikian, hasil empiris penelitian ini memperkuat model teoritis $T \propto 26^L$ dan menunjukkan bahwa panjang kunci adalah determinan utama resistensi kriptografis.

Analisis Pengaruh Variabel Panjang Teks (P).

Analisis ini bertujuan untuk memvalidasi hipotesis bahwa P memiliki dampak linear terhadap T. Variabel L dijaga konstan untuk mengisolasi pengaruh P.

ISSN : 2477-359X (Online)
ISSN: 2407-6007 (Print)

Komparasi pada L Konstan (L=5 karakter).

Perbandingan dilakukan antara Percobaan I (L=5, P=22) dan Percobaan IV (L=5, P=420).

Rasio Peningkatan P = $\frac{420\ karakter}{22\ karakter} = 19.09$Kali lipat.

Rasio Peningkatan T= $\frac{3427.8\ detik}{166.2\ detik} = 20.62$kali lipat.

Kedekatan antara rasio peningkatan P (19.09x) dan rasio peningkatan T (20.62x) mengindikasikan korelasi linear yang kuat. Temuan ini diperkuat secara signifikan oleh data iterasi pada Gambar 2: jumlah iterasi aktual untuk menemukan kunci "MALAM" pada kedua percobaan adalah hampir identik (5,491,161 vs 5,491,163). Ini membuktikan bahwa jumlah total "tebakan" tidak berubah, dan peningkatan waktu pemecahan yang teramati murni disebabkan oleh peningkatan beban kerja komputasi per iterasi, yang proporsional secara linear dengan P.

Komparasi pada L Konstan (L=3 karakter).

Validasi dilakukan dengan membandingkan Percobaan II (L=3, P=22) dan Percobaan III (L=3, P=420).

Rasio Peningkatan P = $\frac{420\ karakter}{22\ karakter} = 19.09$Kali lipat.

Rasio Peningkatan T = $\frac{9.2714\ detik}{0.4469\ detik} = 20.75$ kali lipat.

Hasil ini sepenuhnya konsisten dengan komparasi pada L Konstan (L=5 karakter). Jumlah iterasi yang diperlukan (12,956) adalah identik untuk kedua percobaan. Peningkatan waktu pemecahan (20.75x) kembali terbukti proporsional dengan peningkatan panjang teks (19.09x). Ini mengonfirmasi bahwa P berkontribusi secara linear terhadap total waktu eksekusi.

Perbandingan dengan penelitian terdahulu:
Hasil ini sejalan dengan penelitian (Adhitya et al., 2024a; Tuga et al., n.d.-a), yang menyimpulkan bahwa waktu pemrosesan decryption meningkat sebanding dengan jumlah karakter plaintext. Panjang teks memengaruhi waktu secara linear, bukan eksponensial, karena jumlah tebakan kunci tetap sama, hanya jumlah operasi per tebakan yang bertambah

Sintesis dan Validasi Model Kompleksitas.

Sintesis dari kedua analisis di atas memberikan validasi empiris yang kuat untuk model kompleksitas waktu teoritis Brute Force Attack (BFA) terhadap Vigenère Cipher, yakni $T \propto O(|P|.26^L)$.

Model ini dapat didekomposisi berdasarkan temuan dari :

Faktor $O(26^L)$ (Kompleksitas Eksponensial): Analisis Pengaruh Variabel Panjang Kunci (L) membuktikan bahwa Panjang Kunci (L) adalah determinan utama keamanan kriptografis. Peningkatan L memperluas keyspace secara eksponensial, yang secara langsung menyebabkan ledakan waktu pemecahan.

Faktor $O(|P|)$ (Kompleksitas Linear): Analisis Pengaruh Variabel Panjang Teks (P) membuktikan bahwa Panjang Teks (P) adalah determinan beban kerja komputasi. Peningkatan P tidak mengubah jumlah total tebakan, namun meningkatkan waktu pemrosesan untuk setiap tebakan secara linear.

Data eksperimen secara konklusif menunjukkan bahwa resistensi Vigenère Cipher terhadap BFA murni ditentukan secara eksponensial oleh panjang kunci, sementara panjang teks hanya memodulasi total waktu eksekusi secara linear yang menunjukkan asimetri fundamental antara waktu enkripsi (misalnya, 10-4 detik) dan waktu BFA (misalnya, 57.13 menit).

4. KESIMPULAN

Berdasarkan hasil eksperimen dan analisis yang telah dilakukan, diperoleh beberapa kesimpulan sebagai berikut:

1. Panjang kunci (L) terbukti memiliki pengaruh eksponensial terhadap waktu pemecahan Brute Force Attack (BFA). Peningkatan panjang kunci dari L=3 menjadi L=5 menghasilkan kenaikan waktu eksekusi sekitar 370 kali lipat, yang secara empiris mendukung model teoritis kompleksitas $O(26^L)$.
2. Panjang teks (|P|) berpengaruh secara linear terhadap waktu eksekusi. Peningkatan

panjang teks dari 22 menjadi 420 karakter meningkatkan waktu pemecahan sekitar 20 kali lipat, sejalan dengan model kompleksitas O(|P|).

3. Hasil empiris secara konsisten memvalidasi model kompleksitas waktu teoritis $T \propto O(|P| \cdot 26^L)$, sehingga dapat disimpulkan bahwa resistensi kriptografis Vigenère Cipher terhadap serangan brute force terutama ditentukan oleh panjang kunci (L), sedangkan panjang teks (|P|) hanya berperan sebagai faktor linear terhadap beban komputasi.

Penelitian lanjutan disarankan untuk mengeksplorasi penerapan metode Brute Force Attack pada algoritma cipher klasik lainnya seperti Hill Cipher atau Playfair Cipher, serta melakukan pengujian dengan panjang kunci yang lebih besar atau integrasi dengan teknik optimasi komputasi modern guna memodelkan batas performa serangan secara lebih luas.

5. REFERENSI

[1] Adhitya, P., Kusumah, D., Kusrini, K., & Kusnawi, K. (2024a). Optimizing Data Security: A Literature Review on the Implementation of Beaufort Cipher for Vigenère Affine Cipher. In *International Journal of Innovative Science and Research Technology* (Vol. 9, Issue 2). www.ijisrt.com

[2] ALABADY, S. A., SHAWKAT, T. F., & ADREES, A. W. (2025). ENHANCED VIGENERE CIPHER ALGORITHM FOR IMPROVED CRYPTOGRAPHIC SECURITY. *Quantum Journal of Engineering, Science and Technology*, *6*(1), 1–12. https://doi.org/10.55197/qjoest.v6i1.194

[3] Budi Handoko, L. (2022a). *SEKURITI TEKS MENGGUNAKAN VIGENERE CIPHER DAN HILL CIPHER* (Vol. 19, Issue 1).

[4] Chemlal, A., Tabti, H., El Bourakkadi, H., Abid, A., Jarjar, A., & Benazzi, A. (2025). A new cryptosystem based on an enhanced Vigenere cipher incorporating large SBoxes. *E3S Web of Conferences*, *601*. https://doi.org/10.1051/e3sconf/202560100002

[5] Gomez, A. N., Huang, S., Zhang, I., Li, B. M., Osama, M., & Kaiser, L. (2018). *Unsupervised Cipher Cracking Using Discrete GANs*. http://arxiv.org/abs/1801.04883

[6] Goud, Sn., Kumar, Mp., & Prasanth Reddy, Gv. (n.d.). *Design of Hybrid Cryptography System based on Vigenere Cipher and Polybius Cipher*.

[7] Guglani, R. (n.d.-a). *An Improved Permutation-Driven Vigenère Cipher with an Extended Secret Key for Enhanced Security*. https://doi.org/10.5281/zenodo.16353324

[8] Hadi, F., Slimani, Y., Douar, A., Alti, A., Saoud, F., & Harkati, M. (2024). Improved Vigenere Cipher-RSA-Based Medical Image Security Through Multiple Encryption Keys. *Ingenierie Des Systemes d'Information*, *29*(2), 599–608. https://doi.org/10.18280/isi.290221

[9] Hassan, A. (2024a). ANALYSIS AND MODIFICATION OF VIGENERE CIPHER. *Article in Journal of Mathematical Sciences & Computational Mathematics*. https://doi.org/10.15864/jmscm.5410

[10] Purwanti, Nurcahya, S. D., & Nazelliana, D. (2024). Message Security in Classical Cryptography Using the Vigenere Cipher Method. *International Journal Software Engineering and Computer Science (IJSECS)*, *4*(1), 350–357. https://doi.org/10.35870/ijsecs.v4i1.2263

[11] Sebhatu, N. (n.d.-b). *ENHANCING THE SECURITY OF VIGEN`EREVIGEN` VIGEN`ERE CIPHER USING PADDING A pattern analysis approach*.

[12] Sopiandi, I., & Jabbar, A. (n.d.). *STUDI KOMPARASI AL-GORITMA KEAMANAN DATA MENGGUNAKAN KRIPTOGRAFI VIGENERE CHIPER DAN RIVEST SHAMIR ADLEMAN (RSA)*.

[14] Tuga, V. F., Vincent, L., & Cubero, P. (n.d.-a). *Simulating Brute Force Attacks on Vigenère and AES Ciphers in Python: Measuring Key Size Impact on Security*. www.ijfmr.com

[15] Vatshayan, S., Haidri, R. A., & Verma, J. K. (2020). Design of Hybrid Cryptography System based on Vigenère Cipher and Polybius Cipher. *2020 International Conference on Computational Performance Evaluation, ComPE 2020*, 848–852. https://doi.org/10.1109/ComPE49325.2020.9199997

J-ENSISTEC (Journal of Engineering and Sustainable Technology)
Vol. 12|No. 01, December 2025
ISSN : 2477-359X (Online)
ISSN: 2407-6007 (Print)