CLOUD
Jurnal Networking System and Security System
E-ISSN 3090-6601

Implementasi Kriptografi Kombinasi Algoritma Affine Dan Vigenere Chiper Untuk Keamanan Data Pada *Cloud Database*

Munjiat Setiani Asih[1], Rismayanti[2], Diah Rizki[3*]
[1,2,3] Universitas Harapan, Medan, Indonesia

[1]munjiat.stth@gmail.com, [2]risma.stth@gmail.com, [3*]Diahrizkyyy07@gmail.com
[*)] Diahrizkyyy07@gmail.com

Abstrak− keamanan data merupakan aspek krusial dalam pengelolaan cloud database, terutama mengingat meningkatnya ancaman terhadap privasi dan integritas informasi. Penelitian ini mengkaji implementasi kriptografi dengan mengombinasikan dua algoritma klasik, yaitu Affine cipher dan Vigenere cipher, untuk meningkatkan keamanan data pada cloud database. Algoritma Affine cipher berperan dalam enkripsi awal, sementara Vigenere cipher digunakan sebagai lapisan enkripsi tambahan untuk memperkuat keamanan. Tujuan dari kombinasi ini adalah untuk menciptakan sebuah sistem enkripsi yang lebih kompleks dan sulit ditembus, sehingga dapat mengurangi risiko kebocoran data. Metodologi yang digunakan dalam penelitian ini meliputi analisis algoritma, pengembangan sistem, serta pengujian efektivitas dan efisiensi proses enkripsi dan dekripsi data. Hasil pengujian menunjukkan bahwa kombinasi kedua algoritma ini berhasil meningkatkan tingkat keamanan data tanpa mengorbankan performa sistem secara signifikan. Dengan demikian, implementasi ini diharapkan dapat menjadi solusi yang efektif dalam menjaga kerahasiaan dan integritas data pada cloud database, serta memberikan kontribusi positif dalam pengembangan teknologi keamanan informasi.

Kata kunci: Keamanan, kriptografi, algoritma, awan, basis data

Abstract− Data security is a crucial aspect of cloud database management, especially given the growing threats to privacy and information integrity. This research examines the implementation of cryptography by combining two classical algorithms, namely the Affine cipher and Vigenere cipher, to enhance data security in cloud databases. The Affine cipher algorithm is used for initial encryption, while the Vigenere cipher is applied as an additional encryption layer to strengthen security. The goal of this combination is to create a more complex and robust encryption system, thereby reducing the risk of data breaches. The methodology used in this study includes algorithm analysis, system development, and testing the effectiveness and efficiency of the encryption and decryption processes. Test results show that the combination of these two algorithms successfully increases the level of data security without significantly compromising system performance. Thus, this implementation is expected to be an effective solution for maintaining the confidentiality and integrity of data in cloud databases, while also contributing positively to the development of information security technology.

Keywords: Security, cryptography, algorithm, cloud, database

1. PENDAHULUAN

Perkembangan teknologi digital telah mengubah in*form*asi secara drastis dalam beberapa tahun terakhir. Fenomena ini didorong oleh percepatan dalam penggunaan data digital yang semakin meluas, yang sebagian besar disimpan dalam database. Namun, seiring dengan meningkatnya jumlah dan pentingnya data yang disimpan, keamanan data menjadi semakin krusial. Keamanan ini mencakup aspek-aspek seperti kerahasiaan, ketersediaan, dan integritas data, yang harus diatasi secara serius. keamanan dan kerahasiaan data adalah salah satu aspek paling penting dalam sistem in*form*asi saat ini[1]. Menurut [2] masalah keamanan merupakan salah satu aspek yang krusial dalam setiap sistem in*form*asi modern. Namun, sayangnya, sering kali masalah keamanan ini kurang mendapat perhatian yang cukup dari pemilik dan pengelola sistem in*form*asi. Hal ini dapat memiliki konsekuensi serius, terutama jika in*form*asi rahasia jatuh ke tangan pihak yang tidak berwenang, seperti pesaing bisnis atau penjahat *cyber*. Kerugian yang timbul dari kebocoran in*form*asi ini bisa berupa hilangnya kepercayaan pelanggan, kerugian finansial, atau bahkan dampak hukum yang signifikan bagi perusahaan.Pesatnya perkembangan ilmu pengetahuan dan teknologi telah memungkinkan munculnya teknik-teknik baru yang dapat dimanfaatkan untuk mengancam keamanan sistem in*form*asi. Risiko in*form*asi jatuh ke tangan pihak yang tidak berwenang dapat menimbulkan kerugian besar bagi pemilik in*form*asi. Untuk mencegah hal ini, diperlukan upaya untuk merahasiakan pesan atau in*form*asi yang hanya dapat dipahami oleh pihak-pihak yang ditentukan, suatu ilmu yang dikenal dengan nama kriptografi [3].

Kriptografi adalah ilmu yang mempelajari teknik matematis yang terkait dengan aspek keamanan in*form*asi seperti tingkat keyakinan, integritas data, autentikasi entitas, dan autentikasi keaslian data. Kriptografi bertujuan agar informasi yang bersifat rahasia, integrasi data, dan ontentika yang dikirim melalui suatu jaringan internet, tidak

dapat diketahui dan dimanfaatkan oleh orang lain atau pihak yang tidak berkepentingan [4]. Kriptografi dibagi menjadi dua jenis yaitu kriptografi simetris dan kriptografi asimetris[5]. Teknik-teknik kriptografi ini mencakup berbagai metode seperti *affine cipher*, *vigenere cipher*. Penggunaan metode ini memungkinkan untuk mengamankan data dengan cara mengenkripsi in*form*asi sehingga hanya pihak yang memiliki kunci atau pengetahuan khusus yang dapat memahaminya. Salah satu teknik kriptografi yang paling tua dan paling sederhana adalah *affine cipher*[6]. Metode ini menggunakan teknik substitusi dimana setiap huruf dalam teks pesan digantikan oleh huruf lain yang berjarak beberapa posisi di dalam alfabet. *Vigenere cipher*, di sisi lain, menggunakan tabel tabulasi huruf yang disebut tabula rekta, yang memungkinkan pengguna untuk mengenkripsi teks pesan menggunakan kata kunci. Setiap huruf dalam kata kunci menentukan pergeseran yang berbeda dalam proses enkripsi. Hal ini membuat *Vigenere cipher* lebih kuat dari pada affine caesar cipher karena lebih sulit untuk dipecahkan, terutama jika panjang kata kunci cukup panjang dan acak [7]

Permasalahan pada penelitian ini dalam hal keamanan untuk ntegritas data dan ketersediaan data yang saat ini pada *cloud database* masih menggunakan enkripsi manual yaitu menggunakan MD5 (Message-Digest algortihm 5) merupakan fungsi hash (prosedur terdefinisi atau fungsi matematika yang mengubah variabel dari suatu data yang berukuran besar menjadi lebih sederhana) yang digunakan dalam pesan teks yang berasal dari komunikasi pada plat*form* media berbasis website sehingga perlu diterapkan Implementasi kriptografi pada *cloud database*. Salah satu pendekatan yang dapat diterapkan untuk meningkatkan keamanan adalah dengan menggabungkan algoritma kriptografi seperti *Affine cipher* dan *Vigenere cipher*. Kombinasi ini memanfaatkan keunggulan masing-masing algoritma untuk menciptakan lapisan keamanan yang lebih kuat. Misalnya, *Affine cipher* dapat digunakan untuk mengenkripsi data pada tahap awal, sementara *Vigenere cipher* dapat digunakan sebagai lapisan tambahan untuk meningkatkan kompleksitas enkripsi.

Penelitian yang dilakukan [8] dengan judul Implementasi Algoritma *Affine cipher* Dan Caesar Cipher Dalam Mengamankan Data Teks menyimpulkan bahwa kedua algoritma kriptografi ini memberikan pendekatan yang berbeda namun efektif dalam melindungi kerahasiaan in*form*asi. *Affine cipher*, dengan kombinasi substitusi dan pergeseran matematis, menyediakan tingkat keamanan yang lebih tinggi dibandingkan dengan Caesar Cipher yang sederhana. Adapun penelitian lainnya yang dilakukan oleh [9] dengan judul Implementasi Kriptografi *Vigenere cipher* untuk Keamanan Data In*form*asi Desa menyimpulkan bahwa penggunaan teknologi ini memberikan lapisan keamanan tambahan yang penting. *Vigenere cipher*, dengan prinsip substitusi polialfabetik menggunakan kata kunci sebagai kunci enkripsi, memungkinkan untuk menghasilkan pesan terenkripsi yang sulit untuk dipecahkan tanpa memiliki kunci yang tepat. Vigenere cipher merupakan pengambangan dari caesar cipher, pada dasarnya vigenere cipher mirip dengan caesar cipher perbedaannya adalah pada vigenere cipher setiap huruf pada pesan aslinya digeser sebanyak satu huruf pada kuncinya sedangkan caesar cipher setiap huruf pesannya digeser sebanyak satu huruf yang sama[10] Secara keseluruhan, implementasi algoritma kriptografi seperti *Affine cipher*, dan *Vigenere cipher* memiliki peran krusial dalam upaya melindungi kerahasiaan dan integritas data. Pemilihan algoritma harus mempertimbangkan kompleksitas keamanan yang dibutuhkan serta karakteristik dan konteks penggunaan data. Dengan menggunakan pendekatan yang tepat dan mengikuti praktik-praktik keamanan yang baik, data yang terdapat pada *cloud database* dapat perlindungan yang baik. Berdasarkan penjelasan diatas maka penulis mempunyai ide melakukan penelitian dengan judul "implementasi kriptografi kombinasi algoritma *Affine cipher* dan *Vigenere cipher* untuk keamanan data pada *cloud database*".

2. METODE PENELITIAN

2.1 Algoritma Affine Chiper

Menurut [11] *Affine cipher* merupakan algoritma kriptografi klasik hasil pengembangan dari *caesar cipher*. Perbedaan yang mendasar dari algoritma ini teletak pada proses enkripsi menggunakan perkalian dengan bilangan yang relatif prima. Algoritma ini menggunakan kunci bilangan relatif prima dan bilangan bulat untuk penggeser. *Affine cipher* termasuk kriptogarfi kunci simetri karena proses enkripsi dan dekripsi menggunakan kunci yang sama. Proses enkripsi dan dekripsi *affine cipher* menggunakan dua jenis kunci untuk mendapatkan *ciphertext* yaitu, kunci *a* sebagai pengali yang merupakan bilangan relatif prima terhadap modulo yang digunakan dan kunci *b* bilangan bulat sebagai penggeser. Kunci *a* harus memiliki invers perkalian sehingga harus memenuhi FPB (a, m) =1. Secara matematis proses enkripsi dan dekripsi sebagai berikut.

Berikut ini rumus Proses enkripsi

$$C_i = (a.P + b)\ mod\ m \quad (1)$$

Berikut ini rumus Proses dekripsi

$$P_i = a^{-1}(C_i - b)\ mod\ m \quad (2)$$

Keterangan :

P_i : *plaintext*

C_i: *ciphertext*

a : kunci bilangan yang relatif prima

b : kunci bilangan *intereger*

a-1 : invers dari *a*

m : modulo yang digunakan

Menurut [12] Berikut ini Langkah Langkah Algoritma *Affine Chiper:*

1. Pemilihan Parameter Kunci

Pilih dua bilangan bulat a dan b sebagai kunci enkripsi dan Pastikan *a* dan ukuran alfabet m (misalnya, 26 untuk alfabet Inggris) adalah bilangan yang coprime (relatif prima).

2. Enkripsi

Konversi Karakter: Ubah setiap karakter dari *plaintext* menjadi indeksnya dalam alfabet (A=0, B=1, ..., Z=25).

Terapkan Fungsi Enkripsi: Gunakan rumus

$$C_i = (a.P + b)\ mod\ m \quad (3)$$

3. Dekripsi

Temukan Invers: Hitung invers a.1 dari a modulo m dengan rumus

$$P_i = a^{-1}(C_i - b)\ mod\ m \quad (4)$$

2.2 Vigenere cipher

Menurut [1] *Vigenere cipher* adalah sebuah teknik kriptografi klasik yang menggunakan tabel *tabula recta* untuk mengenkripsi teks. Metode ini dinamai dari seorang diplomat Prancis, Blaise de Vigenère, yang diketahui menggunakan sistem ini dalam komunikasi rahasia. Sandi Vigenère bekerja dengan cara menggeser setiap huruf pesan asli berdasarkan huruf-huruf kunci yang dibuat sebagai sebuah kata atau frase yang berulang. Prinsip dasar dari *Vigenere cipher* adalah penggunaan polialfabetik, yang berarti setiap huruf dari teks asli dapat dienkripsi dengan cara yang berbeda-beda tergantung pada huruf kunci yang sesuai pada saat itu. Tabel *tabula recta* digunakan untuk menunjukkan hubungan antara huruf-huruf di dalam pesan asli dan huruf-huruf di dalam kunci. Dalam tabel ini, setiap baris dan kolomnya berisi alfabet dari A sampai Z, dimana setiap baris dimulai dengan alfabet A, B, C, dan seterusnya. Jadi, untuk menenkripsi pesan, penerima mengurangkan. *Vigenere cipher* menjadi populer karena kemampuannya mengatasi kelemahan sandi Caesar yang sederhana, di mana sandi Caesar hanya menggunakan satu pergeseran huruf untuk mengenkripsi seluruh pesan. *Vigenere cipher*, di sisi lain, menggunakan kunci yang lebih panjang (biasanya sebuah kata atau frase) yang diulang secara berulang dalam proses enkripsi. Berikut ini rumus dari algoritma *Vigenere cipher* untuk enkripsi dan dekripsi:

Enkripsi: C=(P+K) mod 26 (5)

Keterangan:

P :adalah huruf dalam teks yang ingin dienkripsi.

K :adalah huruf dalam kunci yang digunakan untuk enkripsi.

C :adalah huruf terenkripsi yang dihasilkan.

Dekripsi: P=(C−K+26) mod 26 (6)

Keterangan:

C: adalah huruf terenkripsi yang ingin didekripsi.

K: adalah huruf dalam kunci yang digunakan untuk enkripsi.

P: adalah huruf dalam teks asli yang dihasilkan setelah dekripsi

Berikut ini Langkah Langkah algoritma Vignere chiper

1. Pemilihan Kunci

Pilih kata atau frasa sebagai kunci enkripsi. Kunci ini harus diulang atau dipotong agar panjangnya sama dengan panjang *plaintext*.

2. Persiapan Data

Plaintext: Ubah *plaintext* menjadi huruf kapital dan hilangkan spasi serta karakter non-alfabetik (jika diperlukan)
Kunci: Ubah kunci menjadi huruf kapital dan sesuaikan panjangnya dengan *plaintext* dengan mengulang atau memotong kunci.

3. Enkripsi

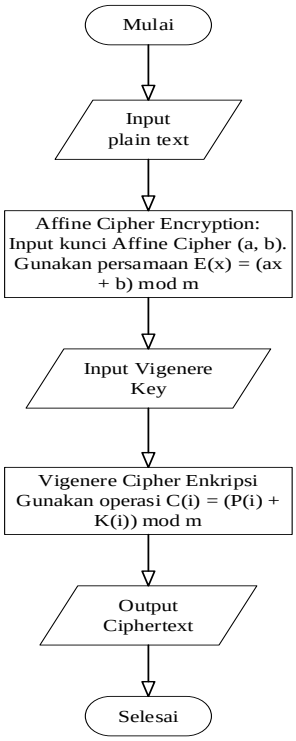
Konversi Karakter: Ubah setiap karakter dari *plaintext* dan kunci menjadi indeksnya dalam alfabet (A=0, B=1, ..., Z=25).

4. Dekripsi

Konversi Karakter: Ubah *ciphertext* dan kunci menjadi indeksnya dalam alfabet.

2.3 Flowchart Algoritma

Flowchart untuk kombinasi algoritma Affine cipher dan Vigenere cipher menggambarkan urutan langkah-langkah yang diambil dalam proses enkripsi dan dekripsi data. Berikut ini flowchart algoritma yang terdapat pada gambar 1. Pada gambar 1 dijelaskan bahwa pada flowchart algoritma akan terdapat Langkah Langkah dari kombinasi algoritma untuk kriptografi pada Langkah awal Pengguna memasukkan teks biasa (plaintext) yang ingin dienkripsi. Teks ini adalah pesan asli yang akan dilindungi kemudian akan diproses oleh algoritma affine chipper dan vignere chipper yang akan menghasilkan Hasil akhir dari proses enkripsi adalah *ciphertext*, yaitu teks yang sudah dienkripsi sepenuhnya dan siap untuk disimpan atau dikirim.



Gambar 1. Flowchart system

3. HASIL DAN PEMBAHASAN

3.1 Kombinasi Algoritma Affine cipher Dan Vigenere cipher

Analisis kombinasi algoritma Affine cipher dan Vigenere cipher dalam implementasi kriptografi untuk keamanan data pada Cloud database menunjukkan bahwa kedua algoritma ini saling melengkapi dalam meningkatkan kompleksitas enkripsi. Affine cipher, yang merupakan cipher substitusi linear, bekerja dengan mengubah setiap huruf dari teks asli menjadi huruf lain berdasarkan persamaan matematika linear. Meskipun efektif dalam memberikan tingkat dasar enkripsi, Affine cipher memiliki kelemahan, terutama ketika pola dalam cipher text dapat dianalisis untuk memecahkan kunci. Di sinilah Vigenere cipher berperan penting. Vigenere cipher menggunakan kunci yang lebih kompleks dengan pergeseran karakter berdasarkan kunci yang berulang, sehingga menambah lapisan keamanan dan menyulitkan analisis frekuensi atau pola. Kombinasi kedua algoritma ini

menghasilkan enkripsi berlapis yang lebih sulit dipecahkan dibandingkan jika digunakan secara terpisah. Proses enkripsi dimulai dengan Affine cipher untuk mengubah teks asli, yang kemudian dienkripsi lebih lanjut menggunakan Vigenere cipher. Hasilnya adalah cipher text yang memiliki kompleksitas lebih tinggi dan lebih tahan terhadap berbagai jenis serangan kriptanalisis, seperti brute-force dan analisis frekuensi. Dalam konteks cloud database, di mana data sering kali menjadi target serangan, kombinasi ini menawarkan perlindungan tambahan dengan menggabungkan kecepatan dan kesederhanaan Affine cipher dengan ketahanan Vigenere cipher. Hal ini memastikan bahwa bahkan jika salah satu kunci atau metode berhasil dipecahkan, lapisan kedua dari enkripsi tetap menjaga keamanan data. Kombinasi ini tidak hanya meningkatkan keamanan tetapi juga memperkuat integritas data, sehingga memberikan solusi yang lebih komprehensif dalam melindungi informasi sensitif di cloud. Untuk memberikan simulasi perhitungan yang jelas, akan menjalankan contoh sederhana menggunakan kombinasi Affine cipher dan Vigenere cipher.

1. Affine cipher

   Affine cipher menggunakan dua parameter kunci, yaitu a dan b, untuk mengenkripsi setiap huruf dalam teks asli. Persamaan enkripsinya adalah:

   $E(x) = (a \times x + b) \bmod 26$

   Dimana:

   x Ini adalah nilai posisi dari suatu huruf dalam alfabet. Dalam sistem ini, alfabet diindeks dari 0 hingga 25, di mana A = 0, B = 1, C = 2, ..., hingga Z = 25. Dengan kata lain, setiap huruf dalam alfabet diberikan nilai numerik yang sesuai dengan urutannya.

   a dan **b**: Ini adalah kunci yang digunakan dalam proses enkripsi dan dekripsi. Keduanya merupakan bilangan bulat.

   a: Bilangan ini digunakan sebagai faktor pengali dalam algoritma *Affine cipher*. Agar algoritma ini berfungsi dengan benar, a dan 26 (jumlah huruf dalam alfabet) harus relatif prima. Dua bilangan dikatakan relatif prima jika tidak ada bilangan selain 1 yang dapat membagi kedua bilangan tersebut secara sempurna. Dalam matematika, ini berarti bahwa a harus dipilih sedemikian rupa sehingga tidak memiliki faktor pembagi bersama dengan 26, kecuali 1. Contoh nilai a yang dapat digunakan adalah 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, dan 25.

   b: Ini adalah bilangan bulat yang ditambahkan setelah pengalian dengan a. Nilai ini tidak harus memenuhi syarat khusus seperti a, tetapi dipilih sebagai bagian dari kunci untuk memberikan tambahan kerumitan pada proses enkripsi

   Misalkan kita ingin mengenkripsi kata "HELLO" menggunakan $a = 5$ dan $b = 8$.

   a. H = 7 → *E* (7) = (5 × 7 +8) mod 26 = 43 mod 26 = 17 (R)
   b. E = 4 → *E* (4) = (5× 4+ 8) mod 26 = 28 mod 26 = 2 (C)
   c. L = 11 → *E* (11) = (5× 11 + 8) mod 26 = 63 mod 26 = 11 (L)
   d. L = 11 → *E* (11) =6 3 mod 26 = 11 (L)
   e. O = 14 → *E* (14) = (5× 14 +8) mod 26 = 78 mod 26= 0 (A)

   Hasil enkripsi *Affine cipher* adalah "RCLLA".

2. Vigenere cipher

   Vigenere cipher menggunakan kunci teks untuk mengenkripsi teks yang telah dihasilkan dari *Affine cipher*. Misalkan kita menggunakan kunci "KEY".

   a. R → K (11) → (17+11) mod 26 = 28 mod 26 =1 (B)
   b. C → E (4) → (2+4) mod 26 = 6 mod 26 = 6 (G)
   c. L → Y (24) → (11+24) mod 26 = 35 mod 26 = 9 (J)
   d. L → K (10) → (11+10) mod 26 = 21 mod 26= 21 (V)
   e. A → E (4) → (0+4) mod 26= 4 mod 26= 4 (E)

   Berikut ini penjelasan perhitungan diatas:

   K (11) → (17+10) mod 26 = 27 mod 26=1 (B)

   a) Huruf R memiliki posisi 17 dalam alfabet (dimulai dari A=0).
   b) Huruf K memiliki posisi 10 dalam alfabet.
   c) Enkripsi dilakukan dengan menambahkan posisi huruf R (17) dengan posisi huruf K (10): 17+11=28
   d) Hasilnya adalah 28, tetapi karena kita bekerja dalam modulo 26 maka ambil sisa dari pembagian 28 dengan 26: 28 mod 26=1
   e) Posisi 1 dalam alfabet adalah huruf B, sehingga R dienkripsi menjadi B.

   C → E (4) → (2+4) mod 26 = 6 mod 26 = 6 (G)

   a) Huruf C memiliki posisi 2 dalam alfabet.
   b) Huruf E memiliki posisi 4 dalam alfabet.
   c) Menambahkan posisi C (2) dengan posisi E (4): 2+4=6

d) Karena 6 masih berada dalam rentang 0-25, tidak perlu dilakukan pengurangan.
e) Posisi 6 dalam alfabet adalah huruf G, sehingga C dienkripsi menjadi G.
L → Y (24) → (11+24) mod 26 = 35 mod 26 = 9 (J)
a) Huruf L memiliki posisi 11 dalam alfabet.
b) Huruf Y memiliki posisi 24 dalam alfabet.
c) Menambahkan posisi L (11) dengan posisi Y (24): 11+24=35
d) Mengambil sisa dari pembagian 35 dengan 26: 35mod 26=9
e) Posisi 9 dalam alfabet adalah huruf J, sehingga L dienkripsi menjadi J.
L → K (10) → (11+10) mod 26 = 21 mod 26= 21 (V)
a) Huruf L memiliki posisi 11 dalam alfabet.
b) Huruf K memiliki posisi 10 dalam alfabet.
c) Menambahkan posisi L (11) dengan posisi K (10): 11 + 10 = 21
d) Karena 21 berada dalam rentang 0-25, tidak perlu dilakukan pengurangan.
e) Posisi 21 dalam alfabet adalah huruf V, sehingga L dienkripsi menjadi V.

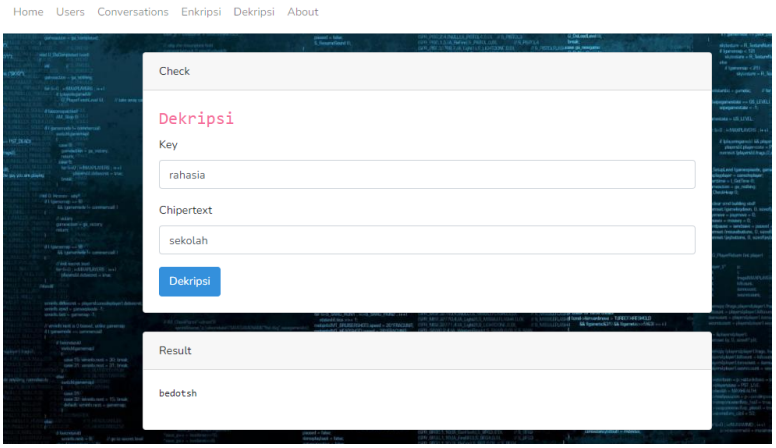
A → E (4) → (0+4) mod 26= 4 mod 26= 4 (E)
a) Huruf A memiliki posisi 0 dalam alfabet.
b) Huruf E memiliki posisi 4 dalam alfabet.
c) Menambahkan posisi A (0) dengan posisi E (4): 0+4 = 4
d) Karena 4 berada dalam rentang 0-25, tidak perlu dilakukan pengurangan.
e) Posisi 4 dalam alfabet adalah huruf E, sehingga A dienkripsi menjadi E.
Hasil akhir setelah menggunakan *Vigenere cipher* adalah "BGJVE".
Kata asli "HELLO" pertama dienkripsi menggunakan *Affine cipher* menjadi "RCLLA", lalu dilanjutkan dengan enkripsi *Vigenere cipher* menggunakan kunci "KEY" untuk menghasilkan teks terenkripsi akhir "BGJVE".

3.2 Tampilan Sistem

Tampilan sistem kriptografi kombinasi algoritma *affine cipher* dan *vigenere cipher* untuk keamanan data pada *cloud database*. Adapun Tampilan yang akan muncul pertama kali ketika menjalankan sistem sebagai berikut

1. Tampilan menu halaman enkripsi

Halaman menu enkripsi bertujuan untuk melakukan enkripsi terhadap pesan untuk dilakukan validasi pada penerapan algoritma. Tampilan menu enkripsi dapat dilihat pada gambar 2 berikut ini



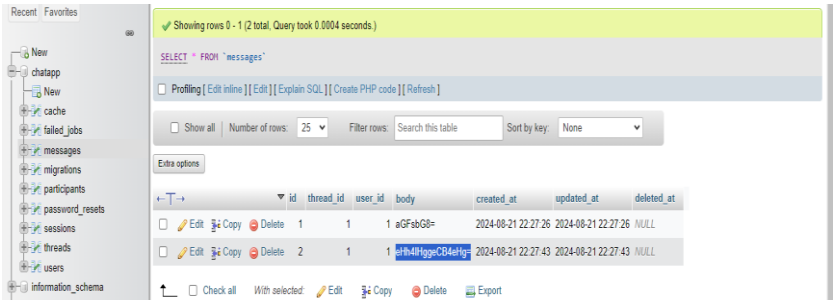
Gambar 2. Halaman menu enkripsi

Keterangan gambar 2 akan menjelaskan bahwa Tampilan menu halaman enkripsi dirancang untuk memberikan pengguna antarmuka yang intuitif dan mudah digunakan dalam proses penyandian data. Pada halaman ini, pengguna akan *input field* untuk memasukkan teks asli yang akan dienkripsi. pengguna dapat menekan tombol

"Enkripsi" yang akan menjalankan proses enkripsi dan menampilkan hasilnya di area output. Antarmuka yang bersih dan terstruktur pada menu ini memastikan bahwa pengguna dapat melakukan enkripsi data dengan efisien dan tanpa kesulitan.

2. Tampilan Database cloud

Tampilan database cloud dengan MySQL memberikan pengguna akses visual yang terstruktur untuk mengelola data secara efisien di lingkungan cloud. Pada halaman ini, pengguna dapat melihat berbagai tabel dan skema yang tersimpan dalam database MySQL mereka, termasuk detail seperti nama tabel, kolom, tipe data, dan jumlah record yang tersimpan. Tampilan database cloud dapat dilihat pada gambar 3 berikut ini.



Gambar 3. Halaman menu *cloud database*

Keterangan gambar 3 menjelaskan antarmuka yang memudahkan pengguna melakukan komunikasi yang sudah aman dengan kombinasi algoritma kriptografi. Tampilan database cloud ini juga akan menamilkan komunikasi yang terenkripsi sehingga tidak dapat dibaca. Untuk dapat memehami pesan harus dilakukan dekripsi pada pesan yang sudah terenkripsi.

4. KESIMPULAN

Berdasarkan rumusan masalah penelitian dan hasil dari penerapan kriptografi kombinasi algoritma *affine cipher* dan *vigenere cipher* untuk keamanan data pada *cloud database*., maka diperoleh kesimpulan sebagai berikut:

1. Kombinasi antara *Affine cipher* dan *Vigenère Cipher* secara signifikan meningkatkan keamanan data yang disimpan di *cloud database*. Dengan dua lapisan enkripsi yang saling melengkapi, proses dekripsi oleh pihak yang tidak berwenang menjadi lebih sulit, sehingga menjaga kerahasiaan dan integritas data dari potensi ancaman.
2. Implementasi kriptografi kombinasi ini terbukti efektif dalam melindungi in*form*asi sensitif di lingkungan *cloud* yang rentan. Penggunaan dua algoritma klasik ini memberikan solusi keamanan yang dapat diandalkan dalam komunikasi percakapan,

REFERENCES

[1] S. Aulansari, D. Sawitri, and A. Ikhwan, “Penerapan kriptografi Vigenere cipher pada keamanan data pesan teks berbasis website,” *J. Inform. Teknol. dan Sains*, vol. 4, no. 4, pp. 421–426, 2022.

[2] M. B. Yel and M. K. M. Nasution, “Keamanan Informasi Data Pribadi Pada Media Sosial,” *J. Inform. Kaputama*, vol. 6, no. 1, pp. 92–101, 2022, doi: 10.59697/jik.v6i1.144.

[3] R. Siringoringo, “Analisis dan Implementasi Algoritma Rijndael (AES) dan Kriptografi RSA pada Pengamanan File,” *KAKIFIKOM Kumpul. Artik. Karya Ilm. Fak*, vol. 2, no. 01, pp. 31–42, 2020.

[4] M. S. Dairi, M. S. Asih, and Khairunnisa, “Implementasi Algoritma Kriptografi RSA Dalam Aplikasi Sistem Informasi Perpustakaaan,” *JIRSI*, vol. 2, no. 1, pp. 214–223, 2023, [Online]. Available: https://jurnal.unity-academy.sch.id/index.php/jirsi/article/view/44/35

[5] M. S. Asih, Rismayanti, M. I. Fadhlurahman, and A. Z. Hasibuan, “Pengembangan Algoritma Vigenere Cipher Berbasis Kunci Dinamis Dalam Pengamanan Pesan Teks,” *JIRSI*, vol. 4, no. 1, pp. 92–99, 2025.

[6] R. Oktafiani, E. I. . Ujianto, and R. Rianto, “Kombinasi Algoritma Kriptografi Vigenere Cipher dan SHA256 untuk Keamanan Basis Data,” *JSON*, vol. 4, no. 3, pp. 433–442, 2023.

[7] V. S. Ginting, “Penerapan Algoritma Vigenere Cipher dan Hill Cipher Menggunakan Satuan Massa,” *J. Teknol. Inf.*, vol. 4, no. 2, pp. 241–246, 2020.

[8] R. Gusmana, H. Haryansyah, and F. Fitria, "Implementasi Algoritma Affine Cipher Dan Caesar Cipher Dalam Mengamankan Data Teks," *Sebatik*, vol. 26, no. 2, pp. 517–524, 2022.

[9] E. Irianti, D. F. Surianto, A. Z. Adistia, M. Juharman, and J. A. Safi'i, "Implementasi Kriptografi Vigenere Cipher untuk Keamanan Data Informasi Desa," *Progress. Information, Secur. Comput. Embed. Syst.*, vol. 1, no. 1, pp. 8–15, 2023.

[10] A. Z. Hasibuan, M. S. Asih, and H. Harahap, "Penerapan QR Code dan Vigenere Cipher dalam Sisem Pelaporan Juru Parkir Ilegal," *QUERY*, vol. 3, no. 1, pp. 53–61, 2019, [Online]. Available: https://jurnal.uinsu.ac.id/index.php/query/article/view/4460/2199

[11] F. Kurniasih, R. Marwati, and R. Sispiyati, "Penggabungan Affine Cipher dan Least Significant Bit-2 untuk Penyisipan Pesan Rahasia pada Gambar," *J. EurekaMatika*, vol. 11, no. 2, pp. 79–88, 2023.

[12] P. G. Pamungkas and A. H. Muhammad, "Modifikasi Algoritma Kriptografi Caesar Chiper pada Deretan Simbol dan Huruf di Smarphone dan Laptop," *J. Inf. Technol.*, vol. 2, no. 1, pp. 1–5, 2022.