JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

Implementasi Enkripsi dan Dekripsi Teks Menggunakan Metode Substitusi Huruf

T. M. Fadhil Aqsa[1*], Rizky Hidayatullah[2]
[1,2]Universitas Malikussaleh, Indonesia
[1]fadhil.230170061@mhs.unimal.ac.id, [2]rizky.230170083@mhs.unimal.ac.id

ABSTRACT

Kriptografi merupakan salah satu teknik penting dalam menjaga kerahasiaan informasi, terutama pada proses pengiriman pesan melalui media yang rawan diakses pihak tidak berwenang. Penelitian ini membahas implementasi enkripsi dan dekripsi teks menggunakan metode substitusi huruf manual sebagai bentuk kriptografi sederhana. Metode ini bekerja dengan menggantikan setiap huruf pada teks asli dengan huruf lain berdasarkan kamus enkripsi yang telah ditentukan, sedangkan proses dekripsi dilakukan menggunakan kamus invers untuk mengembalikan pesan ke bentuk semula. Hasil pengujian menunjukkan bahwa proses enkripsi mampu menyamarkan pesan secara efektif sehingga tidak dapat dibaca secara langsung tanpa kamus yang sesuai. Selain itu, proses dekripsi berhasil mengembalikan seluruh teks terenkripsi ke bentuk asli tanpa kehilangan atau perubahan data, yang menandakan integritas pesan tetap terjaga. Meskipun memiliki keterbatasan terhadap analisis frekuensi, metode ini dinilai efisien, fleksibel, dan mudah diimplementasikan, sehingga cocok digunakan untuk pembelajaran kriptografi dasar dan pengamanan pesan dengan tingkat kerahasiaan sederhana.

Kata Kunci/ Keywords:
Kriptografi, Enkripsi, Dekripsi, Substitusi Huruf.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang sangat pesat telah membawa dampak signifikan terhadap pertukaran data dan informasi di berbagai bidang kehidupan. Kemudahan dalam berbagi informasi ini juga menimbulkan tantangan baru terkait keamanan dan kerahasiaan data, terutama data yang bersifat sensitif dan rahasia (Jawahar et al., 2023). Keamanan informasi menjadi aspek yang sangat penting karena banyaknya ancaman dari pihak yang tidak bertanggung jawab yang dapat mengakses, merusak, atau menyalahgunakan data penting (Ardiansyah et al., 2023).

Kriptografi merupakan ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara mengubah informasi yang dapat dibaca (plaintext) menjadi bentuk yang tidak dapat dipahami (ciphertext) (Salman et al., 2024). Dalam kriptografi, terdapat dua proses utama yaitu enkripsi dan dekripsi. Enkripsi adalah proses mengubah plaintext menjadi ciphertext menggunakan algoritma dan kunci tertentu, sedangkan dekripsi adalah proses sebaliknya untuk mengembalikan ciphertext ke bentuk plaintext asli (Thabrani Rahim, Muhardi, 2021).

Berbagai metode kriptografi telah dikembangkan untuk mengamankan data, baik menggunakan teknik klasik maupun modern. Algoritma kriptografi klasik seperti Caesar Cipher, Vigenere Cipher, Playfair Cipher, dan Shift Cipher masih banyak dipelajari sebagai dasar pemahaman konsep kriptografi (Dan et al., 2023)(Aufia et al., 2021). Sementara itu, algoritma modern seperti Advanced Encryption Standard (AES), Data Encryption Standard (DES), dan Elgamal telah digunakan secara luas dalam aplikasi keamanan data (Elektronik & Komputer Udayana, 2023)(Permatasari et al., 2020).

Penelitian tentang enkripsi dan dekripsi telah banyak dilakukan dengan menggunakan berbagai algoritma dan pendekatan. Beberapa penelitian mengkombinasikan algoritma kriptografi untuk meningkatkan tingkat keamanan data melalui teknik super enkripsi (Aufia et al., 2021)(Bharti Kaushik, Vikas Malik, 2023). Penelitian lain fokus pada implementasi algoritma kriptografi dalam berbagai aplikasi seperti pengamanan file, pesan teks, dan komunikasi data (Basorudin et al., 2024).

TINJAUAN PUSTAKA

Steganografi

Steganografi merupakan salah satu teknik dalam bidang keamanan informasi yang bertujuan menyembunyikan keberadaan pesan sehingga tidak diketahui oleh pihak yang tidak berwenang. Berbeda dengan kriptografi yang hanya menyamarkan isi pesan, steganografi menyembunyikan pesan itu sendiri di dalam media lain, seperti teks, gambar, audio, atau video. Dengan kata lain, steganografi berfokus pada *covert communication*, yaitu komunikasi yang tersembunyi sehingga pihak luar tidak menyadari adanya pesan yang dikirimkan. Secara historis, steganografi telah digunakan sejak zaman kuno, contohnya menulis pesan rahasia pada kulit binatang atau menggunakan tinta tak terlihat. Dalam era digital, steganografi berkembang menjadi metode yang lebih kompleks, seperti menyisipkan pesan ke dalam file gambar digital dengan memanfaatkan bit-bit tertentu yang tidak memengaruhi kualitas visual (*Least Significant Bit*). Keunggulan steganografi adalah kemampuannya menjaga kerahasiaan komunikasi tanpa menarik perhatian pihak

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

luar. Namun, metode ini juga memiliki kelemahan, antara lain terbatasnya kapasitas pesan yang dapat disembunyikan dan risiko terdeteksi jika metode penyisipannya diketahui.

Metode Substitusi Furuf

Metode substitusi huruf merupakan salah satu teknik klasik dalam kriptografi dan steganografi yang digunakan untuk menyamarkan pesan teks. Pada metode ini, setiap huruf pada teks asli (*plaintext*) digantikan oleh huruf lain sesuai dengan aturan tertentu atau kamus enkripsi. Contohnya, huruf "a" bisa diganti menjadi "m", huruf "b" diganti menjadi "n", dan seterusnya. Prinsip dasar metode ini adalah penggantian satu-ke-satu huruf dari alfabet. Terdapat beberapa jenis metode substitusi huruf:

1. Substitusi Monoalfabetik
   Setiap huruf dalam alfabet diganti dengan huruf lain menggunakan satu kamus tetap. Contohnya, alfabet "a–z" diganti menjadi "m–z, a–l". Metode ini sederhana dan mudah diterapkan, namun relatif mudah dipecahkan melalui analisis frekuensi huruf.
2. Substitusi Polialfabetik
   Menggunakan beberapa kamus pengganti secara bergantian sehingga satu huruf dapat diganti dengan huruf yang berbeda tergantung posisi atau aturan tertentu. Contohnya, *cipher Vigenère*. Metode ini lebih aman dibandingkan substitusi monoalfabetik karena lebih sulit dianalisis frekuensinya.
3. Substitusi Homofonik
   Satu huruf dapat diganti oleh beberapa simbol atau huruf berbeda secara acak. Hal ini dilakukan untuk mengurangi kemungkinan analisis frekuensi dan meningkatkan keamanan.

Metode substitusi huruf dipilih karena kemudahan implementasinya dan kemampuannya menyembunyikan pesan dalam bentuk teks biasa. Dalam penelitian ini, digunakan substitusi monoalfabetik dengan kamus enkripsi yang tetap setiap huruf, sehingga setiap huruf plaintext memiliki pengganti spesifik yang dapat dikembalikan saat dekripsi.

Kamus Enkripsi & Deskripsi

Kamus enkripsi dan dekripsi merupakan komponen penting dalam penerapan metode substitusi huruf. Kamus ini berisi pasangan antara huruf asli dengan huruf pengganti yang digunakan dalam proses enkripsi, serta pasangan sebaliknya untuk proses dekripsi. Kamus enkripsi dapat dibuat secara berurutan, acak, atau berdasarkan pola tertentu sesuai dengan kebutuhan sistem keamanan yang dibangun. Dalam proses enkripsi, setiap karakter pada plaintext akan dicocokkan dengan kamus enkripsi untuk menentukan huruf penggantinya. Hasil dari proses ini adalah ciphertext, yaitu pesan yang telah disamarkan sehingga tidak dapat dibaca secara langsung. Sebaliknya, pada proses dekripsi, ciphertext akan dicocokkan dengan kamus dekripsi untuk mengembalikan pesan ke bentuk semula. Kamus enkripsi dan dekripsi harus bersifat konsisten dan rahasia. Konsistensi diperlukan agar setiap huruf selalu memiliki pasangan yang sama, sedangkan kerahasiaan diperlukan untuk mencegah pihak yang tidak berwenang melakukan dekripsi pesan. Dalam implementasi berbasis program, kamus enkripsi umumnya direpresentasikan dalam bentuk array, dictionary, atau tabel relasi. Selain itu, kamus juga dapat diperluas untuk mencakup karakter lain seperti angka, spasi, dan simbol tertentu agar sistem dapat menangani berbagai jenis pesan.

Proses Enkripsi & Deskripsi

Proses enkripsi adalah tahapan penting dalam steganografi dan kriptografi yang bertujuan untuk mengubah teks asli (*plaintext*) menjadi teks yang tidak dapat dibaca secara langsung oleh pihak yang tidak berwenang, yang disebut teks terenkripsi (*ciphertext*). Proses ini dilakukan dengan menggunakan kamus enkripsi, yaitu tabel yang memetakan setiap huruf dari teks asli ke huruf pengganti tertentu. Enkripsi dapat dilakukan secara manual maupun otomatis menggunakan program komputer, tergantung kebutuhan dan kompleksitas data yang akan diamankan. Proses enkripsi terdiri dari:

1. Menyiapkan teks asli (plaintext)
   Teks yang akan dienkripsi harus terlebih dahulu disiapkan. Teks ini bisa berupa kata, kalimat, atau dokumen yang berisi informasi penting yang ingin disembunyikan. Pada tahap ini, dilakukan pengecekan agar teks bebas dari karakter yang tidak diinginkan atau simbol yang tidak termasuk dalam kamus enkripsi.
2. Mengidentifikasi setiap huruf pada teks
   Setiap karakter pada teks asli diidentifikasi satu per satu. Identifikasi ini penting untuk memastikan setiap huruf diganti sesuai aturan yang telah ditetapkan. Proses ini dapat dilakukan secara manual dengan melihat huruf satu per satu atau secara otomatis melalui komputer yang membaca teks karakter demi karakter.
3. Mengganti huruf sesuai dengan kamus enkripsi
   Setiap huruf plaintext diganti dengan huruf pengganti sesuai tabel kamus enkripsi. Misalnya, huruf "a" diganti menjadi "m", huruf "b" diganti menjadi "n", dan seterusnya. Proses ini menyamarkan isi pesan sehingga pihak yang tidak memiliki kamus tidak dapat memahami teks tersebut.

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

4. Menyusun kembali huruf-huruf yang telah diganti menjadi teks baru (ciphertext)
   Huruf-huruf yang telah diganti kemudian disusun kembali untuk membentuk teks terenkripsi. Teks ini terlihat acak atau tidak bermakna bagi orang yang tidak mengetahui kamus enkripsi, sehingga dapat dikirimkan atau disimpan dengan aman.
5. Menyimpan atau mengirim teks terenkripsi kepada penerima
   Setelah teks terenkripsi selesai dibuat, teks tersebut dapat dikirim melalui media komunikasi digital, seperti email, pesan instan, atau disimpan dalam dokumen digital. Keamanan pesan tetap terjaga karena hanya penerima yang memiliki kamus dekripsi yang dapat membaca teks asli.

Proses dekripsi adalah tahap kebalikan dari enkripsi, yaitu mengembalikan teks terenkripsi menjadi teks asli (*plaintext*). Dekripsi menggunakan kamus deskripsi, yang merupakan inversi dari kamus enkripsi, sehingga setiap huruf terenkripsi dikembalikan ke bentuk aslinya. Langkah-langkah dekripsi adalah sebagai berikut:

1. Menerima teks terenkripsi (ciphertext)
   Penerima menerima teks yang telah dienkripsi melalui media komunikasi yang digunakan, baik itu email, pesan instan, maupun dokumen digital. Teks ini terlihat acak atau tidak bermakna bagi pihak yang tidak memiliki kamus dekripsi, sehingga informasi tetap aman dari akses tidak sah.
2. Mengidentifikasi setiap huruf terenkripsi
   Setiap karakter pada ciphertext diidentifikasi secara berurutan. Proses identifikasi ini penting agar setiap huruf dapat dicocokkan dengan benar pada kamus deskripsi. Ketelitian pada tahap ini memastikan bahwa tidak ada huruf yang terlewat atau salah interpretasi, sehingga teks asli dapat dikembalikan dengan sempurna.
3. Mengganti huruf sesuai dengan kamus deskripsi
   Setiap huruf terenkripsi diganti kembali menjadi huruf asli sesuai dengan kamus deskripsi. Langkah ini memastikan bahwa setiap karakter kembali ke bentuk awalnya tanpa kehilangan atau perubahan informasi. Proses ini bisa dilakukan secara manual dengan mencocokkan huruf satu per satu atau secara otomatis menggunakan program komputer yang memproses seluruh teks secara cepat dan akurat.
4. Menyusun kembali huruf-huruf yang telah dikembalikan menjadi teks asli (plaintext)
   Huruf-huruf yang telah dikembalikan kemudian disusun kembali membentuk teks asli yang dapat dibaca dan dipahami oleh penerima. Tahap ini memastikan bahwa pesan tetap utuh, akurat, dan sesuai dengan maksud pengirim, sehingga integritas data tetap terjaga.

Dalam implementasi digital, proses enkripsi dan dekripsi dilakukan melalui program komputer yang membaca karakter demi karakter dari teks, melakukan pencocokan pada kamus, dan menghasilkan teks terenkripsi atau teks asli. Keunggulan metode ini adalah prosesnya yang sederhana, efisien, dan cepat, sehingga dapat diterapkan pada berbagai ukuran teks. Selain itu, hasil dekripsi selalu identik dengan teks asli, sehingga integritas data dan keaslian pesan tetap terjaga. Dengan memahami proses enkripsi dan dekripsi, pengguna dapat memastikan keamanan informasi, mencegah akses tidak sah, dan meminimalkan risiko manipulasi data. Metode ini menjadi dasar pengembangan sistem keamanan informasi digital, termasuk dalam komunikasi rahasia, penyimpanan data sensitif, dan aplikasi steganografi modern.

METODE PENELITIAN

Pendekatan Penelitian

Pendekatan penelitian yang digunakan dalam penelitian ini adalah pendekatan deskriptif kualitatif dengan dukungan eksperimen sederhana (experimental approach). Pendekatan deskriptif digunakan untuk menjelaskan secara sistematis konsep, proses, dan hasil penerapan metode enkripsi dan dekripsi menggunakan substitusi huruf manual. Sementara itu, pendekatan eksperimen diterapkan melalui pengujian langsung terhadap program yang dikembangkan untuk melihat bagaimana teks asli (plaintext) diubah menjadi teks terenkripsi (ciphertext) dan kemudian dikembalikan lagi ke bentuk semula melalui proses dekripsi.

Variabel Penelitian

Dalam penelitian ini, terdapat beberapa variabel yang diamati, yang dibagi menjadi variabel input, variabel proses, dan variabel output. Variabel-variabel ini berperan penting dalam memastikan keberhasilan implementasi program enkripsi dan dekripsi teks menggunakan metode substitusi huruf manual.

1. Variabel Input
   Teks Asli (Plaintext)
   Variabel input utama dalam penelitian ini adalah teks asli atau kata-kata yang akan mengalami proses enkripsi. Teks ini menjadi objek utama yang diamati untuk menilai efektivitas metode substitusi huruf. Teks asli ini dipilih karena mengandung variasi huruf yang cukup untuk menguji seluruh kamus enkripsi yang telah dibuat. Variabel ini bersifat penting karena kualitas dan panjang teks dapat memengaruhi proses enkripsi, sehingga teks yang

E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

lebih panjang atau mengandung huruf kapital dan karakter khusus memberikan tantangan tersendiri dalam pengolahan data..

2. Variabel Proses
   1) Proses Enkripsi
      Proses enkripsi merupakan tahapan utama di mana teks asli diubah menjadi bentuk yang tidak mudah dikenali, agar pesan rahasia tetap terlindungi. Setiap huruf pada teks asli diganti dengan huruf lain sesuai dengan kamus enkripsi yang telah ditentukan sebelumnya. Proses ini dilakukan secara sistematis, huruf demi huruf, dengan memperhatikan kapitalisasi huruf agar struktur teks tetap terlihat alami. Proses enkripsi ini juga mencakup mekanisme penggantian huruf yang bersifat tetap (one-to-one), sehingga setiap huruf tertentu selalu digantikan oleh huruf yang sama, menjamin konsistensi dalam seluruh teks yang dienkripsi.

   2) Proses Dekripsi
      Proses dekripsi adalah kebalikan dari enkripsi, bertujuan mengembalikan teks terenkripsi (ciphertext) menjadi teks asli (plaintext). Proses ini menggunakan kamus dekripsi, yaitu invers dari kamus enkripsi, untuk memastikan setiap huruf terenkripsi dapat dikonversi kembali ke huruf asli secara akurat. Variabel ini penting untuk menilai integritas data, yaitu memastikan bahwa proses enkripsi tidak mengubah isi pesan dan semua informasi tetap utuh setelah didekripsi.
3. Variabel Output
   1) Teks Terenkripsi (Ciphertext)
      Teks terenkripsi merupakan hasil dari proses enkripsi, berupa rangkaian huruf yang telah tersubstitusi sehingga tampak acak dan sulit dibaca tanpa kamus enkripsi. Variabel ini digunakan untuk menilai efektivitas metode enkripsi dalam menyamarkan isi pesan, serta memastikan substitusi huruf telah dilakukan secara konsisten.
   2) Teks Didekripsi (Decrypted Text)
      Teks didekripsi adalah hasil dari proses dekripsi yang harus identik dengan teks asli. Variabel ini digunakan untuk mengukur tingkat keberhasilan metode enkripsi-dekripsi, yaitu apakah proses pengembalian teks ke bentuk asli berhasil tanpa kehilangan atau perubahan karakter.

Prosedur Penelitian

Prosedur penelitian ini disusun secara sistematis agar seluruh tahapan dapat berjalan dengan terarah, terkontrol, dan sesuai dengan tujuan penelitian, yaitu mengevaluasi efektivitas metode substitusi huruf dalam enkripsi dan dekripsi teks. Setiap tahapan dirancang untuk memastikan bahwa data yang digunakan, proses yang dilakukan, serta hasil yang diperoleh dapat dianalisis secara objektif dan akurat. Tahapan penelitian yang dilakukan adalah sebagai berikut:

1. Studi Literatur
   Tahap awal penelitian dilakukan dengan mempelajari berbagai referensi yang berkaitan dengan konsep dasar kriptografi dan steganografi, metode substitusi huruf, rinsip enkripsi dan dekripsi teks, dan penelitian terdahulu yang relevan. Studi literatur ini bertujuan untuk memperkuat landasan teori serta memastikan metode yang digunakan sesuai dengan tujuan penelitian.
2. Perancangan Kamus Enkripsi dan Dekripsi
   Pada tahap ini dilakukan penyusunan kamus enkripsi dengan mengganti setiap huruf alfabet (a–z) dengan huruf lain secara acak namun unik dan pembuatan kamus dekripsi sebagai kebalikan (invers) dari kamus enkripsi agar proses pengembalian teks dapat dilakukan dengan tepat.
3. Perancangan dan Implementasi Program
   Setelah kamus ditentukan, dilakukan pengembangan program menggunakan bahasa pemrograman Python yang meliputi input teks asli (plaintext), proses enkripsi berdasarkan kamus enkripsi, proses dekripsi berdasarkan kamus dekripsi, dan penanganan huruf kapital dan karakter non-alfabet agar tetap konsisten.
4. Pengujian Sistem
   Program yang telah dibuat kemudian diuji menggunakan beberapa contoh teks untuk memastikan teks dapat dienkripsi dengan benar, teks terenkripsi dapat didekripsi kembali ke bentuk asli dan tidak terjadi kehilangan atau perubahan data selama proses berlangsung.
5. Analisis Hasil
   Hasil pengujian dianalisis untuk menilai konsistensi hasil enkripsi dan dekripsi. tingkat penyamaran pesan dan kelebihan dan keterbatasan metode substitusi huruf manual.
6. Penarikan Kesimpulan
   Tahap akhir penelitian adalah menarik kesimpulan berdasarkan hasil analisis yang telah dilakukan, serta memberikan saran untuk pengembangan metode atau penelitian selanjutnya.

HASIL DAN PEMBAHASAN

Bab ini membahas hasil implementasi program enkripsi dan dekripsi teks menggunakan metode substitusi huruf manual, yang merupakan salah satu bentuk sederhana dari teknik kriptografi. Substitusi huruf merupakan teknik di

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

mana setiap huruf pada teks asli (plaintext) digantikan dengan huruf lain sesuai dengan aturan atau kamus enkripsi yang telah ditentukan. Tujuan proses ini menjaga kerahasiaan pesan sehingga pesan asli tidak mudah terbaca oleh pihak yang tidak berwenang. Dalam penelitian ini, kamus enkripsi dibuat dengan mengganti setiap huruf alfabet dengan huruf lain secara acak, dan kamus dekripsi dibentuk sebagai kebalikan dari kamus enkripsi. Program ini kemudian diuji dengan memasukkan teks tertentu, dienkripsi, dan kemudian didekripsi kembali untuk memastikan integritas data tetap terjaga.

Kamus Enkripsi & Deskripsi

Kamus enkripsi merupakan komponen penting dalam proses penyandian pesan, karena berfungsi sebagai peta pengganti yang menentukan bagaimana setiap huruf pada teks asli (plaintext) diubah menjadi huruf baru yang digunakan untuk menyamarkan isi pesan. Dengan menggunakan kamus enkripsi, setiap karakter dalam teks asli akan digantikan oleh karakter lain sesuai aturan yang telah ditetapkan, sehingga pesan menjadi sulit dibaca oleh pihak yang tidak berwenang. Dalam penelitian ini, kamus enkripsi dibuat menggunakan metode substitusi sederhana, di mana setiap huruf alfabet digantikan dengan huruf lain yang sudah ditentukan. Substitusi ini bersifat satu-satu, artinya setiap huruf asli memiliki padanan huruf terenkripsi yang unik. Berikut kamus enkripsi yang digunakan dalam program:

Table 1. Kamus Enkripsi & Deskripsi

Huruf Asli	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
Huruf Enkripsi	m	n	b	v	c	x	z	l	k	j	h	g	f	d	s	a	q	w	e	r	t	y	u	i	o	p

Pada tabel tersebut, setiap huruf asli digantikan dengan huruf lain sesuai kamus enkripsi, misalnya huruf ‘a’ menjadi ‘m’ dan ‘b’ menjadi ‘n’, sehingga teks asli tersamarkan dan tampak seperti rangkaian huruf acak bagi pihak yang tidak mengetahui pola penggantiannya. Sebaliknya, proses dekripsi menggunakan kamus invers dari kamus enkripsi untuk mengembalikan setiap huruf terenkripsi ke bentuk aslinya, seperti huruf ‘m’ menjadi ‘a’ dan ‘n’ menjadi ‘b’, sehingga pesan yang telah disandikan dapat dibaca kembali secara akurat tanpa kehilangan informasi. Selain itu, penerapan kamus enkripsi dan dekripsi dalam program memiliki beberapa keunggulan:

1. Keamanan Sederhana
   Meskipun metode ini tergolong sederhana dibandingkan algoritma enkripsi modern, pesan yang telah terenkripsi tidak dapat dibaca secara langsung oleh pihak yang tidak memiliki kamus. Hal ini memberikan lapisan keamanan dasar yang cukup untuk komunikasi yang tidak membutuhkan tingkat kerahasiaan tinggi. Keunggulan ini membuat metode substitusi huruf menjadi pilihan yang tepat untuk praktik awal steganografi atau untuk tujuan pendidikan.
2. Efisiensi Implementasi
   Kamus enkripsi dan dekripsi dapat diterapkan dengan mudah menggunakan struktur data sederhana, seperti list atau dictionary dalam bahasa pemrograman Python. Penggunaan struktur data ini memungkinkan proses pencarian huruf pengganti atau huruf asli berlangsung dengan cepat, sehingga program dapat memproses pesan dalam jumlah besar tanpa mengorbankan performa. Selain itu, implementasi ini juga mudah dipahami dan dimodifikasi oleh programmer pemula maupun mahir.
3. Fleksibilitas
   Kamus ini dapat diubah sesuai kebutuhan tanpa merubah algoritma dasar dari sistem enkripsi. Misalnya, jika ingin meningkatkan tingkat kerahasiaan, pengembang dapat membuat kamus dengan susunan huruf yang berbeda atau menambahkan simbol dan angka sebagai pengganti huruf tertentu. Fleksibilitas ini meningkatkan kesulitan bagi pihak yang mencoba membongkar pesan secara tidak sah, karena setiap perubahan pada kamus akan menghasilkan pola penggantian huruf yang berbeda, sehingga pesan terenkripsi menjadi lebih sulit ditebak.

Proses Enkripsi

Proses enkripsi merupakan tahap penting dalam penelitian ini, di mana teks asli diubah menjadi bentuk yang tidak mudah dikenali agar pesan rahasia tetap terlindungi. Enkripsi dilakukan dengan mengganti setiap huruf pada teks asli sesuai dengan kamus enkripsi yang telah dibuat sebelumnya. Kamus ini berisi pasangan huruf asli dan huruf pengganti yang bersifat tetap, sehingga setiap huruf tertentu selalu digantikan huruf yang sama. Salah satu hal penting dalam proses ini adalah kapitalisasi huruf. Huruf kapital pada teks asli tetap dipertahankan sebagai huruf kapital pada hasil enkripsi, sehingga struktur teks asli dapat sedikit terlihat tetapi isi pesan tetap aman bagi pihak yang tidak mengetahui kamus enkripsi. Dalam penelitian ini, teks yang digunakan sebagai sampel untuk proses enkripsi adalah kata:

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

Teks Asli (Plaintext): steganografi

Enkripsi dilakukan secara sistematis dan berurutan. Setiap huruf pada teks asli diganti sesuai dengan kamus enkripsi hingga seluruh teks selesai dienkripsi. Langkah-langkahnya adalah sebagai berikut:

1. Pemilihan huruf pertama
   Huruf pertama pada teks asli adalah ‘s’. Berdasarkan kamus enkripsi yang telah dibuat, huruf ‘s’ diganti dengan huruf ‘e’. Hal ini menandai awal proses substitusi dan menjadi pola untuk huruf-huruf berikutnya.
2. Pemilihan huruf kedua
   Huruf kedua pada teks asli adalah ‘t’. Mengacu pada kamus, huruf ‘t’ diganti dengan huruf ‘r’. Dengan cara ini, proses substitusi berjalan secara berurutan sesuai posisi huruf dalam teks.
3. Penggantian huruf berikutnya
   Proses ini berlanjut untuk semua huruf dalam teks. Misalnya, huruf ‘e’ menjadi ‘c’, ‘g’ menjadi ‘z’, ‘a’ menjadi ‘m’, ‘n’ menjadi ‘d’, ‘o’ menjadi ‘s’, dan seterusnya hingga huruf terakhir. Proses ini memastikan seluruh teks asli tersubstitusi dengan huruf baru secara konsisten.

Setelah semua huruf diganti, huruf-huruf tersebut digabung kembali menjadi sebuah kata atau kalimat yang tidak dapat dimengerti secara langsung tanpa kamus enkripsi. Proses ini memastikan bahwa teks asli telah teracak secara sistematis, sehingga pihak luar yang tidak mengetahui kamus enkripsi akan sulit untuk menebak isi pesan. Namun, bagi pihak yang memiliki kamus enkripsi, proses dekripsi menjadi mudah dilakukan karena substitusi huruf bersifat tetap dan konsisten. Hasil enkripsi dari teks *steganografi* menggunakan kamus enkripsi yang telah dibuat adalah:

Teks Terenkripsi (Ciphertext): erczmdszwmxk

Ciphertext ini merupakan hasil substitusi huruf demi huruf, di mana setiap huruf pada teks asli diganti dengan huruf tertentu sesuai dengan kamus enkripsi yang telah ditentukan sebelumnya. Proses ini tidak hanya mengubah huruf, tetapi juga membuat teks tampak acak dan sulit ditebak, sehingga pihak luar yang melihat ciphertext tidak akan dapat memahami isi pesan tanpa mengetahui kamus yang digunakan. Tabel 2 berikut menunjukkan penggantian masing-masing huruf pada teks asli menjadi huruf terenkripsi secara rinci:

Table 2. Substitusi Tiap Huruf

Huruf Asli	**s**	**t**	**e**	**g**	**a**	**n**	**o**	**g**	**r**	**a**	**f**	**i**
Huruf Enkripsi	e	r	c	z	m	d	s	z	w	m	x	k

Dari tabel ini terlihat bahwa setiap huruf telah diganti secara sistematis sesuai dengan kamus enkripsi. Misalnya, huruf ‘s’ selalu menjadi ‘e’ dan huruf ‘t’ selalu menjadi ‘r’. Dengan metode ini, teks asli steganografi telah berhasil disamarkan menjadi bentuk yang tidak dapat dibaca langsung, sehingga meningkatkan keamanan informasi yang disampaikan. Selain itu, proses ini dapat diterapkan pada teks yang lebih panjang, termasuk kalimat atau paragraf, dengan prinsip yang sama, yaitu mengganti setiap huruf sesuai kamus enkripsi. Metode ini juga mudah diimplementasikan secara manual maupun dengan program komputer, sehingga efisien untuk penggunaan dalam penelitian maupun aplikasi nyata. Enkripsi menggunakan metode substitusi huruf seperti ini merupakan bagian dari steganografi sederhana, yang meskipun tidak sekuat algoritma enkripsi modern, cukup efektif untuk mengamankan pesan dalam konteks tertentu, terutama ketika informasi dikirim melalui media yang rawan dibaca pihak ketiga.

Proses Deskripsi

Proses dekripsi merupakan kebalikan dari proses enkripsi, yaitu upaya untuk mengembalikan teks yang telah terenkripsi (ciphertext) menjadi teks asli (plaintext) menggunakan kamus dekripsi. Dekripsi memiliki tujuan utama untuk memastikan pesan yang dikirim tetap utuh, tidak berubah, dan dapat dibaca kembali oleh pihak yang memiliki otorisasi. Proses ini sangat penting dalam komunikasi aman karena tanpa dekripsi, teks yang terenkripsi hanya akan terlihat sebagai rangkaian karakter acak yang tidak bermakna bagi pihak yang tidak mengetahui kamus dekripsinya. Dalam penelitian ini, teks yang digunakan sebagai contoh dekripsi adalah:

Teks Terenkripsi: erczmdszwmxk

Langkah-langkah dekripsi dilakukan secara sistematis dengan mengacu pada kamus dekripsi yang merupakan invers dari kamus enkripsi. Proses dekripsi dilakukan sebagai berikut:

1. Ambil huruf pertama
   Huruf pertama pada ciphertext adalah e. Mengacu pada kamus dekripsi, huruf e dikembalikan menjadi huruf asli s. Proses ini menunjukkan bagaimana setiap huruf terenkripsi memiliki padanan tertentu dalam teks asli. Pada tahap ini, penting memastikan bahwa huruf yang dikonversi sesuai dengan kamus dekripsi agar tidak terjadi kesalahan.
2. Ambil huruf kedua

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

Huruf kedua pada ciphertext adalah r. Berdasarkan kamus dekripsi, huruf r dikembalikan menjadi huruf t. Langkah ini diulang secara konsisten, sehingga setiap huruf pada ciphertext dapat dikembalikan ke bentuk aslinya.

3. Ambil huruf ketiga hingga huruf terakhir
   Proses ini diulang untuk setiap huruf dalam teks terenkripsi, secara berurutan, sampai seluruh huruf dikembalikan ke bentuk asli. Misalnya, huruf c dikembalikan menjadi e, huruf z menjadi g, dan seterusnya hingga huruf terakhir k dikembalikan menjadi i.

Setelah seluruh huruf dikonversi menggunakan kamus dekripsi, huruf-huruf tersebut disusun kembali dalam urutan semula sehingga membentuk kata atau kalimat asli. Hasil akhir dari proses dekripsi menunjukkan bahwa teks asli berhasil dikembalikan tanpa kehilangan atau perubahan data. Hal ini membuktikan bahwa integritas pesan tetap terjaga selama proses enkripsi dan dekripsi.

Teks Didekripsi (Decrypted Text): steganografi

Untuk mempermudah pemahaman, berikut tabel pemetaan dari huruf terenkripsi ke huruf asli, yang menunjukkan hubungan satu per satu antara ciphertext dan plaintext:

Table 3. Pemetaan Ciphertext Ke Plaintext

Huruf Terenkripsi	**e**	**r**	**c**	**z**	**m**	**d**	**s**	**z**	**w**	**m**	**x**	**k**
Huruf Asli	s	t	e	g	a	n	o	g	r	a	f	i

Dari tabel tersebut dapat diamati bahwa setiap huruf pada ciphertext memiliki padanan huruf unik pada plaintext, sehingga proses dekripsi dapat dilakukan secara akurat. Tidak ada huruf yang hilang atau tertukar, yang menegaskan bahwa integritas pesan tetap terjaga. Selain itu, proses dekripsi juga menunjukkan keandalan metode Null Cipher dalam menyembunyikan pesan rahasia. Meskipun teks terenkripsi terlihat seperti rangkaian huruf acak, pihak yang memiliki kamus dekripsi dapat dengan mudah mengembalikan teks tersebut ke bentuk asli tanpa kesalahan. Hal ini menegaskan bahwa Null Cipher tetap efektif untuk komunikasi yang membutuhkan tingkat kerahasiaan sederhana. Secara praktis, proses dekripsi dapat dilakukan secara manual seperti pada contoh di atas, atau dapat diotomatisasi menggunakan program komputer untuk mempercepat konversi teks terenkripsi ke plaintext, terutama jika jumlah data yang dienkripsi sangat besar. Dengan demikian, dapat disimpulkan bahwa proses dekripsi merupakan tahap penting dalam menjaga keamanan dan integritas pesan. Proses ini tidak hanya memastikan pesan rahasia dapat dibaca kembali, tetapi juga menjadi indikator keberhasilan metode enkripsi yang digunakan.

Analisis Analisis

Berdasarkan hasil implementasi program enkripsi dan dekripsi menggunakan metode substitusi huruf, dapat dilakukan beberapa analisis sebagai berikut:

1. Keamanan sederhana
   Metode substitusi huruf yang digunakan dalam penelitian ini relatif sederhana, namun mampu menyamarkan pesan dengan baik. Teks terenkripsi tidak dapat langsung dibaca tanpa menggunakan kamus enkripsi, sehingga pesan tetap terlindungi dari pihak yang tidak berwenang. Meskipun sederhana, teknik ini cukup efektif untuk menjaga kerahasiaan pesan dalam konteks komunikasi yang tidak terlalu sensitif.
2. Konsistensi data
   Proses dekripsi yang dilakukan berhasil mengembalikan teks terenkripsi ke bentuk aslinya secara utuh. Hal ini membuktikan bahwa integritas data tetap terjaga dan tidak terjadi kehilangan informasi selama proses enkripsi maupun dekripsi. Dengan demikian, program ini dapat diandalkan untuk menjaga keaslian pesan.
3. Fleksibilitas penggunaan
   Program yang dikembangkan memiliki kemampuan untuk mengenkripsi teks dengan panjang dan karakter yang berbeda-beda. Karakter yang tidak termasuk alfabet, seperti angka atau simbol, dibiarkan tetap sama agar pesan tetap terbaca meskipun mengandung karakter khusus.
4. Keterbatasan metode
   Meskipun metode ini efektif untuk menyamarkan pesan, metode substitusi huruf memiliki kelemahan terhadap analisis frekuensi atau pola penggantian huruf. Jika pihak ketiga mengetahui pola penggantian atau melakukan analisis yang cermat, pesan dapat dengan mudah dipecahkan. Oleh itu, metode cocok digunakan untuk komunikasi yang tidak terlalu rahasia atau untuk tujuan pembelajaran dan demonstrasi teknik steganografi sederhana.

Table 4. Ringkasan Hasil

Teks Asli	**Teks Terenkripsi**	**Teks Didekripsi**	**Status**
steganografi	erczmdszwmxk	steganografi	Berhasil
enkripsi	cwvzmrwz	enkripsi	Berhasil
kriptografi	hqzfzwczrwmxk	kriptografi	Berhasil

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

Dari tabel di atas terlihat bahwa proses enkripsi dan dekripsi berjalan sesuai harapan. Setiap teks yang terenkripsi berhasil dikembalikan ke bentuk asli tanpa adanya perubahan karakter, sehingga menegaskan bahwa program ini bekerja secara konsisten, akurat, dan dapat diandalkan. Selain itu, hasil ini menunjukkan bahwa metode substitusi huruf manual cukup efektif untuk menjaga kerahasiaan pesan dalam konteks penggunaan yang sesuai, terutama untuk tujuan edukasi, praktik laboratorium, atau komunikasi sederhana.

KESIMPULAN

Berdasarkan keseluruhan hasil implementasi dan pembahasan program enkripsi dan dekripsi teks menggunakan metode substitusi huruf manual, dapat disimpulkan bahwa metode ini terbukti efektif dalam menyamarkan pesan sehingga teks asli tidak dapat dibaca secara langsung tanpa mengetahui kamus enkripsi yang digunakan. Proses enkripsi berjalan secara sistematis dengan mengganti setiap huruf dalam teks asli sesuai aturan kamus enkripsi, sementara proses dekripsi berhasil mengembalikan teks terenkripsi ke bentuk aslinya secara utuh, sehingga integritas data tetap terjaga tanpa adanya kehilangan atau perubahan informasi. Program ini juga menunjukkan fleksibilitas yang tinggi, karena dapat mengenkripsi teks dengan panjang dan karakter yang berbeda, termasuk huruf kapital, angka, maupun simbol, sehingga pengguna dapat menyesuaikan penerapannya sesuai kebutuhan komunikasi. Selain itu, implementasi metode ini cukup efisien karena menggunakan struktur data sederhana, memungkinkan proses enkripsi dan dekripsi berjalan cepat dan mudah dipahami. Meskipun metode substitusi huruf memiliki keterbatasan, metode ini tetap efektif untuk komunikasi yang tidak memerlukan tingkat kerahasiaan tinggi, serta sangat cocok untuk pendidikan, demonstrasi, atau praktik awal steganografi. Secara keseluruhan, sistem enkripsi dan dekripsi yang dikembangkan terbukti konsisten, andal, dan dapat diandalkan untuk menjaga kerahasiaan pesan dalam konteks yang sesuai, sambil memberikan kemudahan penggunaan, keamanan dasar, dan fleksibilitas modifikasi kamus enkripsi sesuai kebutuhan pengguna.

REFERENSI

Ardiansyah, F. D., Damayanti, A., Putri, C. A. M., Rany, A. F. D., Biroso, yaidin J., & Tahire, M. (2023). Implementasi Kriptografi Caesar Chiper Pada Aplikasi Enkripsi Dan Dekripsi. *Jurnal Ilmiah Sistem Informasi Dan Ilmu Komputer*, *3*(1), 105–112.

Aufia, Z., Turmudi, T., & Alisah, E. (2021). Enkripsi dan Dekripsi Pesan Menggunakan Metode Vigenere Cipher dan Route Cipher. *Jurnal Riset Mahasiswa Matematika*, *1*(2), 93–104. https://doi.org/10.18860/jrmm.v1i2.14207

Basorudin, B., Thoriq, M., Nasution, M. R., Mustafa, S. R., & Rouza, E. (2024). Penerapan Kriptografi untuk Enkripsi dan Dekripsi Text dengan Algoritma Subtitusi Cipher. *Journal of Information System and Technology*, *5*(3), 31–36. https://doi.org/10.37253/joint.v5i3.10009

Bharti Kaushik, Vikas Malik, V. S. (2023). A Review Paper on Data Encryption and Decryption. *Bussiness Law Binus*, *7*(2), 33–48. http://repository.radenintan.ac.id/11375/1/PERPUS PUSAT.pdf%0Ahttp://business-law.binus.ac.id/2015/10/08/pariwisata-syariah/%0Ahttps://www.ptonline.com/articles/how-to-get-better-mfi-results%0Ahttps://journal.uir.ac.id/index.php/kiat/article/view/8839

Dan, E., Dengan, D., Aes, M., & Uniska, D. I. (2023). *Jurnal Fasilkom*. *13*(2), 259–268.

Elektronik, J., & Komputer Udayana, I. (2023). *Pengamanan Teks Dalam File Menggunakan Metode Enkripsi/Dekripsi Kombinasi Vigenere Cipher Dan Shift Cipher*. *12*(2), 341–350.

Jawahar, G. G., Anto, D. S., Thomas, T. J., Krishnendu, & Jousva, M. (2023). A Study on Encryption and Decryption using the Caesar Cipher Method. *International Journal of Intelligent Systems and Applications in Engineering*, *11*(3), 357–360.

Permatasari, S., Aminudin, A., & Arifianto, S. (2020). Modifikasi Enkripsi dan Dekripsi AES dengan Polybius Chiper dalam Pengamanan Data. *JRST (Jurnal Riset Sains Dan Teknologi)*, *4*(1), 41. https://doi.org/10.30595/jrst.v4i1.6208

Salman, H. M., Ajam, M. H. O., & Kadhim, H. I. (2024). *Text Encryption Functions and Decryption using Mathematical*. *5*(July), 121–131.

Thabrani Rahim, Muhardi, F. (2021). Enkripsi Dan Dekripsi File Dokumen Dengan Metode Elgamal. *Prosiding Seminar Ilmiah Sistem Informasi Dan Teknologi Informasi*, *X*(2), 66–73.