IMPLEMENTASI KRIPTOGRAFI KLASIK UNTUK PENGAMANAN DATABASE BERBASIS WEB

Hidayatullah Sholihin[1], Herlina Latipa Sari[2], Hari Aspriyono[3]

[1]Mahasiswa Program Studi Informatika Fakultas Ilmu Komputer Universitas Dehasen Bengkulu
e-mail : dayatsholihin19@gmail.com
[2]Dosen Tetap Program Studi Informatika Fakultas Ilmu Komputer Universitas Dehasen Bengkulu
e-mail: [2]herlinalatifasari@unived.ac.id, [3]hariaspriyono@gmail.com
Jl. Meranti Raya No. 32 Kota Bengkulu 38228 (Telp. (0736) 22027, 26957 Fax. (0736) 341139

***(received**: November 2021, **revised** : Februari 2022, **accepied** : April 2022)*

ABSTRACT : Database is a fundamental component of an information system, where its development or use must be viewed from a broader perspective based on the needs of the organization. With the database all work becomes easier, both in data processing and viewing the output of the data. However, in addition to this convenience, it takes the security side of each record in the database to maintain data confidentiality. Implementation of Classical Cryptography in database security is made using the PHP Programming Language and MySQL Database. The classical cryptographic algorithm applied in this study is the Railfence Ciper Algorithm. Applications and application databases are uploaded online through the hosting domain https://kriptografihidayat.my.id/ and can be accessed from anywhere and anytime via the internet. Based on the tests that have been carried out, the results show that the application is able to secure the employee database in each storage field, and the functionality of the application runs as expected. The key used cannot be changed dynamically, but can be changed statically because it has been integrated into the program code to perform encryption and decryption on each input field. Record Table in the employee database that has been encrypted using the Railfence Ciper algorithm, so it cannot be read. Wireshark managed to capture the packet, but it was detected that there was an encryption process going on
Keywords: Classical Cryptography, Database, Web-Based

Intisari : *Database* merupakan komponen mendasar suatu sistem informasi, dimana pengembangan atau penggunaannya harus dilihat dari perspektif yang lebih luas berdasarkan kebutuhan organisasi. Dengan adanya *database* semua pekerjaan menjadi lebih mudah, baik dalam pengolahan data maupun melihat output dari data tersebut. Namun di samping kemudahan tersebut, dibutuhkan sisi keamanan pada setiap *record* di dalam *database* agak terjaga kerahasiaan data. Implementasi Kriptografi Klasik dalam pengamanan database dibuat menggunakan Bahasa Pemrograman PHP dan Database MySQL. Algoritma kriptografi klasik yang diterapkan dalam penelitian ini yaitu Algoritma Railfence Chiper. Aplikasi dan database aplikasi diupload secara online melalui hosting domain https://kriptografihidayat.my.id/ dan dapat diakses dari mana saja dan kapan saja melalui internet. Berdasarkan pengujian yang telah dilakukan, didapatkan hasil bahwa Aplikasi mampu mengamankan database karyawan di setiap field penyimpanan, dan fungsionalitas dari aplikasi berjalan sesuai harapan. Kunci yang digunakan tidak dapat diubah secara dinamis, namun dapat diubah secara statis karena sudah terintegrasi ke dalam kode program untuk melakukan enkripsi dan dekripsi pada setiap field yang telah diinputkan. Record Tabel pada database karyawan yang telah dienkripsi menggunakan algoritma *Railfence Chiper*, sehingga tidak dapat dibaca. Wireshark berhasil capturing packet, namun terdeteksi bahwa terdapat proses encryption yang terjadi
Kata Kunci : *Kriptografi Klasik, Database, Berbasis Web*

I. PENDAHULUAN

Teknologi informasi dan Komunikasi saat ini berkembang pesat di berbagai aspek baik Pemerintahan, Kesehatan, Politik, dan lain-lain. Pemanfaatan aplikasi memberikan kemudahan dalam pengaksesannya dan mempermudah proses komputerisasi yang dilakukan. Tidak dipungkiri, kemajuan teknologi sekarang ini sudah merambah di banyak lini kehidupan. Memang sebagai besar membawa kemajuan dan bersifat positif, namun ada pula sisi negatifnya. *Database* merupakan komponen mendasar suatu sistem informasi, Dengan adanya *database* semua pekerjaan menjadi lebih mudah, baik dalam pengolahan data maupun melihat output dari data tersebut. Namun di samping kemudahan tersebut, dibutuhkan sisi keamanan pada setiap *record* di dalam *database* agak terjaga kerahasiaan data.

Adanya kemudahan dalam pengaksesan memberikan celah bagi pihak yang tidak berkepentingan (penyusup) untuk mencuri informasi, memanipulasi data atau bahkan melakukan merusak data. Salah satu pencegahan yang dapat digunakan adalah dengan mengamankan *database* melalui algoritma kriptografi. Dari uraian di atas, penulis mengangkat judul skripsi tentang "**Implementasi Kriptografi Klasik Untuk Pengamanan *Database* Berbasis Web**".

p-ISSN 1858-2680
e-ISSN 2723-4673

II. LANDASAN TEORI

A. Implementasi

Implementasi adalah pelaksanaan atau penerapan. Implementasi suatu proses interaksi antara suatu perangkat tujuan dan tindakan yang mampu untuk meraihnya (Musrifah, 2017).Implementasi adalah suatu tindakan atau pelaksanaan dari sebuah rencana yang sudah disusun secara matang dan terperinci. Implementasi biasanya dilakukan setelah perencanaan sudah dianggap sempurna (Sulehu & Mualo, 2017).

B. Kriptografi

Kriptografi merupakan seni dan ilmu dalam menciptakan sebuah sistem kripto yang mampu menyediakan keamanan informasi. Kriptografi berkaitan erat dengan pengamanan data digital. Ilmu ini terdiri dari mekanisme-mekanisme perancangan yang didasarkan pada algoritma-algoritma matematik yang menawarkan sejumlah layanan keamanan informasi fundamental (Siahaan & Sianipar, 2019).

C. Kriptografi Klasik

Kriptografi klasik merupakan suatu algoritma yang menggunakan satu kunci untuk mengamankan data. Teknik ini sudah digunakan beberapa abad yang lalu. Dua teknik dasar yang biasa digunakan pada algoritma jenis ini adalah (Ariyus & Andri, 2020) :

1. Tenik Substitusi yaitu penggantian setiap karakter teks asli dengan karakter lain
2. Teknik Transposisi (permutasi), teknik ini menggunakan permutasi karakter

D. Bahasa Pemrograman *PHP*

PHP merupakan bahasa pemrograman berbasis web yang memiliki kemampuan memproses mengolah data secara dinamis. PHP dapat di katakan sebagai sebuah *server-side embedded script language*, artinya sintak-sintak dan perintah program yang ditulis akan sepenuhnya dijalankan

E. Konsep Perancangan Basis Data

MySQL adalah sebuah basis data yang mengandung satu atau jumlah tabel. Tabel terdiri atas sejumlah baris dan setiap baris mengandung satu atau sejumlah tabel. Tabel terdiri atas sejumlah baris dan setiap baris mengandung satu atau sejumlah tabel (Hans, 2016).

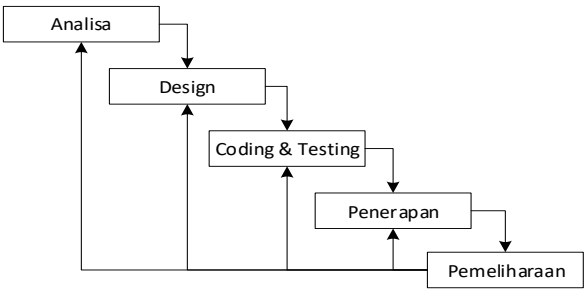
III. METODE PENELITIAN

A. Gambaran Umum Peenelitian

Tempat penelitian ini akan dilaksanakan di CV. Mega Abadi Sejahtera. Dan waktu penelitian akan dimulai pada Bulan Mei 2021 sampai dengan Oktober 2021.

B. Metode Penelitian

Metode penelitian yang diterapkan pada penelitian ini adalah dengan pengembangan metode waterfall. Metode Waterfall memiliki tahapan-tahapan terlihat pada Gambar 3.1.



Gambar .1. Tahapan Metode *Waterfall*

C. Metode Pengumpulan Data

Metode pengumpulan data digunakan untuk memperoleh data yang dapat mendukung permasalahan yang akan dibahas, antara lain :

a. Metode Studi Pustaka

Studi pustaka adalah suatu metode pengumpulan data yang diambil dari perpustakaan atau instansi yang berupa karya ilmiah, jurnal, buku-buku yang berhubungan dengan penulisan ini

b. Metode Observasi

Pada metode ini, penulis melakukan pengamatan langsung di CV. Mega Abadi Sejahtera terhadap objek yang diteliti.

c. Metode Wawancara

Penulis melakukan wawancara dengan memberikan pertanyaan kepada Bapak Suprayitno selaku Direktur CV. Mega Abadi Sejahtera Bengkulu

p-ISSN 1858-2680
e-ISSN 2723-4673

D. Metode Perancangan Sistem

a. Analisis Sistem Aktual

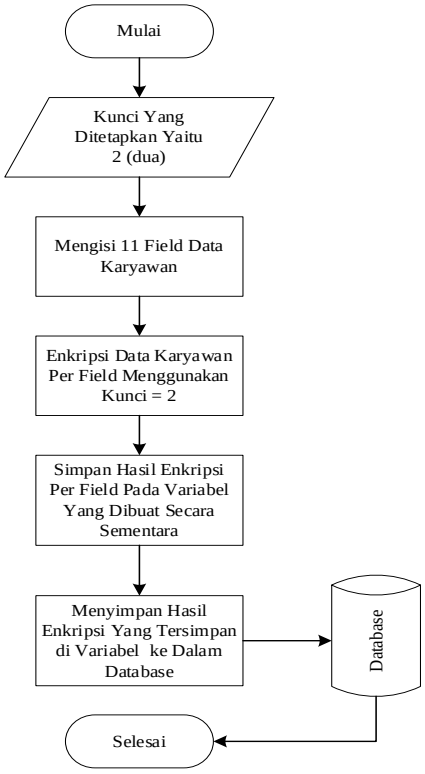
Selama ini pengolahan data pada CV. Mega Abadi Sejahtera sudah menggunakan paket aplikasi office Excel dan Word. Dengan adanya aplikasi tersebut, pihak CV Mega Abadi Sejahtera dapat mendata data karyawan. Namun hal ini menjadi suatu kendala, karena belum adanya aplikasi khusus yang dapat menampung hasil pengolahan data tersebut.

b. Analisis Sistem Baru

Analisis sistem baru dibuat untuk mengatasi permasalahan yang ada pada sistem aktual. Dimana pada sistem baru ini akan dikembangkan suatu aplikasi yang dapat membantu proses pengolahan data karyawan. Pada aplikasi ini, akan disisipkan salah satu algoritma kriptografi klasik yaitu *Railfence Chiper*

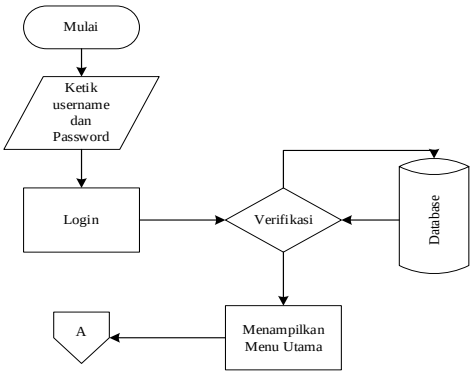
A. Penerapan algoritma railfance chiper

1. Proses Enkripsi Adapun Flowchart Proses Enkripsi
2. Proses Deskripsi

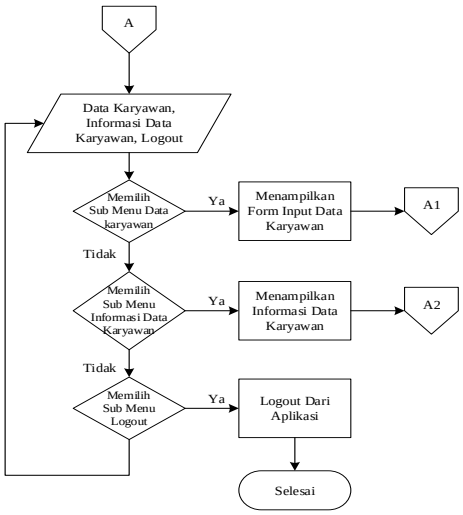


Gambar 2 proses deskripsi

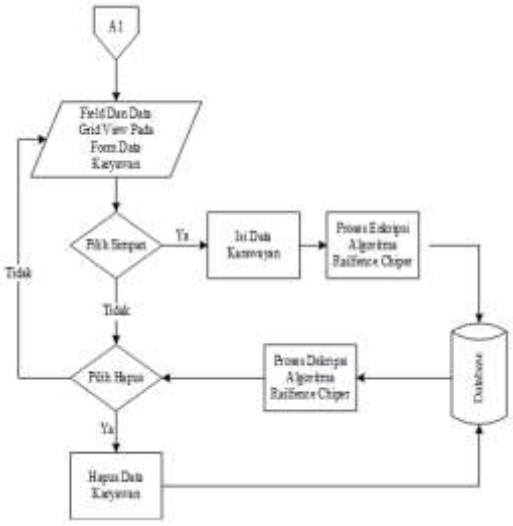
B. Flowchart Sistem



Gambar 3 flowchart login

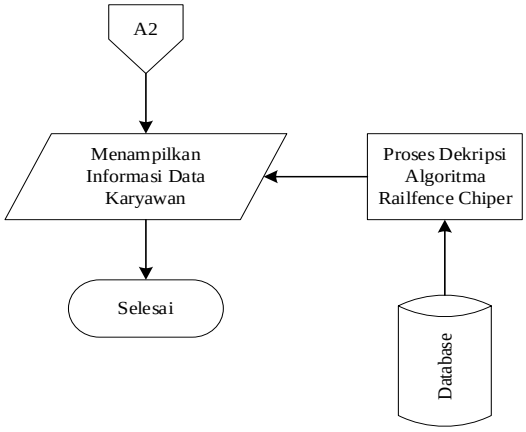


Gambar 4 flowchart menu utama



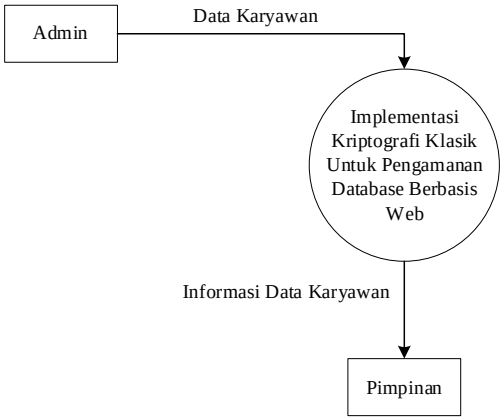
Gambar flowchat .5 flowchart input data karyawan

p-ISSN 1858-2680
e-ISSN 2723-4673

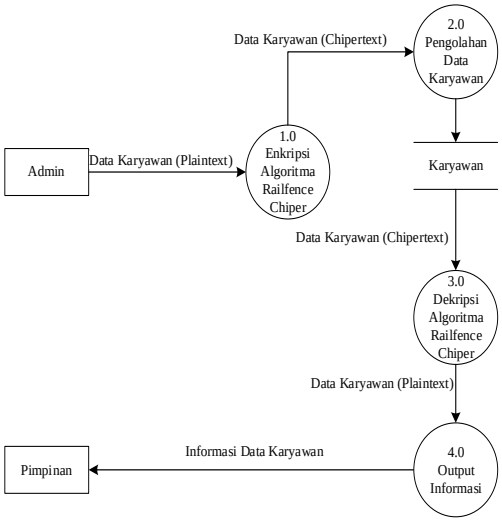


Gambar 6 Flowchart Informasi Data Karyawan

C. Data Flow Diagram



Gambar 7 Diagram Konteks



Gambar.8 Diagram Level 0

IV. HASIL DAN PEMBAHASAN

A. Hasil

Implementasi Kriptografi Klasik dalam pengamanan database dibuat menggunakan Bahasa Pemrograman PHP dan Database MySQL. Algoritma kriptografi klasik yang diterapkan dalam penelitian ini yaitu Algoritma Railfence Chiper. Proses enkripsi dilakukan pada data karyawan yang akan tersimpan ke dalam database. Kunci yang digunakan dalam proses enkripsi dan dekripsi yaitu angka 2 (dua). Kunci tersebut tidak dapat diubah secara dinamis, namun dapat diubah secara statis karena sudah terintegrasi ke dalam kode program untuk melakukan enkripsi dan dekripsi pada setiap field yang telah diinputkan.

Aplikasi dan database aplikasi diupload secara online melalui hosting domain https://kriptografihidayat.my.id/ dan dapat diakses dari mana saja dan kapan saja melalui internet. Adapun menu antarmuka pada sistem keamanan file berbasis jaringan client server, antara lain :

1. Login

Merupakan antarmuka aplikasi yang digunakan untuk masuk ke dalam aplikasi dengan menginputkan data username dan password yang benar. Adapun halaman login seperti Gambar 9

Gambar 9 Tampilan Login

2. Menu Utama

Merupakan antarmuka menu utama yang memiliki sub menu untuk mengolah data karyawan dan melihat informasi data karyawan. Adapun antarmuka menu utama seperti Gambar 10

p-ISSN 1858-2680
e-ISSN 2723-4673

Gambar 10. Menu Utama

3. Data Karyawan

Merupakan antarmuka aplikasi yang digunakan untuk mengolah data karyawan dengan mengisi *field* yang telah disediakan. Pada halaman ini, admin tidak dapat mengoreksi data karyawan, namun admin hanya bisa menambahkan data dan menghapus data karyawan. Pada halaman ini juga telah diterapkan Algoritma *Railfence Chiper* untuk mengenkripsi data karyawan dan menyimpan hasil enkripsi tersebut ke dalam *database*. Halaman ini juga terdapat tabel yang memberikan informasi data karyawan yang telah diinputkan (dekripsi data karyawan). Adapun halaman input data karyawan

Gambar 11. Data Karyawan

4. Informasi Karyawan

Merupakan antarmuka aplikasi yang digunakan untuk melihat informasi data karyawan dimana terjadi proses dekripsi didalamnya sehingga dapat melihat isi teks asli. Adapun halaman informasi data karyawan seperti Gambar 12.

Gambar 12 Informasi Karyawan

B. Pembahasan

Dalam pembahasan ini akan dibahas proses enkripsi dan dekripsi yang terjadi dalam aplikasi ini. Adapun proses enkripsi dan dekripsi tersebut antara lain :

1. Proses Enkripsi

Proses enkripsi terjadi pada form input data karyawan dimana mengisi data seperti Gambar 13

Gambar 13. Mengisi Data Karyawan (Plaintext)

Pada Gambar 14. ini data karyawan tersebut disebut dengan plaintext yang akan diubah menjadi chipertext melalui tombol simpan. Ketika tombol simpan diklik, plaintext tersebut akan diubah ke dalam bentuk chipertext berdasarkan algoritma rail fence chiper yang kemudian hasil chipertext tersebut akan tersimpan ke dalam database, seperti terlihat pada Gambar 14

Gambar 14 Chipertext Yang Tersimpan Dalam Database

2. Proses Dekripsi

Proses dekripsi dilakukan dengan membuka form informasi karyawan, dimana, akan terlihat data karyawan

Gambar 15 Chipertext

Pada gambar . tersebut terlihat chipertext yang tersimpan dalam database, dimana tidak bisa dibaca karena teracak melalui algoritma rail fence chiper. Dalam proses

p-ISSN 1858-2680
e-ISSN 2723-4673

dekripsi, akan dilakukan pengubahan terhadap data chipetext menjadi plaintext, sehingga diperoleh hasil dekripsi seperti Gambar 16., sehingga data karyawan dapat dibaca.

Gambar 16. Hasil Dekripsi (Plaintext)

C. Pengujian Sistem

Pengujian proses enkripsi dan dekripsi menggunakan wireshark antara lain :

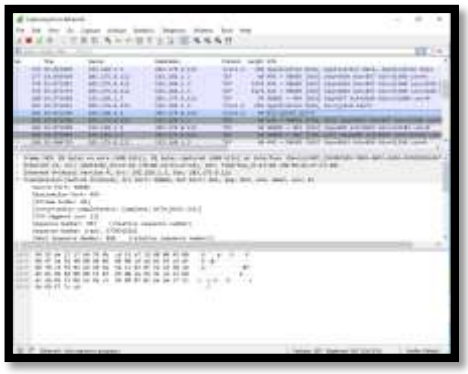
1. Membuka Aplikasi Wireshark seperti Gambar 17.

Gambar 17. Informasi Karyawan

2. Melakukan Capturing pada Interface Ethernet, kemudian klik start seperti Gambar 18

Gambar 18. Start Capturing Packet

3. Adapun hasil Capturing Packets pada saat proses enkripsi dan dekripsi dilakukan, seperti Gambar 19.



Gambar 19. Hasil Capturing

Tersebut terdapat IP Address 203.175.8.112 yang merupakan Shared IP Address dari Domain kriptografihidayat.my.id, seperti Gambar 20

Gambar 20. Shared IP Address kriptografihidayat.my.id

Berdasarkan pengujian yang telah dilakukan melalui Metode Black box dan Wireshark didapatkan hasil bahwa :

1. Aplikasi mampu mengamankan database karyawan di setiap field penyimpanan, dan fungsionalitas dari aplikasi berjalan sesuai harapan
2. Proses enkripsi dilakukan pada data karyawan yang akan tersimpan ke dalam database. Kunci yang digunakan dalam proses enkripsi dan dekripsi yaitu angka 2 (dua).
3. Kunci tersebut tidak dapat diubah secara dinamis, namun dapat diubah secara statis karena sudah terintegrasi ke dalam kode program untuk melakukan enkripsi dan dekripsi pada setiap field yang telah diinputkan.
4. Record Tabel pada database karyawan yang telah dienkripsi menggunakan algoritma *Railfence Chiper*, sehingga tidak dapat dibaca.
5. Wireshark berhasil capturing packet, namun terdeteksi bahwa terdapat proses encryption yang terjadi

p-ISSN 1858-2680
e-ISSN 2723-4673

V. PENUTUP

A. Kesimpulan

Berdasarkan hasil dan pembahasan serta pengujian, maka dapat disimpulkan bahwa :

1. Implementasi Kriptografi Klasik dalam pengamanan database dibuat menggunakan Bahasa Pemrograman PHP dan Database MySQL. Algoritma kriptografi klasik yang diterapkan dalam penelitian ini yaitu Algoritma Railfence Chiper.
2. Aplikasi dan database aplikasi diupload secara online melalui hosting domain https://kriptografihidayat.my.id/ dan dapat diakses dari mana saja dan kapan saja melalui internet.
3. Berdasarkan pengujian yang telah dilakukan, didapatkan hasil bahwa :
   a. Aplikasi mampu mengamankan database karyawan di setiap field penyimpanan, dan fungsionalitas dari aplikasi berjalan sesuai harapan
   b. Kunci yang digunakan tidak dapat diubah secara dinamis, namun dapat diubah secara statis karena
   c. sudah terintegrasi ke dalam kode program untuk melakukan enkripsi dan dekripsi pada setiap field yang telah diinputkan.
   d. Record Tabel pada database karyawan yang telah dienkripsi menggunakan algoritma *Railfence Chiper*, sehingga tidak dapat dibaca.
   e. Wireshark berhasil capturing packet, namun terdeteksi bahwa terdapat proses encryption yang terjadi

B. Saran

Berdasarkan kesimpulan, maka penulis menyarankan agar dapat menggunakan aplikasi ini untuk mengamankan file yang akan dikirim ke komputer lain.

DAFTAR PUSTAKA

[1] Ariyus, D & Andri , R, 2020 *Komunikasi Data*, Yogyakarta : Andi

[2] Hans, A. F., 2016. Sistem Informasi Perpustakaan Online Berbasis Web. *E-Journal Teknik Elektro dan Komputer* , Volume Vol.5 No.2 .

[3] Musrifah, 2017. Implementasi Teknologi Informasi Menggunakan Human Organization Technology (HOT) Fit Model Di Perpustakaan Perguruan Tinggi. *Jurnal Ilmu Perpustakaan dan Informasi*, Volume Vol.2 No.2.

[4] Siahaan, V. & Sianipar, R. H., 2019. *Database Dan Kriptografi Menggunakan Java/MySQL*. Yogyakarta: Sparta Publishing.

[5] Sulehu, M. & Mualo, A., 2017. Implementasi Web Service Dalam Pengembangan Sistem Informasi Akademik Berbasis Mobile Pada STIKES Nani Hasanuddin Makassar. *Jurnal Inspiration* , Volume

p-ISSN 1858-2680
e-ISSN 2723-4673