

PENERAPAN KEAMANAN DATA DENGAN MENGGUNAKAN METODE CAESAR CHIPER UNTUK MENGAMANKAN DATABASE MYSQL

Meriska Hamni¹, Muhammad Khairul Amri², Sherly Rezeky³, Adnan Buyung Nasution⁴

^{1,2,3,4}Prodi Sistem Informasi, Sains dan Teknologi, UIN Sumatera Utara
email: mhdkhairulamri64@gmail.com

Abstrak: Masalah keamanan tidak menjadi perhatian sebagian besar manajer database. Terlepas dari kenyataan bahwa keamanan basis data sangat penting karena data dapat dicuri dari basis data yang tidak memiliki keamanan. Selain itu, database dapat diakses langsung dengan membuka aplikasi database seperti MySQL yang dapat dibuka di localhost, sehingga memudahkan pencuri atau perusak informasi untuk mengubah atau merusaknya dan menelusuri database secara langsung. Keamanan basis data sebelumnya hanya mengandalkan sistem autentikasi, yang memiliki kelemahan karena seseorang dapat mengetahui kata sandi dan menyebabkan pemalsuan identitas. Kriptografi adalah metode yang digunakan para peneliti dalam hal ini. Diantisipasi bahwa isi database MySQL akan menerima peningkatan keamanan berkat metode Caesar Cipher. Dengan menggunakan aplikasi database MySQL dan program aplikasi Visual Basic 2010, dapat dibuat sebuah program yang dapat mengamankan database MySQL. Manfaatnya adalah aplikasi itu dapat melindungi kumpulan data dengan dua teknik kode yang mudah digunakan Namun, keamanannya sangat baik. Secara alami, tujuannya adalah untuk melindungi database MySQL dari pencuri informasi. Rancangan penelitian ini adalah kualitatif yang bertujuan untuk mencari, menganalisis mengelola peristiwa langsung di lapangan. Metode penelitian kualitatif adalah metode berbasis filosofi yang digunakan dalam eksperimen ilmiah dimana peneliti menggunakan instrumen, metode pengumpulan data, dan analisis kualitatif untuk lebih memfokuskan pada makna.

Kata Kunci : Database, Kriptografi, Caesar Cipher

Abstract: The majority of database managers do not worry about security issues. Despite the fact that data can be stolen from unprotected databases, database security is crucial. In addition, the database can be accessed directly by opening a database application like MySQL on localhost. This makes it easier for thieves or people who destroy information to modify or harm the database and browse it directly. Previously, database security relied solely on authentication systems, which had the drawback that passwords could be cracked and identity impersonation could occur. Researchers employ cryptography as their approach in this regard. The Caesar Cipher method is anticipated to provide greater security for the MySQL database's contents. A program that can secure the MySQL database can be created using the MySQL database application and the Visual Basic 2010 application program. The application has the advantage of being able to protect data sets using two simple code techniques. However, safety is excellent. Naturally, protecting the MySQL database from data thieves is the objective. This research design is qualitative which aims to find, analyze, and manage events directly in the field to understand social interactions through interviews and observations. Qualitative research methods are philosophy-based methods used in scientific experiments where researchers use instruments, data collection methods, and qualitative analysis to focus more on meaning.

Keywords : Caesar Cipher, databases, and cryptography

PENDAHULUAN

Jika menyangkut keamanan, kepentingan publik, dan kepentingan pribadi, suatu informasi akan memiliki nilai yang lebih tinggi. Kriptografi digunakan untuk melindungi informasi berbasis teks, berbagai metode keamanan telah dikembangkan untuk mencapai tujuan dan menjaga kerahasiaan tersebut. Secara khusus, teknik kriptografi digunakan untuk menjaga kerahasiaan data dan menjaga agar tidak dapat diakses oleh individu yang tidak memiliki hak untuk itu. Menjaga kerahasiaan pesan dengan menyandikannya dalam bentuk yang tidak memungkinkan untuk menguraikan maknanya lagi adalah tujuan dari kriptografi, yang merupakan ilmu dan seni.

Basis data merupakan suatu susunan atau kumpulan data operasional yang lengkap dari suatu organisasi atau perusahaan yang diorganisir atau dikelola dan disimpan secara terintegrasi dengan menggunakan metode tertentu menggunakan komputer sehingga mampu menyediakan informasi

optimal yang diperlukan pemakainya atau juga bisa digunakan untuk menyimpan data, membuka data, mengelola banyak data dan juga dapat mengelola informasi.

Berdasarkan beberapa sumber jurnal dan buku yang menjadi referensi kami, metode berbasis teks yang ada dapat digunakan untuk mendapatkan informasi keamanan. Ini akan menjadi modifikasi metode Caesar Cipher yang akan didukung oleh metode Caesar Cipher. Nilai ASCII diubah menjadi biner dalam mekanisme Caesar Cipher, dan kunci berdasarkan rumus Caesar digunakan sebagai gantinya. Di Vernam, Cipher menggabungkan plaintext dengan kunci untuk menghasilkan Cipertxt, dan sebaliknya, Cipher menggabungkan plaintext dengan keystream untuk mengembalikannya. Untuk menghasilkan aplikasi yang mampu memproses enkripsi dan dekripsi, penelitian ini akan menggunakan logika XOR dan XNOR pada Vernam Cipher untuk menghasilkan cipertext.

TINJAUAN PUSTAKA

1. Database

Kumpulan data yang disimpan secara sistematis di komputer dikenal sebagai basis data atau database, dan program komputer dapat digunakan untuk memperoleh informasi dari basis data. Untuk membuat basis data, berbagai perangkat lunak sumber terbuka atau berpelik tersedia. MySQL adalah satu bahasa pemrograman tingkat tinggi yang digunakan dalam perangkat lunak. Kumpulan data MySQL dapat dibuat menggunakan tampilan phpmyadministrator atau melibatkan konten dalam PHP.MySQL adalah perangkat lunak sistem manajemen basis data SQL multithreaded dan multi-pengguna. Faktanya, MySQL adalah turunan dari salah satu konsep utama dalam basis data, yaitu bahwa entri data dan operasi pemilihan dapat dilakukan secara otomatis dan mudah.

2. Keamanan Data

Pengamanan data dan informasi digital dari akses tidak sah, penyalahgunaan, atau pencurian di seluruh jaringan dan sistem yang digunakan dikenal sebagai keamanan data. Dari keamanan fisik perangkat penyimpanan dan administrasi dan kontrol akses hingga keamanan logis aplikasi perangkat lunak, prosedur organisasi, dan kebijakan, keamanan data mencakup semua aspek keamanan informasi.

3. Caesar Cipher

Algoritma caesar cipher adalah metode pengkodean berbasis substitusi pertama yang pernah dikembangkan. Algoritma ROT3 adalah nama lain untuk algoritma tradisional ini. Julius Caesar awalnya menggunakan strategi ini untuk berkomunikasi dengan pasukan garis depan. Caesar menggeser setiap huruf dalam pesan atau mengubah huruf menjadi angka untuk menjaga keamanan data yang dikirim.

METODE

Rancangan penelitian ini adalah kualitatif yang bertujuan untuk mencari, menganalisis, dan mengelola peristiwa secara langsung di lapangan untuk memahami interaksi sosial melalui wawancara dan observasi. Sugiyono (2018:213) mengatakan bahwa metode penelitian kualitatif adalah metode berbasis filosofi yang digunakan dalam eksperimen ilmiah dimana peneliti menggunakan instrumen, metode pengumpulan data, dan analisis kualitatif untuk lebih memfokuskan pada makna. Rencana pendekatan pemeriksaan subyektif untuk dipecah dan menggambarkan kekhasan atau objek pemeriksaan melalui latihan ramah, mentalitas dan pandangan individu secara eksklusif atau dalam pertemuan. Studi ini berlangsung selama lima bulan, dari April 2021 hingga November 2021, dan mencakup analisis kebutuhan, desain sistem, pengumpulan data, pengembangan sistem, pengujian sistem, dan

evaluasi sistem. Penulis penelitian ini bekerja melalui semua fase ini.

HASIL DAN PEMBAHASAN

A. Metode enkripsi Caesar Cipher

Analisis permasalahan yang dapat penulis simpulkan pada Pengamanan data adalah bahwa dalam pelaksanaan operasional pengamanan data pada perusahaan, pada saat ini masih menggunakan metode manual dan belum adanya algoritma kriptografi Caesar Cipher yang berfungsi mengamankan data. Oleh karena itu, proses ini tidak efisien dalam segi waktu yang digunakan. Selain itu, belum adanya penggunaan Algoritma kriptografi Caesar Cipher ini mengakibatkan keamanan data dapat hilang atau diretas. Caesar cipher adalah salah satu algoritma atau sandi kriptografi yang paling sederhana dan paling awal ditemukan. Tipe penyandian yang digunakan oleh caesar cipher adalah substitusi dimana setiap huruf yang ada pada plaintext digeser beberapa tingkatan huruf. Orang yang dapat menterjemahkan pesan tersebut hanyalah orang-orang yang mengetahui bahwa kunci pergeserannya adalah 3. Caesar Cipher adalah salah satu teknik sederhana enkripsi yang mengganti setiap karakter alfabet dengan karakter lain dengan panjang alfabet sejumlah 26. Secara umum rumus enkripsi dan dekripsi Caesar Cipher adalah sebagai berikut:

Enkripsi :

$$E(x)=x +K \bmod 36$$

Dekripsi:

$$D(x)=x-\bmod 36$$

dimana K adalah nilai kunci yang digunakan untuk menggeser setiap karakter x. Misal ingin melakukan enkripsi plaintext yang berisi Nama Nim Jurusan dengan kunci 3, maka huruf N diganti dengan huruf K, huruf N diganti dengan huruf D, huruf J diganti dengan huruf O dan seterusnya. Hasil ciphertext akan berisi KDOR DSD NDEDU. Metode ini memiliki kelemahan yaitu orang lain yang tidak berwenang akan dapat memecahkan cipher text dengan menggunakan metode Brute force dengan cara mencoba semua kunci maupun dengan mencocokkan distribusi frekuensi dari huruf yang muncul.

1. Enkripsi

Berikut ini adalah rumus enkripsi metode caesar Cipher beserta contohnya : Rumus enkripsi caesar cipher :

$$C_i=(P_i+K_i) \bmod 36$$

a. Proses Enkripsi

Prosedur yang mengubah kode yang dapat dipahami (plaintext) menjadi kode yang tidak dapat

dipahami (ciphertext). Misalkan diketahui plaintext sebagai berikut :

“JURUSAN SISTEM INFORMASI”

Dengan menggunakan kunci 3, maka ciphertext yang di dapat yaitu:

Chipertext: MXUXVDQ VLVWHP LQIRUPDVL

Dengan menyandikan setiap huruf bilangan bulat $A=0$, $B=1$, $C=2$, dan $Z=25$, persamaan berikut dapat digunakan untuk menggeser secara matematis tiga huruf alfabet dari teks biasa P menjadi teks sandi C , yang setara dengan melakukan operasi modulo:

$$\begin{aligned} C_i &= P_i + K \text{ Mod } 36 \\ &= J + 3 \text{ Mod } 36 \\ &= 9 + 3 \text{ Mod } 36 \\ &= 12 \text{ mod } 36 \\ &= 12 \text{ dengan huruf "M"} \end{aligned}$$

$$\begin{aligned} C_i &= P_i + K \text{ Mod } 36 \\ &= U + 3 \text{ Mod } 36 \\ &= 20 + 3 \text{ Mod } 36 \\ &= 23 \text{ mod } 36 \\ &= 23 \text{ dengan huruf "X"} \end{aligned}$$

$$\begin{aligned} C_i &= P_i + K \text{ Mod } 36 \\ &= R + 3 \text{ Mod } 36 \\ &= 17 + 3 \text{ Mod } 36 \\ &= 20 \text{ mod } 36 \\ &= 20 \text{ dengan huruf "U"} \end{aligned}$$

$$\begin{aligned} C_i &= P_i + K \text{ Mod } 36 \\ &= U + 3 \text{ Mod } 36 \\ &= 20 + 3 \text{ Mod } 36 \\ &= 23 \text{ mod } 36 \\ &= 23 \text{ dengan huruf "X"} \end{aligned}$$

$$\begin{aligned} C_i &= P_i + K \text{ Mod } 36 \\ &= S + 3 \text{ Mod } 36 \\ &= 18 + 3 \text{ Mod } 36 \\ &= 21 \text{ mod } 36 \\ &= 21 \text{ dengan huruf "V"} \end{aligned}$$

$$\begin{aligned} C_i &= P_i + K \text{ Mod } 36 \\ &= A + 3 \text{ Mod } 36 \\ &= 0 + 3 \text{ Mod } 36 \\ &= 3 \text{ mod } 36 \\ &= 3 \text{ dengan huruf "D"} \end{aligned}$$

$$\begin{aligned} C_i &= P_i + K \text{ Mod } 36 \\ &= N + 3 \text{ Mod } 36 \\ &= 13 + 3 \text{ Mod } 36 \\ &= 16 \text{ mod } 36 \\ &= 16 \text{ dengan huruf "Q"} \end{aligned}$$

$$\begin{aligned} C_i &= P_i + K \text{ Mod } 36 \\ &= S + 3 \text{ Mod } 36 \\ &= 18 + 3 \text{ Mod } 36 \\ &= 21 \text{ mod } 36 \\ &= 21 \text{ dengan huruf "V"} \end{aligned}$$

$$\begin{aligned} C_i &= P_i + K \text{ Mod } 36 \\ &= I + 3 \text{ Mod } 36 \\ &= 8 + 3 \text{ Mod } 36 \\ &= 11 \text{ mod } 36 \\ &= 11 \text{ dengan huruf "L"} \end{aligned}$$

$$C_i = P_i + K \text{ Mod } 36$$

$$\begin{aligned} &= S + 3 \text{ Mod } 36 \\ &= 18 + 3 \text{ Mod } 36 \\ &= 21 \text{ mod } 36 \\ &= 21 \text{ dengan huruf "V"} \end{aligned}$$

$$\begin{aligned} C_i &= P_i + K \text{ Mod } 36 \\ &= T + 3 \text{ Mod } 36 \\ &= 19 + 3 \text{ Mod } 36 \\ &= 22 \text{ mod } 36 \\ &= 22 \text{ dengan huruf "W"} \end{aligned}$$

$$\begin{aligned} C_i &= P_i + K \text{ Mod } 36 \\ &= E + 3 \text{ Mod } 36 \\ &= 4 + 3 \text{ Mod } 36 \\ &= 7 \text{ mod } 36 \\ &= 7 \text{ dengan huruf "H"} \end{aligned}$$

$$\begin{aligned} C_i &= P_i + K \text{ Mod } 36 \\ &= M + 3 \text{ Mod } 36 \\ &= 12 + 3 \text{ Mod } 36 \\ &= 15 \text{ mod } 36 \\ &= 15 \text{ dengan huruf "P"} \end{aligned}$$

$$\begin{aligned} C_i &= P_i + K \text{ Mod } 36 \\ &= I + 3 \text{ Mod } 36 \\ &= 8 + 3 \text{ Mod } 36 \\ &= 11 \text{ mod } 36 \\ &= 11 \text{ dengan huruf "L"} \end{aligned}$$

$$\begin{aligned} C_i &= P_i + K \text{ Mod } 36 \\ &= N + 3 \text{ Mod } 36 \\ &= 13 + 3 \text{ Mod } 36 \\ &= 16 \text{ mod } 36 \\ &= 16 \text{ dengan huruf "Q"} \end{aligned}$$

$$\begin{aligned} C_i &= P_i + K \text{ Mod } 36 \\ &= F + 3 \text{ Mod } 36 \\ &= 5 + 3 \text{ Mod } 36 \\ &= 8 \text{ mod } 36 \\ &= 8 \text{ dengan huruf "I"} \end{aligned}$$

$$\begin{aligned} C_i &= P_i + K \text{ Mod } 36 \\ &= O + 3 \text{ Mod } 36 \\ &= 14 + 3 \text{ Mod } 36 \\ &= 17 \text{ mod } 36 \\ &= 17 \text{ dengan huruf "R"} \end{aligned}$$

$$\begin{aligned} C_i &= P_i + K \text{ Mod } 36 \\ &= R + 3 \text{ Mod } 36 \\ &= 17 + 3 \text{ Mod } 36 \\ &= 20 \text{ mod } 36 \\ &= 20 \text{ dengan huruf "U"} \end{aligned}$$

$$\begin{aligned} C_i &= P_i + K \text{ Mod } 36 \\ &= M + 3 \text{ Mod } 36 \\ &= 12 + 3 \text{ Mod } 36 \\ &= 15 \text{ mod } 36 \\ &= 15 \text{ dengan huruf "P"} \end{aligned}$$

$$\begin{aligned} C_i &= P_i + K \text{ Mod } 36 \\ &= A + 3 \text{ Mod } 36 \\ &= 0 + 3 \text{ Mod } 36 \\ &= 3 \text{ mod } 36 \\ &= 3 \text{ dengan huruf "D"} \end{aligned}$$

$$\begin{aligned} C_i &= P_i + K \text{ Mod } 36 \\ &= S + 3 \text{ Mod } 36 \\ &= 18 + 3 \text{ Mod } 36 \\ &= 21 \text{ mod } 36 \\ &= 21 \text{ dengan huruf "V"} \end{aligned}$$

$$C_i = P_i + K \text{ Mod } 36$$

$$\begin{aligned} &= I + 3 \text{ Mod } 36 \\ &= 8 + 3 \text{ Mod } 36 \\ &= 11 \text{ mod } 36 \\ &= 11 \text{ dengan huruf "L"} \end{aligned}$$

Kemudian diperoleh ciphertext:
MXUXVDQ VLVWHP LQIRUPDVL

b. Proses Deskripsi

Proses mengubah kode dari tidak dapat dipahami (ciphertext) menjadi dapat dimengerti (plaintext) adalah kebalikan dari enkripsi[14].

Chipertext: "MXUXVDQ VLVWHP LQIRUPDVL"

Persamaan berikut memungkinkan penerima pesan untuk mendekripsi ciphertext:

$$\begin{aligned} P_i &= C_i - K \text{ mod } 36 \\ &= M - 3 \text{ mod } 36 \\ &= 12 - 3 \text{ mod } 36 \\ &= 9 \text{ mod } 26 \\ &= 9 \text{ dengan huruf "J"} \\ P_i &= C_i - K \text{ mod } 36 \\ &= X - 3 \text{ mod } 36 \\ &= 23 - 3 \text{ mod } 36 \\ &= 20 \text{ mod } 36 \\ &= 20 \text{ dengan huruf "U"} \\ P_i &= C_i - K \text{ mod } 36 \\ &= U - 3 \text{ mod } 36 \\ &= 20 - 3 \text{ mod } 36 \\ &= 17 \text{ mod } 36 \\ &= 17 \text{ dengan huruf "R"} \\ P_i &= C_i - K \text{ mod } 36 \\ &= X - 3 \text{ mod } 36 \\ &= 23 - 3 \text{ mod } 36 \\ &= 20 \text{ mod } 36 \\ &= 20 \text{ dengan huruf "U"} \\ P_i &= C_i - K \text{ mod } 36 \\ &= V - 3 \text{ mod } 36 \\ &= 21 - 3 \text{ mod } 36 \\ &= 18 \text{ mod } 36 \\ &= 18 \text{ dengan huruf "S"} \\ P_i &= C_i - K \text{ mod } 36 \\ &= D - 3 \text{ mod } 36 \\ &= 3 - 3 \text{ mod } 36 \\ &= 0 \text{ mod } 36 \\ &= 0 \text{ dengan huruf "A"} \\ P_i &= C_i - K \text{ mod } 36 \\ &= Q - 3 \text{ mod } 36 \\ &= 16 - 3 \text{ mod } 36 \\ &= 13 \text{ mod } 36 \\ &= 13 \text{ dengan huruf "N"} \\ P_i &= C_i - K \text{ mod } 36 \\ &= V - 3 \text{ mod } 36 \\ &= 21 - 3 \text{ mod } 36 \\ &= 18 \text{ mod } 36 \\ &= 18 \text{ dengan huruf "S"} \\ P_i &= C_i - K \text{ mod } 36 \\ &= L - 3 \text{ mod } 36 \\ &= 11 - 3 \text{ mod } 36 \end{aligned}$$

$$\begin{aligned} &= 8 \text{ mod } 36 \\ &= 8 \text{ dengan huruf "I"} \\ P_i &= C_i - K \text{ mod } 36 \\ &= V - 3 \text{ mod } 36 \\ &= 21 - 3 \text{ mod } 36 \\ &= 18 \text{ mod } 36 \\ &= 18 \text{ dengan huruf "S"} \\ P_i &= C_i - K \text{ mod } 36 \\ &= W - 3 \text{ mod } 36 \\ &= 22 - 3 \text{ mod } 36 \\ &= 19 \text{ mod } 36 \\ &= 19 \text{ dengan huruf "T"} \\ P_i &= C_i - K \text{ mod } 36 \\ &= H - 3 \text{ mod } 36 \\ &= 7 - 3 \text{ mod } 36 \\ &= 4 \text{ mod } 36 \\ &= 4 \text{ dengan huruf "E"} \\ P_i &= C_i - K \text{ mod } 36 \\ &= P - 3 \text{ mod } 36 \\ &= 15 - 3 \text{ mod } 36 \\ &= 12 \text{ mod } 36 \\ &= 12 \text{ dengan huruf "M"} \\ P_i &= C_i - K \text{ mod } 36 \\ &= L - 3 \text{ mod } 36 \\ &= 11 - 3 \text{ mod } 36 \\ &= 8 \text{ mod } 36 \\ &= 8 \text{ dengan huruf "I"} \\ P_i &= C_i - K \text{ mod } 36 \\ &= Q - 3 \text{ mod } 36 \\ &= 16 - 3 \text{ mod } 36 \\ &= 13 \text{ mod } 36 \\ &= 13 \text{ dengan huruf "N"} \\ P_i &= C_i - K \text{ mod } 36 \\ &= I - 3 \text{ mod } 36 \\ &= 8 - 3 \text{ mod } 36 \\ &= 5 \text{ mod } 36 \\ &= 5 \text{ dengan huruf "F"} \\ P_i &= C_i - K \text{ mod } 36 \\ &= R - 3 \text{ mod } 36 \\ &= 17 - 3 \text{ mod } 36 \\ &= 14 \text{ mod } 36 \\ &= 14 \text{ dengan huruf "O"} \\ P_i &= C_i - K \text{ mod } 36 \\ &= U - 3 \text{ mod } 36 \\ &= 20 - 3 \text{ mod } 36 \\ &= 17 \text{ mod } 36 \\ &= 17 \text{ dengan huruf "R"} \\ P_i &= C_i - K \text{ mod } 36 \\ &= P - 3 \text{ mod } 36 \\ &= 15 - 3 \text{ mod } 36 \\ &= 12 \text{ mod } 36 \\ &= 12 \text{ dengan huruf "M"} \\ P_i &= C_i - K \text{ mod } 36 \\ &= D - 3 \text{ mod } 36 \\ &= 3 - 3 \text{ mod } 36 \\ &= 0 \text{ mod } 36 \\ &= 0 \text{ dengan huruf "A"} \\ P_i &= C_i - K \text{ mod } 36 \\ &= V - 3 \text{ mod } 36 \\ &= 21 - 3 \text{ mod } 36 \end{aligned}$$

$$\begin{aligned}
 &= 18 \bmod 36 \\
 &= 18 \text{ dengan huruf "S"} \\
 P_i &= C_i - K \bmod 36 \\
 &= 11 - 3 \bmod 36 \\
 &= 8 \bmod 36 \\
 &= 8 \text{ dengan huruf "I"}
 \end{aligned}$$

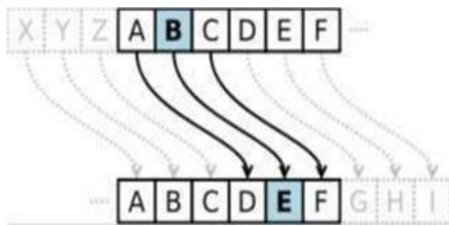
Maka Plaintext yang di dapat adalah:
“JURUSAN SISTEM INFORMASI”

B. Desain Sistem

Aplikasi penerapan metode Caesar Cipher dalam mengamankan database mysql dirancang dengan menggunakan perangkat lunak Visual Studio 2010. Perancangan sistem yang dirancang terdiri dari use case, activity diagram, sequence diagram serta desain dan penjelasan dari sistem yang dirancang.

C. Use Case Diagram

Use case mendiskripsikan sebuah interaksi antara satu atau lebih aktor dengan sistem yang akan dibuat. Use case digunakan untuk mengetahui fungsi yang ada didalam sistem informasi tersebut.

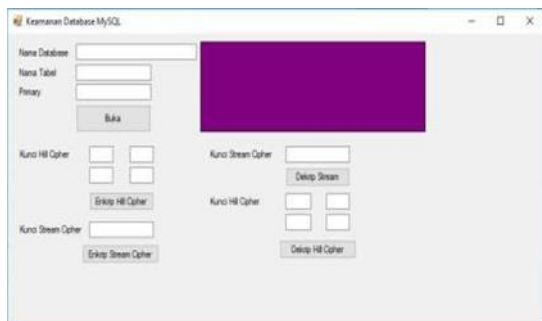


Gambar 1. Use Case penerapan metode Caesar cipher dalam mengamankan Database MYSQL

1. Tampilan Hasil

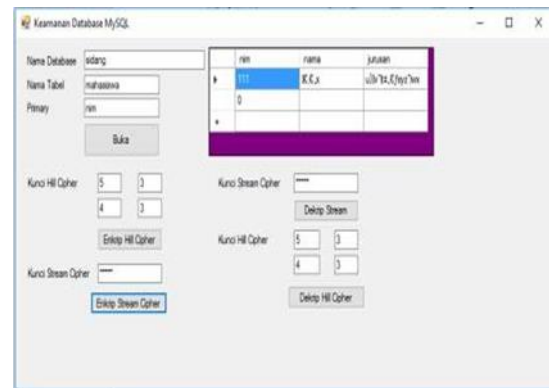
Aplikasi penerapan metode Caesar cipher dalam menggunakan database MySQL memiliki tampilan sebagai berikut :

a. Tampilan Form Keamanan Database MySQL



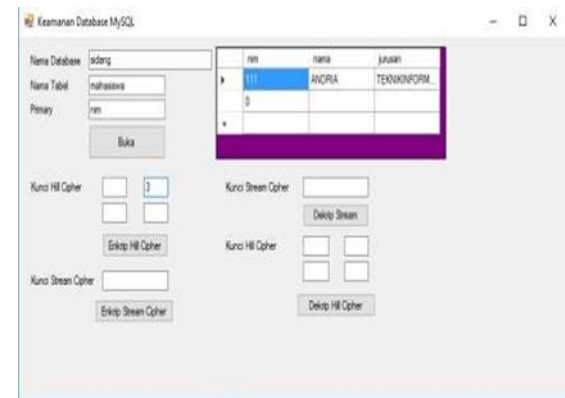
Gambar 2. Tampilan Form Keamanan Database MySQL

b. Tampilan Form Keamanan Database Sebelum di Enkripsi



Gambar 3. Tampilan Form Keamanan Database MySQL Sebelum di Enkripsi

c. Tampilan keamanan Database MySQL Setelah Di Enkripsi



Gambar 4. Tampilan Form keamanan Database MySQL Setelah di Enkripsi

2. Hasil Uji Coba BlackBox

Penulis melakukan pengujian *black box* terhadap aplikasi untuk mengetahui hasil dari perancangan antar muka aplikasi saat dijalankan pada *smartphone* android. Hasil pengujian dapat dilihat pada tabel 1.

Tabel 1. Hasil Uji Coba

No	Form keamanan Database MySQL	Hasil Uji	Validasi
1.	Pengguna mengisi <i>textbox</i> nama database, <i>textbox</i> nama table	Aplikasi menampilkan isi table pada database sesuai dengan nama database, <i>textbox</i> nama	Sesuai

	dan <i>textbox</i> primary kemudian klik <i>button</i> buka	<i>table</i> dan <i>textbox</i> primary	
2.	Isi <i>textbox</i> kunci <i>caesarcipher</i> , kemudian pilih <i>table</i> yang akan dienkrip dan klik <i>button</i> enkripsi	Aplikasi menyandikan isi teks pada <i>table database</i>	Sesuai
3.	Pilih <i>table</i> yang akan didekrip data dan klik <i>button</i> dekrip	Aplikasi membuka pesan asli seluruh isi teks pada <i>table database</i>	Sesuai

KESIMPULAN DAN SARAN

Berdasarkan pembahasan dari bab-bab sebelumnya yang telah dilakukan maka dapat diambil beberapa kesimpulan sebagai berikut :

1. Dengan menggunakan teknik kriptografi dan kemudian menyandikan isi teks database MySQL maka isi teks database MySQL mendapatkan keamanan yang baik.
2. Dengan menggunakan teks database MySQL sebagai input data dan mengubahnya menjadi kode ascii kemudian menggunakan rumus dan langkah dari Caesar cipher maka dapat mengamankan isi database MySQL.
3. Dengan menggunakan pemrograman visual basic 2010 maka dapat menghasilkan aplikasi Penerapan Metode Caesar Cipher Dalam Mengamankan Database MySQL.

Penulis dengan rendah hati masih banyak kekurangan dan belum mencapai target yang diinginkan. Sehingga penulis akan menyempurnakan makalah ini dengan beberapa panduan. Selain itu ada beberapa saran agar aktivitas bisa lebih efektif. Di antaranya adalah: perlunya pelatihan yang telaten dalam menggunakan aplikasi, terutama dalam mengoperasikan MySQL, karena banyak mahasiswa yang belum menguasai dunia pemrograman.

DAFTAR PUSTAKA

- [1] Puspita, K , Wayahdi, M. (2012) "Analisis Kombinasi Metode Caesar Cipher, Vernam Cipher, Dan Hill Cipher Dalam Proses Kriptografi", *International Journal of*

Computer Science and Information Security (IJCSIS), Vol. 10, No. 9.

- [2] Zulham, M, Kurniawan, H, and Rahmad, IF. (2017) "Perancangan Aplikasi Keamanan Data Email Menggunakan Algoritma Enkripsi RC6 Berbasis Android", *Seminar Nasional Informatika (SNIf)*. Vol. 1. No. 1.
- [3] Triandi, B. "Pengembangan Aplikasi Kriptografi Berbasis Bit Inserted Carrier (Bic)", *CSRID jurnal* Vol. 2 No. 2 hal 94-105.
- [4] Rambe, M. R., Haryanto, E. V., & Setiawan, A. (2018). Aplikasi Pengamanan Data dan Disisipkan Pada Gambar dengan Algoritma RSA Dan Modified LSB Berbasis Android. *Konferensi Nasional Sistem Informasi (KNSI) 2018*.
- [5] Sembiring, NS. (2018) . "Perancangan Aplikasi Kriptografi Dengan Metode Modifikasi *Ceaser Cipher* Yang diperkuat Dengan *Vernam Cipher* Untuk Keamanan Teks".
- [6] Pratama, FR. (2016). "Pembelajaran Penyandian Data Di Dalam *Database Mysql* Menggunakan Metode *Vernam Cipher* Dan *Gronsfeld Cipher*".
- [7] Wanto. (2016). "Analisis Mengatasi Sniffing Dan Spoofing Menggunakan Metode Enkripsi Dan Dekripsi Algoritma Hill Cipher", Universitas Sumatera Utara, *Jurnal SNIKOM*, Vol. 4, No. 2.
- [8] Nurwiyati dan Yatini B. (2015). "Enkripsi Dekripsi Data Menggunakan Metode Stream Dan Vigenere Cipher", *STMIK AKAKOM Yogyakarta, Jurnal Informatika*, Vol. 3, No. 23.
- [9] Adhar, D. (2019). Implementasi Algoritma DES (Data Encryption Standard) Pada Enkripsi Dan Deskripsi SMS Berbasis Android. *Jurnal Teknik Informatika Kaputama*, 3(2).
- [10] Kurniawan, H. (2016). Perancangan Aplikasi Chatting Menggunakan Algoritma Vigenere Cipher Sebagai Pengaman Pesan Dalam Jaringan Local Area Network Berbasis Java.