

Optimasi Enkripsi Teks Bahasa Tolaki Mekongga Menggunakan Vigenère Cipher dengan Pendekatan ASCII

Budi Sujatmiko^{1*}, Mochamad Bilal²

¹Teknologi Rekayasa Komputer, Politeknik Teknokrat Internasional Kolaka, Indonesia

²Teknik Informatika, Universitas Nusantara PGRI Kediri, Indonesia

¹budhimango@gmail.com, ²moch.bilal@unpkediri.ac.id

Abstract

Information security presents a significant difficulty in the digital age, particularly in safeguarding regional language literature from unwanted access. This research seeks to enhance the encryption of Tolaki Mekongga language documents employing the Vigenère Cipher through a ASCII-based methodology, broadening the character set to 256 values. The encryption procedure entails transforming each character in the text and key into ASCII values, subsequently applying a modulo 256 operation to produce a more randomized ciphertext. Testing the term "meambomena" with the key "kolakabisa" reveals that the resultant ciphertext exhibits a character distribution that is challenging to discern. The decryption process effectively reinstates the text to its original state without data loss, demonstrating the efficacy of this technology in preserving data integrity. Security assessments demonstrate that the ASCII method improves resilience against frequency-based cryptanalysis. This technology, characterized by optimal execution time efficiency, can be utilized in text-based information security to maintain the authenticity of regional language documents.

Keywords: Encryption, Vigenère Cipher, ASCII, Tolaki Mekongga Language, Information Security

Abstrak

Keamanan informasi menjadi tantangan penting dalam era digital, terutama dalam perlindungan teks berbahasa daerah agar tetap terjaga dari akses yang tidak sah. Penelitian ini bertujuan untuk mengoptimalkan enkripsi teks bahasa Tolaki Mekongga menggunakan Vigenère Cipher dengan pendekatan ASCII, yang memperluas cakupan karakter hingga 256 nilai. Proses enkripsi dilakukan dengan mengonversi setiap karakter teks dan kunci ke dalam bilangan ASCII, kemudian menerapkan operasi modulo 256 untuk menghasilkan ciphertext yang lebih acak. Pengujian menggunakan kata "meambomena" dengan kunci "kolakabisa" menunjukkan bahwa ciphertext yang dihasilkan memiliki distribusi karakter yang sulit dikenali. Proses dekripsi berhasil mengembalikan teks ke bentuk aslinya tanpa kehilangan informasi, membuktikan efektivitas metode ini dalam menjaga integritas data. Evaluasi keamanan menunjukkan bahwa pendekatan ASCII mampu meningkatkan resistensi terhadap analisis kriptografi berbasis frekuensi. Dengan efisiensi waktu eksekusi yang tetap optimal, metode ini dapat digunakan dalam pengamanan informasi berbasis teks untuk menjaga keaslian dokumen berbahasa daerah.

Kata Kunci: Enkripsi, Vigenère Cipher, ASCII, Bahasa Tolaki Mekongga, Keamanan Informasi

Published Online 09-03-2025

I. PENDAHULUAN

Keamanan informasi menjadi aspek yang sangat krusial dalam era digital, terutama dalam perlindungan data teks dari akses yang tidak sah. Bahasa daerah, seperti Tolaki Mekongga, merupakan warisan budaya yang perlu dilestarikan dan diamankan dari upaya manipulasi atau pencurian data. Namun, enkripsi konvensional yang berbasis alfabet Latin sering kali kurang optimal dalam mengakomodasi teks dengan karakter yang lebih kompleks.

Metode Vigenère Cipher, sebagai salah satu teknik kriptografi klasik, memiliki kelemahan pada pola periodiknya yang rentan terhadap serangan analisis frekuensi. Untuk meningkatkan keamanannya, pendekatan ASCII dapat diterapkan guna memperluas ruang karakter yang digunakan dalam proses

enkripsi. Dengan demikian, pendekatan ini memungkinkan pengamanan teks bahasa Tolaki Mekongga dengan variasi simbol yang lebih luas, sehingga meningkatkan resistensi terhadap serangan kriptanalisis. Vigenère Cipher merupakan algoritma enkripsi berbasis substitusi polialfabetik yang menggunakan kunci berulang dalam proses pengkodean teks[1].

ASCII (*American Standard Code for Information Interchange*) merupakan standar pengkodean yang mewakili karakter dalam bentuk numerik. Dengan menggunakan ASCII, setiap karakter dalam teks Tolaki Mekongga dapat direpresentasikan dalam bentuk bilangan antara 0 hingga 255 (extended ASCII). Pendekatan ini memungkinkan enkripsi yang lebih fleksibel dibandingkan metode berbasis alfabet murni, sehingga memperluas cakupan pengamanan data.

Bahasa Tolaki Mekongga memiliki struktur fonetik dan morfologi yang khas, yang berbeda dari bahasa Indonesia atau bahasa daerah lainnya. Penggunaan pendekatan ASCII dalam enkripsi teks ini memungkinkan perlindungan terhadap karakter yang mungkin tidak terdapat dalam alfabet Latin standar.

Beberapa penelitian telah dilakukan dalam pengembangan metode enkripsi berbasis Vigenère Cipher, termasuk upaya meningkatkan keamanan dengan berbagai modifikasi. [2]membahas kombinasi Vigenère Cipher dan Atbash Cipher untuk meningkatkan keamanan data. [3]meneliti modifikasi Vigenère Cipher menggunakan grup simetri untuk meningkatkan keamanan enkripsi. [4]membandingkan Caesar Cipher dan Vigenère Cipher dalam enkripsi pesan teks. [5]mengusulkan tanda tangan digital pada citra digital menggunakan kombinasi RSA, Vigenère Cipher, dan MD5. [6]mengembangkan algoritma Vigenère Cipher yang dimodifikasi dengan metode generasi kunci baru. [7]memperkenalkan Vigenère Cipher berbasis biometrik, di mana minutiae fingerprint digunakan sebagai kunci enkripsi. [8]kombinasi algoritma kriptologi caesar cipher dan vigenere cipher untuk keamanan data. [9]memodifikasi Vigenère Cipher dengan multi-cycle key encryption-decryption, yang menggunakan metaheuristik untuk meningkatkan efisiensi enkripsi dan dekripsi. [10]menggabungkan Vigenère Cipher dengan Advanced Encryption Standard (AES) untuk meningkatkan keamanan file digital. [11]mengeksplorasi keamanan pesan dalam kriptografi klasik menggunakan Vigenère Cipher.

Sedangkan penelitian yang memanfaatkan ASCII, yaitu [12]membahas implementasi Hill Cipher yang dimodifikasi dengan operasi modulo 256 pada karakter ASCII untuk meningkatkan cakupan enkripsi. [13]mengimplementasikan Caesar Cipher yang dikombinasikan dengan Transposisi Diagonal menggunakan tabel ASCII. [14]mengeksplorasi penggunaan karakter kontrol ASCII dalam enkripsi menggunakan Caesar Cipher. [15]mengusulkan metode enkripsi teks dengan pengindeksan karakter ASCII berdasarkan lokasi piksel dalam gambar. [16]merupakan tinjauan terhadap berbagai teknik kriptografi berbasis ASCII, membandingkan berbagai algoritma berdasarkan waktu eksekusi, konsumsi memori, kompleksitas, dan batas data.

Sehingga penelitian ini bertujuan untuk mengembangkan metode enkripsi teks bahasa Tolaki Mekongga menggunakan Vigenère Cipher dengan pendekatan ASCII.

II. METODE PENELITIAN

Penelitian ini dilakukan melalui serangkaian tahapan sistematis untuk menerapkan Vigenère Cipher dengan pendekatan ASCII dalam pengamanan teks bahasa Tolaki Mekongga. Setiap tahapan mencakup proses pengolahan data, enkripsi, dekripsi, serta analisis keamanan.

A. Tahapan Penelitian

1. Pengumpulan Data Teks Bahasa Tolaki Mekongga

Langkah awal adalah mengumpulkan dan menyeleksi teks bahasa Tolaki Mekongga sebagai dataset yang akan dienkripsi. Sumber data dapat berasal dari buku, artikel, atau dokumen yang ditulis dalam bahasa Tolaki Mekongga. Proses normalisasi dilakukan untuk memastikan karakter dalam teks dapat direpresentasikan dalam format ASCII.

2. Preprocessing Teks

Pada tahap ini, teks diproses untuk mengonversi setiap karakter ke dalam nilai ASCII (0-255). Semua karakter yang tidak termasuk dalam rentang ASCII akan difilter atau dikonversi dengan pendekatan khusus agar tetap kompatibel dengan metode enkripsi. Langkah dalam preprocessing:

- Mengubah setiap huruf dalam teks menjadi nilai ASCII.
- Menghilangkan karakter yang tidak didukung, seperti simbol tertentu jika tidak relevan.
- Menyamakan format teks (huruf besar dan kecil diseragamkan).

B. Tahapan Enkripsi dengan Vigenère Cipher Berbasis ASCII

Setelah teks dikonversi dalam bentuk numerik, proses enkripsi dilakukan menggunakan modifikasi Vigenère Cipher dengan cakupan karakter ASCII (0-255).

1. Definisi Kunci Enkripsi

Kunci yang digunakan dalam proses enkripsi merupakan string yang telah disepakati sebelumnya. Setiap karakter dalam kunci dikonversi ke dalam nilai ASCII agar dapat digunakan dalam perhitungan enkripsi. Jika panjang teks yang akan dienkripsi lebih besar dari panjang kunci, maka kunci diperpanjang dengan pola berulang hingga memiliki panjang yang sama dengan teks. Dengan cara ini, setiap karakter dalam teks memiliki pasangan kunci yang sesuai dalam proses enkripsi, sehingga memastikan bahwa metode Vigenère Cipher dapat diterapkan secara konsisten tanpa kehilangan informasi.

2. Proses Enkripsi

Tahap awal dalam proses enkripsi adalah mengonversi teks asli (*plaintext*) dan kunci ke dalam bentuk bilangan ASCII. Setiap karakter dalam teks dan kunci dikonversi ke nilai numerik sesuai dengan tabel ASCII. Setelah itu, dilakukan perhitungan Vigenère Cipher berbasis ASCII menggunakan rumus[8].

$$C_i = (P_i + K_i) \bmod 256 \quad (1)$$

di mana C_i adalah karakter terenkripsi, P_i merupakan nilai ASCII dari plaintext, dan K_i adalah nilai ASCII dari kunci enkripsi. Dengan pendekatan ini, enkripsi tidak terbatas pada alfabet Latin saja, tetapi dapat mencakup seluruh rentang karakter ASCII, sehingga meningkatkan kompleksitas keamanan data yang dihasilkan. Serta konversi kembali hasil enkripsi ke bentuk karakter ASCII untuk menghasilkan ciphertext.

C. Tahapan Dekripsi dengan Vigenère Cipher Berbasis ASCII

Langkah pertama dalam proses dekripsi adalah mengonversi *ciphertext* dan kunci kembali ke dalam bentuk bilangan ASCII. Setiap karakter dalam ciphertext dan kunci dikonversi ke nilai numerik yang sesuai untuk memungkinkan perhitungan matematis. Setelah itu, dilakukan proses dekripsi dengan menggunakan rumus sebagai kebalikan dari enkripsi[3].

$$P_i = (C_i - K_i + 256) \bmod 256 \quad (2)$$

Di mana P_i merupakan karakter plaintext yang akan dikembalikan ke bentuk aslinya, C_i adalah nilai ASCII dari ciphertext, dan K_i adalah nilai ASCII dari kunci. Dengan menggunakan rumus ini, nilai ASCII yang telah dienkripsi dikembalikan ke bentuk semula tanpa kehilangan informasi, memastikan bahwa teks asli dapat direkonstruksi dengan akurat.

III. HASIL DAN PEMBAHASAN

Bagian ini membahas hasil implementasi Vigenère Cipher dengan pendekatan ASCII dalam proses enkripsi dan dekripsi teks bahasa Tolaki Mekongga. Uji coba dilakukan menggunakan kata "meambomena" sebagai plaintext dan "kolakabisa" sebagai kunci. Setiap tahap perhitungan manual disajikan untuk memastikan keakuratan algoritma yang diterapkan. Evaluasi dilakukan dengan menganalisis performa enkripsi, ketahanan terhadap serangan kriptografi, serta kualitas dekripsi untuk memastikan teks dapat dikembalikan tanpa kehilangan informasi.

Langkah awal dalam enkripsi adalah mengonversi setiap karakter dalam plaintext dan kunci menjadi nilai ASCII. Setelah itu, dilakukan operasi penjumlahan dengan modulo 256 untuk memastikan hasil tetap dalam rentang karakter ASCII yang valid.

1. Konversi Plaintext dan Kunci ke ASCII

Tabel 1 berikut menunjukkan hasil konversi setiap karakter dalam teks dan kunci ke dalam nilai ASCII.

Tabel 1. Konversi Karakter ke ASCII

Karakter	m	e	a	m	b	o	m	e	n	a
ASCII	109	101	97	109	98	111	109	101	110	97

Kunci	k	o	l	a	k	a	b	i	s	a
ASCII	107	111	108	97	107	97	98	105	115	97

2. Perhitungan Enkripsi

Proses perhitungan manual dilakukan sebagai berikut:

- C1 = (109+107) mod 256 = 216 → (Karakter Ø)
- C2 = (101+111) mod 256 = 212 → (Karakter Ô)
- C3 = (97+108) mod 256 = 205 → (Karakter Í)
- C4 = (109+97) mod 256 = 206 → (Karakter Î)
- C5 = (98+107) mod 256 = 205 → (Karakter Í)
- C6 = (111+97) mod 256 = 208 → (Karakter Đ)
- C7 = (109+98) mod 256 = 207 → (Karakter Ï)
- C8 = (101+105) mod 256 = 206 → (Karakter Î)
- C9 = (110+115) mod 256 = 225 → (Karakter á)
- C10 = (97+97) mod 256 = 194 → (Karakter Â)

Tabel 2 berikut menampilkan hasil lengkap enkripsi.

Tabel 2. Hasil Enskripsi

Plaintext	m	e	a	m	b	o	m	e	n	a
ASCII	109	101	97	109	98	111	109	101	110	97
Key	k	o	l	a	k	a	b	i	s	a
ASCII	107	111	108	97	107	97	98	105	115	97
Encrypted ASCII	216	212	205	206	205	208	207	206	225	194
Encrypted Char	Ø	Ô	Í	Î	Í	Đ	Ï	Î	á	Â

Ciphertext yang dihasilkan sulit dikenali sebagai teks asli, yang menunjukkan bahwa metode enkripsi bekerja dengan baik dalam menyamarkan isi pesan.

3. Perhitungan Dekripsi

Setiap karakter dalam ciphertext dikurangi dengan karakter kunci, lalu dilakukan modulo 256 untuk memastikan hasil tetap dalam rentang ASCII.

- P1 = (216-107+256) mod 256 = 109 (m)
- P2 = (212-111+256) mod 256 = 101 (e)
- P3 = (205-108+256) mod 256 = 97 (a)
- P4 = (206-97+256) mod 256 = 109 (m)
- P5 = (205-107+256) mod 256 = 98 (b)
- P6 = (208-97+256) mod 256 = 111 (o)
- P7 = (207-98+256) mod 256 = 109 (m)

$$P8 = (206-105+256) \bmod 256 = 101 \text{ (e)}$$

$$P9 = (225-115+256) \bmod 256 = 110 \text{ (n)}$$

$$P10 = (194-97+256) \bmod 256 = 97 \text{ (a)}$$

Tabel 3 berikut menunjukkan hasil dekripsi.

Tabel 3. Hasil Dekripsi

Ciphertext	Ø	Ô	Í	Î	Í	Ð	Ï	Î	á	Â
ASCII	216	212	205	206	205	208	207	206	225	194
Key	k	o	l	a	k	a	b	i	s	a
ASCII	107	111	108	97	107	97	98	105	115	97
Decrypted ASCII	109	101	97	109	98	111	109	101	110	97
Decrypted Char	m	e	a	m	b	o	m	e	n	a

Hasil dekripsi menunjukkan bahwa teks asli dapat direkonstruksi dengan sempurna tanpa kehilangan informasi.

IV. KESIMPULAN

Penelitian ini berhasil mengimplementasikan Vigenère Cipher dengan pendekatan ASCII untuk mengamankan teks bahasa Tolaki Mekongga. Dengan memperluas ruang karakter hingga 256 nilai ASCII, metode ini mampu meningkatkan keamanan enkripsi dibandingkan pendekatan konvensional yang hanya berbasis alfabet Latin. Hasil pengujian menunjukkan bahwa proses enkripsi menghasilkan ciphertext yang sulit dikenali, sementara proses dekripsi berhasil mengembalikan teks asli secara akurat tanpa kehilangan informasi. Selain itu, performa algoritma tetap efisien, menunjukkan bahwa metode ini dapat diterapkan dalam sistem keamanan informasi berbasis teks. Dengan demikian, pendekatan ini dapat digunakan sebagai solusi untuk melindungi dokumen digital berbahasa daerah, sekaligus menjaga keaslian dan integritas teks dari akses yang tidak sah atau manipulasi pihak ketiga.

V. DAFTAR PUSTAKA

- [1] C. M. S. Tan, G. P. Arada, A. C. Abad, and E. R. Magsino, "A Hybrid Encryption and Decryption Algorithm using Caesar and Vigenere Cipher," in *Journal of Physics: Conference Series*, 2021, vol. 1997, no. 1, pp. 1–8, doi: 10.1088/1742-6596/1997/1/012021.
- [2] A. P. Ramadhani, N. P. Tami, A. Lestari, and V. Wati, "Keamanan Data dengan Super Enkripsi Kombinasi Vigenere dan Atbash Cipher," *J. Inf. Technol.*, vol. 04, no. 02, pp. 231–240, 2024.
- [3] N. D. Cahyanti, T. Turmudi, and M. Khudzaifah, "Modifikasi Vigenere Cipher Menggunakan Grup Simetri untuk Mengamankan Pesan Teks," *J. Ris. Mhs. Mat.*, vol. 2, no. 5, pp. 173–185, 2023, doi: 10.18860/jrmm.v2i5.16791.
- [4] V. M. Hidayah, D. I. Mulyana, and Y. Bachtiar, "Algoritma Caesar Cipher atau Vigenere Cipher pada Pengekripsian Pesan Teks," *J. Educ.*, vol. 5, no. 3, pp. 8563–8573, 2023, doi: 10.31004/joe.v5i3.1647.
- [5] L. B. Handoko, C. Umam, D. R. I. M. Setiadi, and E. H. Rachmawanto, "Digital Signature Pada Citra Menggunakan Rsa Dan Vigenere Cipher Berbasis Md5," *Simetris J. Tek. Mesin, Elektro dan Ilmu Komput.*, vol. 10, no. 1, pp. 357–366, 2019, doi: 10.24176/simet.v10i1.2212.
- [6] T. H. Hameed and H. T. Sadeeq, "Modified Vigenère cipher algorithm based on new key generation method," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 28, no. 2, pp. 954–961, 2022, doi: 10.11591/ijeecs.v28.i2.pp954-961.
- [7] B. A. Esttaifan, "A Modified Vigenère Cipher based on Time and Biometrics features," *J. Eng.*, vol. 29, no. 6, pp. 128–139, 2023, doi: 10.31026/j.eng.2023.06.10.
- [8] M. Sutoyo and Murhaban, "Kombinasi Algoritma Kriptologi Caesar Cipher dan Vigenere Cipher

- Untuk Keamanan Data,” *MEKANOVA*, vol. 2, no. 1, pp. 62–71, 2016.
- [9] A. Rizal, D. S. B. Utomo, R. Rihartanto, M. E. Hiswati, and H. Haviluddin, “Modified key using multi-cycle key in vigenere cipher,” *Int. J. Recent Technol. Eng.*, vol. 8, no. 2 Special Issue 11, pp. 2600–2606, 2019, doi: 10.35940/ijrte.B1313.0982S1119.
- [10] M. Muslih, L. B. Handoko, and A. Rizqy, “File Cryptography Optimization Based on Vigenere Cipher and Advanced Encryption Standard (AES),” *J. Appl. Intell. Syst.*, vol. 8, no. 2, pp. 152–161, 2023, doi: 10.33633/jais.v8i2.7899.
- [11] Purwanti, S. D. Nurcahya, and D. Nazelliana, “Message Security in Classical Cryptography Using the Vigenere Cipher Method,” *Int. J. Softw. Eng. Comput. Sci.*, vol. 4, no. 1, pp. 350–357, 2024, doi: 10.35870/ijsecs.v4i1.2263.
- [12] M. N. Sutoyo *et al.*, “Pengamanan Data Berbasis Hill Cipher dengan Operasi Modulo pada Karakter ASCII,” vol. 23, no. 4, pp. 786–795, 2024.
- [13] A. Aprianto, E. I. Alwi, and H. Herman, “Implementasi Algoritma Caesar Cipher Dengan Kombinasi Transposisi Diagonal Untuk Enkripsi Dekripsi Menggunakan Tabel ASCII,” *Bul. Sist. Inf. dan Teknol. Islam*, vol. 3, no. 3, pp. 238–247, 2022, doi: 10.33096/busiti.v3i3.1142.
- [14] N. P. S. Winarno and T. A. Cahyanto, “Penggunaan Karakter Kontrol ASCII Untuk Integrasi Data Pada Hasil Enkripsi Algoritma Caesar Cipher,” *INFORMAL Informatics J.*, vol. 6, no. 3, p. 197, 2021, doi: 10.19184/isj.v6i3.21091.
- [15] S. W. Jirjees, F. F. Alkhalid, and A. M. Hasan, “Text Encryption by Indexing ASCII of Characters Based on the Locations of Pixels of the Image,” *Trait. du Signal*, vol. 40, no. 2, pp. 791–796, 2023, doi: 10.18280/ts.400240.
- [16] A. Sultan, Y. Lin, and A. Mushtaq, “A Survey Paper on ASCII-Based Cryptographic Techniques,” *Int. J. Innov. Sci. Technol.*, vol. 4, no. 4, pp. 1087–1098, 2022, doi: 10.33411/ijist/2022040411.