e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

Expert System to Diagnose Angina Pectoris Disease (Sitting Wind) Using the Naïve Bayes Method

Sistem Pakar Untuk Mendiagnosa Penyakit Angina Pectoris (Angin Duduk) Dengan Menggunakan Metode Naïve Bayes

Intan Diba Aulia Sari [1]; Herlina Latipa Sari [2]; Juju Jumadi [3]
[1]Study Program of Informatics, Faculty of Computer Science, Universitas Dehasen Bengkulu
[2,3] Department of Informatics, Faculty of Computer Science, Universitas Dehasen Bengkulu
Email: [1] intandiba002@gmail.com

How to Cite :
Sari, A, D, I. Sari, L, H. Jumadi, J. (2023). Expert System to Diagnose Angina Pectoris Disease (Sitting Wind) Using the Naïve Bayes Method. Jurnal Media Computer Science, 2(2).

ARTICLE HISTORY
Received [01 Juni 2023]
Revised [27 Juni 2023]
Accepted [15 Juli 2023]

KEYWORDS
Database Security, Cryptography, Rail Fence Cipher

ABSTRAK

Keamanan dan kerahasiaan data atau informasi merupakan salah satu aspek yang penting dari suatu data atau informasi. Masalah keamanan dan kerahasiaan data komputer merupakan sesuatu yang penting dalam era informasi ini terutama bagi Kantor Camat Teluk Segara Kota Bengkulu. Berbagai cara pun dilakukan untuk melindungi data atau informasi tersebut. Salah satunya dengan menggunakan kriptografi dengan algoritma Rail Fence Cipher. Algoritma Rail Fence Cipher menerapkan teknik tranposisi dengan menyusun plaintext pada matrik secara baris. Implementasi sistem menggunakan bahasa pemrograman PHP dengan database MySql. Metode yang digunakan dalam penelitian ini adalah waterfall, aplikasi ini dirancang menggunakan UML (Unified Modelling Language). Dari analisa dan pembahasan penelitian diperoleh bahwa hasil enkripsi yang dihasilkan oleh Rail Fence Cipher tidak merubah hasil plaintext menjadi ciphertext jika kunci dari lebih besar atau banyak dari karakter plaintext.

ABSTRACT

Security and confidentiality of data or information is one of the important aspects of data or information. The issue of security and confidentiality of computer data is something that is important in this information era, especially for the Teluk Segara Sub-District Office, Bengkulu City. Various ways are done to protect the data or information. One of them is by using cryptography with the Rail Fence Cipher algorithm. The Rail Fence Cipher algorithm applies the tranposition technique by arranging the plaintext in the matrix in rows. The system implementation uses PHP programming language with MySql database. The method used in this research is waterfall, this application is designed using UML (Unified Modeling Language). From the analysis and discussion of the research obtained that the encryption results produced by Rail Fence Cipher do not change the plaintext results into ciphertext if the key is greater or more than the plaintext character.

PENDAHULUAN

Perkembangan Ilmu Pengetahuan dan Teknologi (IPTEK) telah menjadikan informasi sebagai kebutuhan primer bagi setiap orang. Data dan informasi merupakan hal vital bagi sebuah instansi baik itu pemerintahan maupun swasta, dimana dengan data dan informasi dapat membantu dalam mengembangkan dan meningkatkan kemampuan bersaing di era globalisasi.Basis data merupakan

sekumpulan informasi yang saling berhubungan secara logis dan berintegrasi sehingga dapat memenuhi kebutuhan suatu organisasi (Hardiansyah & Dewi, 2020).

Keamanan basis data menjadi pertahanan terakhir ketika suatu sistem mengalami serangan dari pihak luar setelah berhasil menembus keamanan jaringan, keamanan sistem operasi dan aplikasi. Kepedulian instansi pemerintahan seperti kantor camat Teluk Segara terhadap data-data kantor serta kurangnya informasi mengenai keamanan data. Aspek keamanan data telah menjadi aspek yang sangat penting dari suatu sistem informasi. Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatu data, pesan dan informasi. Namun, dalam perkembangan teknologi komputer dapat terjadi ancaman dari pihak-pihak yang tidak bertanggung jawab. Pengamanan data dapat dilakukan dengan menggunakan kriptografi. Salah satu cara menjaga keamanan dan kerahasiaan data tersebut yaitu dengan digunakannya algoritma kriptografi untuk melakukan penyandian data.

Penerapan teknik kriptografi pada keamanan database kantor camat dapat melindungi informasi-informasi penting seperti data penilaian kinerja pegawai. Penilaian kinerja dengan form yang sudah ditetapkan. Setiap tahunnya akan dilakukan evaluasi kinerja pegawai untuk mengambil suatu keputusan dan bahan pertimbangan dalam mengetahui kinerja yang diperoleh pegawai tersebut. Adapun kriteria penilaian kinerja pegawai pada Dinas Pendidikan dan Kebudayaan Kabupaten Bengkulu Selatan yaitu Nilai SKP, Orientasi Pelayanan, Integritas, Komitmen, Disiplin, dan Kerjasama

Kriptografi merupakan suatu ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya (Yusfrizal, 2019). Dalam kriptografi, dilakukan enkripsi untuk menyandikan plaintext (pesan asli) menjadi ciphertext (pesan tersandi) dengan mengubah pesan menjadi bentuk lain. Ciphertext tersebut dapat di dekripsi untuk mengembalikannya menjadi plaintext. Rail Fence atau bisa juga disebut alur pagar adalah bentuk penyandian transposisi dengan cara menuliskan huruf-huruf teks asli secara turun naik dalam sebuah pagar imajiner. Teks sandinya dibaca secara baris per baris. Rail Fence Chiper telah diteliti oleh beberapa penelitian seperti yang dilakukan oleh Ajit Singh dkk dengan judul penelitian Implementation of Caesar Cipher with Rail Fence for Enhancing Data Security (Singh et al, 2012).

LANDASAN TEORI

Pengertian Kriptografi

Kriptografi (cryptographi) berasal dari BahasaYunani: “cryptos” artinya “secret” (rahasia), sedangkan “graphein” artinya “writing” (tulisan). Sehingga kriptografi berarti “secret writing” (tulisan rahasia). Jadi kriptografi didefinisikan sebagai ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya kebentuk yang tidak dapat dimengerti lagi maknanya. Secara umum kriptografi merupakan teknik pengamanan informasi yang dilakukan dengan cara mengolah informasi awal (plainteks) dengan suatu kunci tertentu menggunakan suatu metode enkripsi tertentu sehingga menghasilkan informasi baru (chipertext) yang tidak dapat dibaca secara langsung. Chipertext tersebut dapat dikembalikan menjadi informasi awal (plainteks) melalui proses deskripsi (Yanti, Munawir, Zulfan, & Erdiwansyah, 2017).

Kriptografi adalah ilmu untuk mempelajari penulisan secara rahasia dengan tujuan bahwa komunikasi dan data dapat dikodekan (encode/encrypt) dan dikodekan (decode/decrypt) kembali untuk mencegah pihak-pihak lain yang ingin mengetahui isinya. Kriptografi (Cryptography) berasal dari bahasa Yunani yaitu dari kata kryptos yang artinya tersembunyi. Kriptografi dapat diartikan sebagai tulisan yang dirahasiakan atau dapat diartikan juga sebagai suatu ilmu ataupun seni yang mempelajari bagaimana sebuah data, informasi dan dokumen dikonversi kebentuk tertentu yang sulit untuk dimengerti (Hidayatulloh, 2017).

e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

Jenis – Jenis Kriptografi

A.Kriptografi `Klasik

Kriptografi klasik merupakan kriptografi yang digunakan pada zaman dahulu sebelum komputer ditemukan atau sudah ditemukan namun belum secanggih sekarang. Kriptografi ini melakukan pengacakan huruf pada kata terang (plaintext). Kriptografi ini hanya melakukan pengacakan pada huruf A-Z, dan sangatlah tidak disarankan untuk mengamankan informasi-informasi penting karena dapat dipecahkan dalam waktu singkat. Biarpun telah ditinggalkan, kriptografi klasik tetap dapat ditemui disetiap pelajaran kriptografi sebagai pengantar kriptografi modern (Pardede, Manurung, & Filina, 2017)Algoritma kriptografi klasik memiliki ciri di antaranya berbasis karakter dan menggunakan kunci simetri.

Dalam kriptografi klasik, teknik enkripsi yang digunakan adalah enkripsi simetris dimana kunci dekripsi sama dengan kunci enkripsi. (Amin, 2016).

Gambar 1 Proses Enkripsi Dekripsi Kriptografi Klasik

Kriptografi Modern

Algoritma kriptografi modern merupakan suatu perbaikan yang mengacu pada kriptografi klasik. Algoritma ini menggunakan pengolahan simbol biner yang dibentuk dari kode ASCII (American Standard Code for Information Interchange) karena berjalan mengikuti operasi komputer digital, sehingga membutuhkan pengetahuan dasar matematika untuk menguasainya. Algoritma ini memiliki tingkat kesulitan yang kompleks yang menyebabkan kriptanalis sangat sulit memecahkan ciphertext tanpa mengetahui kuncinya. Adapun jenis kunci dalam kriptografi modern terdiri dari 3 yaitu: simetri, asimetri, dan hibrida. Pada kriptografi modern terdapat berbagai macam algoritma yang dimaksudkan untuk mengamankan informasi yang dikirim melalui jaringan komputer. Contoh kriptografi modern yaitu MD5, RC4, AES dan lain-lain (Sumandri, 2017)

Kriptografi modern merupakan suatu perbaikan yang mengacu pada kriptografi klasik. Pada kriptografi modern terdapat berbagai macam algoritma yang dimaksudkan untuk mengamankan informasi yang dikirim melalui jaringan komputer. Algoritma kriptografi modern (Manaor & Pardede, 2017)

a. Algoritma Simetris
   Algoritma simetris adalah algoritma yang menggunakan kunci yang sama untuk enkripsi dan dekripsinya. Algoritma kriprografi simetris sering disebut algoritma kunci rahasia, algoritma kunci tunggal, atau algoritma satu kunci, dan mengharuskan pengirim dan penerima menyetujui suatu kunci tertentu. Kelebihan dari algoritma kriprografi simetris adalah waktu proses untuk enkripsi dan dekripsi relatif cepat. Hal ini disebabkan efesiensi yang terjadi pada pembangkit kunci. Karena prosesnya cepat maka algoritma ini tepat untuk digunakan pada sistem komunikasi digital secara real time.
b. Algoritma Asimetris
   Algoritma Asimetris adalah pasangan kunci kriptografi yang salah satunya digunakan untuk proses enkripsi dan satu lagi deskripsi. Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsi suatu pesan, sedangkan hanya satu orang saja yang memiliki rahasia itu, yang dalam hal ini kunci rahasia untuk melakukan pembongkaran terhadap kode yang dikirim untuknya. Contoh algoritma terkenal yang menggunakan kunci asimetris adalah RSA (Rivest, Shamir dan Adleman).

Algoritma Rail Fence Cipher

Rail Fence Cipher merupakan salah satu variasi implementasi cipher transposisi. Pada Rail Fence Cipher, plaintext dituliskan secara vertikal kebawah sepanjang n-rails, dan menulis lagi ke kolom baru ketika telah mencapai karakter ke-n. Ciphertext yang dihasilkan adalah urutan karakter yang dibaca secara horizontal (Yazid & Haryanto, 2021).

Metode Rail Fence Cipher merupakan salah satu algoritma kriptografi klasik dengan teknik transposisi. Metode transposisi adalah metode yang enkripsi dengan menyusun plaintext pada matriks secara baris, lalu dari hasil susunan tersebut menghasilkan sebuah ciphertext dengan mengambil rangkaian karakter secara kolom (Siregar, Asih, & Wulan, 2019)Rail Fence Cipher digunakan oleh orang Yunani kuno di scytale, sebuah sistem mekanis untuk menghasilkan cipher transposisi. Sistem terdiri dari sebuah silinder dan pita yang melilit silinder. Pesan yang akan dienkripsi ditulis pada pita melingkar. Surat-surat dari pesan asli akan disusun ulang ketika pita dilepas dari silinder. Namun, pesan itu mudah didekripsi ketika pita tersebut ditarik kembali pada silinder dengan diameter yang sama dengan silinder enkripsi.Cipher Rail Fence adalah cipher transposisi yang mudah diaplikasikan yang mengacaukan urutan huruf-huruf pesan dengan cara cepat dan nyaman. Ini juga memiliki keamanan kunci untuk membuatnya sedikit lebih sulit untuk dihancurkan. Cipher Rail Fence berfungsi dengan menulis pesan Anda pada baris alternatif di seluruh halaman, dan kemudian membacakan setiap baris secara bergantian.

Sebagai contoh jika kita ingin mengenkripsi kata " SELAMAT SIANG" maka spasi yang terdapat dalam kalimat dihilangkan kemudian disusun dalam bentuk diagonal membentuk pola zig-zag. Sebagai contoh kita ingin membuat dengan kedalaman (jumlah baris) 3, maka hasil enkripsi dari perubahan susunannya adalah sebagai berikut :

S				M				I			
	E		A		A		S		A		G
		L				T				N	

Maka hasil enkripsi dari kata SELAMAT SIANG menjadi SMIEAASAGLTN.Terdapat pola tertentu berdasarkan jumlah baris yang digunakan. Misal jika ada dua baris maka huruf ke 1,3,5,7,….akan berada dibaris pertama dan huruf ke 2,4,6,… akan berada dibaris kedua. Metode rail fence ini memiliki tingkat keamanan yang rendah sehingga mudah di bobol oleh seorang ahli dengan mencoba beberapa nilai kedalaman untuk menentukan banyaknya baris yang digunakan.

Perancangan Database

Basis Data sebagai kumpulan terorganisasi dari data-data yang berhubungan sedemikian rupa sehingga mudah disimpan, dimanipulasi serta dipanggil oleh pengguna. Terminologi hubungan berarti data mendeskripsikan domain (ranah) tertentu sehingga pengguna mudah untuk mendapatkan jawaban atas pertanyaan yang diajukan ke basis data tersebut. Sedangkan pengertian sistem basis data adalah sebagai koleksi dari data-data yang terorganisasi sedemikian rupa sehingga data mudahdisimpan dan dimanipulasi (diperbarui, dicari, diolah dengan perhitungan-perhitungan tertentu, serta dihapus (Novendri, Saputra, & Firman , 2019).Database adalah kumpulan informasi yang disimpan di dalam komputer secara sistematik, sehingga dapat digunakan oleh suatu program komputer untuk memeroleh informasi dari basis data tersebut. Basis data adalah sekumpulan data yang terhubung satu sama lain secara logika dan suatu deskripsi data yang dirancang untuk memenuhi kebutuhan informasi suatu organisasi atau perusahaan. Jadi Database merupakan suatu sistem atau perangkat lunak yang dibuat untuk mengelola basis data dan menjalankan operasi terhadap data yang dibutuhkan banyak pengguna (Rizki & OP, 2021)

e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

MySQL (My Structure Query Languange)

MySQL adalah sebuah perangkat lunak sistem manajemen basis data SQL (bahasa Inggris: database management system) atau DBMS yang multithread, multi-user, dengan sekitar 6 juta instalasi di seluruh dunia. MySQL AB membuat MySQL tersedia sebagai perangkat lunak gratis di bawah lisensi GNU General Public License (GPL), tetapi mereka juga menjual dibawah lisensi komersial untuk

kasus-kasus dimana penggunaannya tidak cocok dengan penggunaan GPL. Tidak seperti PHP atau Apache yang merupakan software yangdikembangkan oleh komunitas umum, dan hak cipta untuk kode sumber dimiliki oleh penulisnya masing-masing, MySQL dimiliki dan disponsori oleh sebuah perusahaan komersial Swedia yaitu MySQL AB (Wahyuni & Irawan, 2020).MySQL merupakan database server yang bersifat multiuser dan multi-threaded. SQL adalah bahasa database standar yang memudahkan penyimpanan, pengubahan dan akses informasi. Pada MySQL dikenal istilah database dan tabel. Tabel adalah sebuah struktur data dua dimensi yang terdiri dari baris-baris record dan kolom (Nurmalasari et al., 2019).MySQL adalah produk DataBase Management System (DBMS) open sorce yang berjalan pada UNIX, Linux, dan Windows. Sumber dan kode biner MySQL dapat didownload dari situs Web MySQL (http://www.mysql.com). Keterbatasan MySQL tidak mendukung View, prosedur tersimpan, maupun trigger. Akan tetapi, semua hal tersebut ada pada to-do-list MySQL, sehingga periksa dokumentasi terakhir untuk menentukan apakah beberapa fitur-fitur tersebut telah ditambahkan ke produk tersebut pada realese-realese yang terbaru.(Sahi, 2020)

MySQL merupakan database server yang bersifat multiuser dan multi-threaded. SQL adalah bahasa database standar yang memudahkan penyimpanan, pengubahan dan akses informasi. Pada MySQL dikenal istilah database dan tabel. Tabel adalah sebuah struktur data dua dimensi yang terdiri dari baris-baris record dan kolom (Nurmalasari, Anna, & Arissusand, 2019).

Website

Website adalah suatu kumpulan-kumpulan halaman yang menampilkan berbagai macam informasi teks, data, gambar, video maupun gabungan dari semuanya bersifat statis dan dinamis (Nursyanti, Alamsyah and Perdana 2019).

Website awalnya merupakan suatu layanan sajian informasi yang menggunakan konsep hiperlink yang memudahkan surfer (sebutan bagi pemakai komputer yang melakukan penyelusuran informasi di internet) untuk mendapatkan informasi dengan cukup mengklik suatu link berupa teks atau gambar maka informasi dari teks atau gambar akan ditampilkan secara lebih terperinci (Nurmalasari, Anna and Arissusand 2019)

Sedangkan web browser menggambarkan bahwa web browser digunakan untuk menampilkan hasil website yang telah dibuat. Web browser yang paling sering digunakan, di antaranya Mozilla Firefox, Google Chrome, Internet Explorer, Opera, dan Safari (Handayani, Wijianto and Anggoro 2018).

UML (Unified Modeling Laguange)

UML adalah salah satu tool atau model untuk merancang pengembangan software yang berbasis object-oriented. UML sendiri juga memberikan standar penulisan sebuah sistem blueprint, yang meliputi konsep proses bisnis, penulisan kelas-kelas dalam bahasa program yang spesifik, skema database, dan komponen yang diperlukan dalam sistem software (Sonata & Sari, 2019)

UML merupakan bahasa visual untuk pemodelan dan komunikasi mengenai sebuah sistem dengan menggunakan diagram dan teks-teks pendukung". Beberapa pemodelan yang termasuk kedalam pemodelan UML seperti use case diagram, class diagram, activity diagram, dan sequence diagram (Syarif & Nugraha, 2020)

Adapun tujuan dari UML adalah:

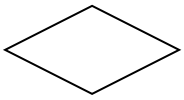
1.Merancang perangkat lunak.
2.Sarana komunikasi antara perangkat lunak dengan proses bisnis.
3.Menjabarkan sistem secara rinci untuk analisa dan mencari apa yang diperlukan sistem.

4.Mendokumentasi sistem yang ada, proses-proses dan organisasinya

Activity Diagram

Activity diagram menggambarkan berbagai aliran aktivitas dalam sistem yang sedang dirancang, bagaimana masing-masing alir berawal, keputusan yang mungkin terjadi, dan bagaimana mereka berakhir (Andrianto dan Softwan, 2018). Pada dasarnya, activity diagram merupakan variasi dari statechart diagram. Activity diagram mempunyai peran seperti halnya flowchart, akan tetapi perbedaannya dengan flowchart adalah activity diagram bisa mendukung perilaku paralel sedangkan flowchart tidak bisa. Berikut adalah notasi activity diagram.

Tabel 1 Notasi Activity Diagram

Gambar	Nama Simbol	Keterangan
	Status Awal	Sebuah diagram aktivitas memiliki sebuah status awal
	Status Akhir	Status akhir yang dilakukan sistem sebuah diagram aktivitas memiliki sebuah status akhir
	Aktivitas	Aktivitas yang dilakukan sistem biasanya diawali dengan kata kerja
	Decision / Percabangan	Percabangan dimana ada pilihan aktivitas yang lebih dari satu
	*Fork*	Digunakan untuk menunjukkan kegiatan yang dilakukan secara paralel atau untuk menggabungkan dua kegiatan paralel menjadi satu

Use Case Diagram

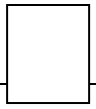
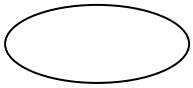
Use case diagram digunakan untuk memodelkan bisnis proses berdasarkan perspektif penggguna (Andrianto dan Softwan, 2018). Use case merupakan sebuah pekerjaan tertentu, misalnya login ke sistem, meng-create sebuah daftar belanja, dan sebagainya.

Seorang/sebuah aktor adalah sebuah entitas manusia atau mesin yang berinteraksi dengan sistem untuk melakukan pekerjaan-pekerjaan tertentu. Use case diagram dapat sangat membantu bila kita sedang menyusun requirement sebuah sistem, mengkomunikasikan rancangan dengan klien, dan merancang test case untuk semua feature yang ada pada sistem. Sebuah use case dapat meng-include fungsionalitas use case lain sebagai bagian dari proses dalam dirinya.

Secara umum diasumsikan bahwa use case yang di-include akan dipanggil setiap kali use case yang meng-include dieksekusi secara normal. Sebuah use case dapat di-include oleh lebih dari satu use case lain, sehingga duplikasi fungsionalitas dapat dihindari dengan cara menarik keluar fungsionalitas yang common. Sebuah use case juga dapat meng-extend use case lain dengan behaviour-nya sendiri. Sementara hubungan generalisasi antar use case menunjukkan bahwa use case yang satu merupakan spesialisasi dari yang lain.

e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

Tabel 2 Simbol Use Case Diagram

Gambar	Nama Simbol	Keterangan
	*Actor*	Menspesifikasikan himpunan peran yang pengguna mainkan ketika berinterasi dengan *Use Case*.
	*Depedency*	Hubungan dimana perubahan yang terjadi pada suatu elemen mandiri (*independent)* akan mempengaruhi elemen yang bergantung padanya elemen yang tidak mandiri (*Independent)*
	*Generalization*	Hubungan dimana objek anak(*Descended)* berbagi prilaku dan struktur data dari objek yang diatasnya objek induk.
	*Include*	Menspesifikasikan bahwa use case sumber secara explicit.
	*Extend*	Menspesifikasikan bahwa use case target memperluas prilaku pada use case sumber pada sebuah titik diberikan.
	Assosiation	Apa yang memhubungkan objek satu dengan objek yang lainnya.
	*System*	Menspesifikasikan paket yang menampilkan sistem secara terbatas.
	*Use Case*	Deskripsi dari urutan aksi-aksi yang ditampilkan sistem yang menghasilkan suatu hasil yang terukur dari sebuah *actor.*
	*Colaboration*	Interaksi aturan-aturan dan elemen lain yang bekerja sama untuk menyediakan prilaku yang lebih besar dari jumlah dan elemen-elemennya.
	*Note*	Elemen fisik yang eksis saat aplikasi dijalankan dan mencerminkan suatu sumber daya komputasi.

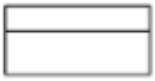
Class Diagram

Class diagram menggambarkan struktur statis dari kelas dalam sistem anda dan menggambarkan atribut, operasi dan hubungan antara kelas (Haviluddin, 2017). Class diagram membantu dalam memvisualisasikan struktur kelas -kelas dari suatu sistem dan merupakan tipe diagram yang paling banyak dipakai. Selama tahap desain, class diagram berperan dalam menangkap struktur dari semua kelas yang membentuk arsitektur sistem yang dibuat.

Class diagram memiliki tiga area pokok:

1.Nama (dan stereotype)
2.Atribut
3.Metoda

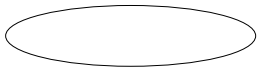
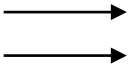
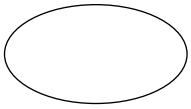
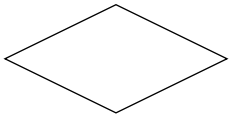
Tabel 3 Simbol Class Diagram

Gambar	Nama Simbol	Keterangan
	*Class*	Himpunan dari objek- objek yang berbagi atribut serta operasi yang sama.
	Associatiom	Apa yang menghubungkan antara objek satu dengan objek lainnya

Flowchart

Flowchart adalah representasi secara simbolik dari suatu algoritma atau prosedur untuk menyelesaikan suatu masalah, dengan menggunakan flowchart akan memudahkan pengguna melakukan pengecekan bagian-bagian yang terlupakan dalam analisis masalah, disamping itu flowchart juga berguna sebagai fasilitas untuk berkomunikasi antara pemrogram yang bekerja dalam tim suatu proyek. Flowchart membantu memahami urutan-urutan logika yang rumit dan panjang. Flowchart membantu mengkomunikasikan jalannya program ke orang lain (bukan pemrogram) akan lebih mudah (Santoso & Nurmalina, 2017).

Tabel 4 Simbol dan Fungsi Flowchart

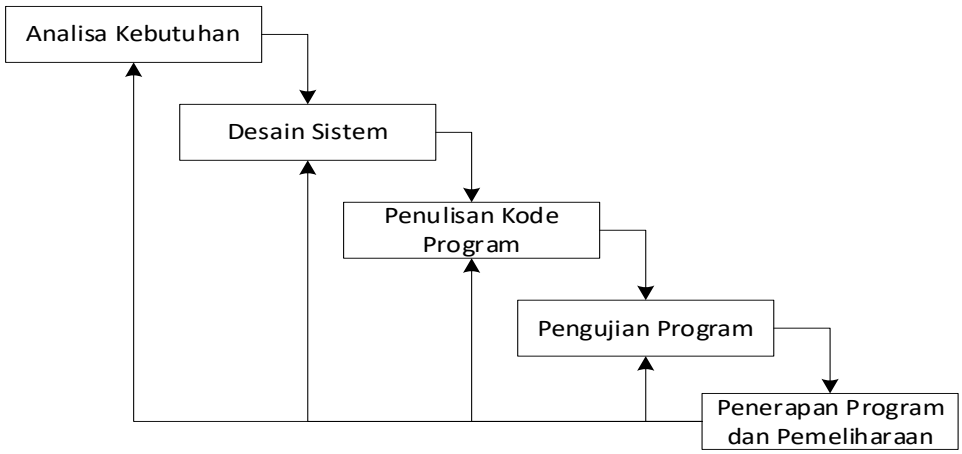
Gambar	Nama Simbol	Keterangan
	*Start / Mulai* *End / Selesai*	Simbol yang digunakan untuk memulai / selesai
	*Flow*	Simbol arus/ *flow* yang menyatakan jalannya proses
	*Connector*	Simbol *connector*, (menyatakan sambungan dari proses ke proses lainnya dalam hal yang sama
	*Process*	Simbol proses yaitu menyatakan suatu tindakan
	*Manual Operation*	Simbol manual, manyatakan suatu tindakan
	*Decision*	Simbol *decision*, menunjukkan suatu kondisi tertentu yang akan menghasilkan dua kemungkinan
	*Keying Operation*	Simbol *keying* operation menyatakan segala jenis operasi yang diproses dengan menggunakan suatu mesin yang mempunyai keyboard
	*Input/Output*	Simbol *input/output* menyatakan proses input/output
	*Document*	Simbol dokumen mencetak keluaran dalam bentuk dokumen

e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

METODE PENELITIAN

Adapun metode penelitian yang digunakan penulis adalah metode pengembangan sistem. Metod pengembangan sistem yang digunakan adalah Waterfall. Adapun tahapan-tahapan metode waterfall, antara lain :

Gambar 2 Tahapan Metode Waterfall

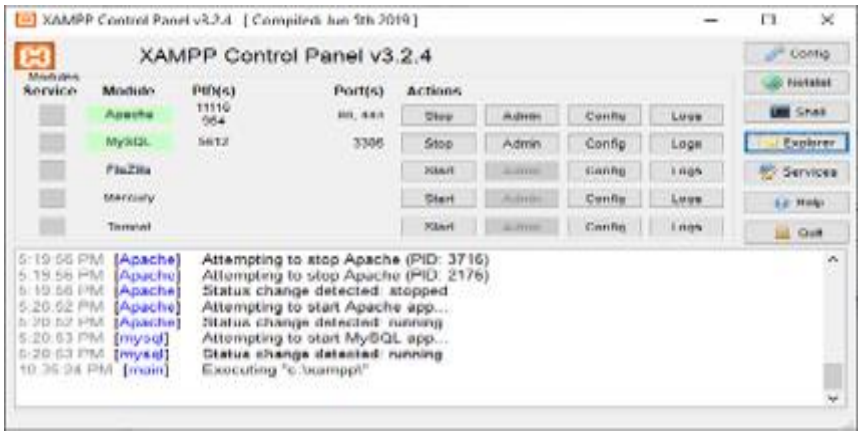


HASIL DAN PEMBAHASAN

Hasil

Aplikasi keamanan database penilaian kinerja pegawai pada Kantor Camat Teluk Segara dibuat menggunakan Bahasa Pemrograman PHP dan Database MySql. Pada aplikasi ini telah diterapkan salah satu algoritma kriptografi klasik yaitu Algoritma Rail Fence Cipher untuk mengamankan isi record database, sehingga yang tersimpan di dalam database record yang telah diacak oleh algoritma tersebut. Aplikasi ini dapat di dijalankan dengan terlebih dahulu mengaktifkan Xampp seperti gambar 3.

Gambar 3 Mengaktifkan Xampp



Pembahasan

Login Aplikasi

Merupakan form yang digunakan untuk membatasi penggunaan aplikasi keamanan database penilaian kinerja pegawai pada Kantor Camat Teluk Segara Kota Bengkulu. Pada form ini user wajib memasukkan username dan password yang benar. Adapun form login seperti gambar 4.

Gambar 4 Login Aplikasi

Menu Utama

Merupakan form yang memiliki sub menu untuk mempermudah user dalam mengelola data penilaian kinerja pegawai pada aplikasi keamanan database nilai kinerja pegawai. Adapun form menu utama seperti gambar 5.

Gambar 5 Menu Utama Aplikasi

Halaman (Form) Data Pegawai

Merupakan form yang digunakan untuk mengolah data pegawai yang terdapat di Kantor Camat Teluk Segara Kota Bengkulu. Adapun tampilan dari data pegawai dapat dilihat pada gambar 6.

Gambar 6 Halaman Data Pegawai

Pada halaman ini terdapat beberapa buttton yang berfungsi untuk melakukan proses di antaranya adalah sebagai berikut :

a.Tambah Pegawai

Halaman tambah data pegawai berfungsi untuk menambah data pegawai yang akan digunakan untuk proses penilaian kinerja dengan menggunakan metode Rail Fence Cipher. Adapun tampilan dari halaman tambah data baru dapat dilihat pada gambar 7.

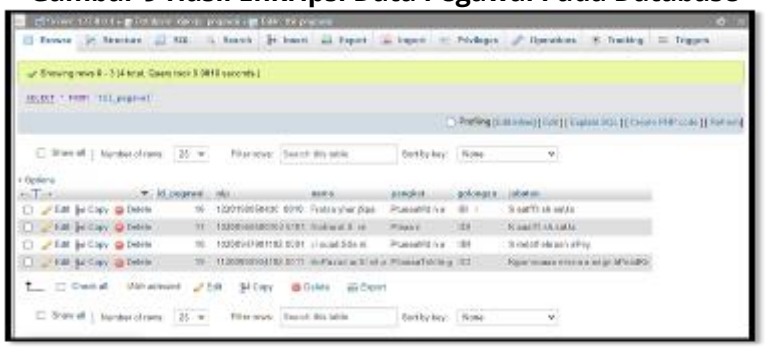
e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

Gambar 7 Halaman Tambah Data Pegawai

Pada halaman tambah data pegawai terdapat tombol “Enkripsi” yang berfungsi untuk proses enkripsi atau merubah plaintext menjadi ciphertext.

Gambar 8 Halaman Hasil Enkripsi Data Pegawai

Gambar 9 Hasil Enkripsi Data Pegawai Pada Database



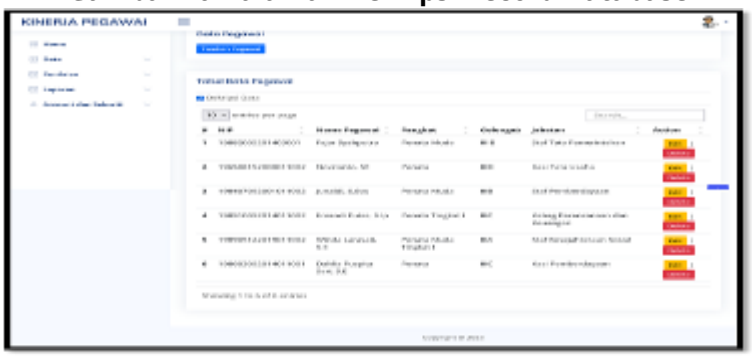
b.Edit

Halaman edit data pegawai untuk melakukan koreksi data pegawai yang telah di input sebelumnya. Adapun tampilan dari halaman edit data pegawai dapat dilihat pada gambar 9.

Gambar 9 Halaman Edit Data Pegawai

Untuk melakukan dekripsi dilakukan dengan memberi tanda pada halaman seperti terlihat pada gambar 10.

Gambar 10 Halaman Dekripsi Record Database



Halaman Penilaian Kinerja Pegawai

Merupakan form yang digunakan untuk mengolah data penilaian kinerja pegawai yang terdapat di Kantor Camat Teluk Segara Kota Bengkulu. Adapun tampilan dari data penilaian kinerja pegawai dapat dilihat pada gambar 11.

Gambar 11 Halaman Data Penilaian Kinerja Pegawai

Pada halaman ini terdapat buttton “Tambah Penilaian” yang berfungsi untuk melakukan proses tambah data penilaian kinerja. Halaman tambah data penilaian kinerja pegawai berfungsi untuk menambah data penilaian pegawai menggunakan metode Rail Fence Cipher. Adapun tampilan dari halaman tambah data baru penilaian kinerja pegawai dapat dilihat pada gambar 12.

Gambar 12 Halaman Tambah Penilaian Kinerja Pegawai

Laporan Kinerja

Merupakan laporan yang menampilkan informasi hasil penilaian kinerja setiap pegawai per tahun. Sebelum menampilkan output laporan hasil penilaian kinerja pegawai, terdapat parameter output yang harus dipilih yaitu tahun dan nama kepala pimpinan (jika terjadi perubahan kepala dinas), seperti Gambat 13.

e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

Gambar 13 Parameter Output Laporan

Setelah memilih parameter output laporan tersebut, klik tombol “Generate Laporan” untuk menampilkan laporan hasil penilaian kinerja pegawai seperti Gambar 14.

Gambar 14 Laporan Hasil Penilaian Kinerja Pegawai

Kunci Enkripsi

Merupakan halaman yang digunakan untuk mengupdate kunci untuk enkripsi dan dekripsi. Adapun halaman update kunci seperti Gambar 15.

Gambar 16 Halaman Update Kunci

Halaman Data User

Merupakan form yang digunakan untuk mengolah data pengguna aplikasi yang terdapat di Kantor Camat Teluk Segara Kota Bengkulu. Adapun tampilan dari data pegawai dapat dilihat pada gambar 16

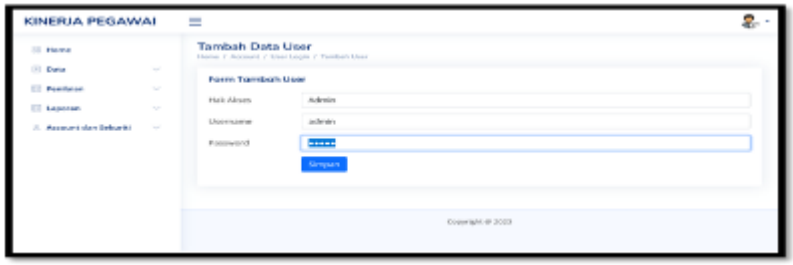
Gambar 16 Halaman Data User

Pada halaman ini terdapat beberapa buttton yang berfungsi untuk melakukan proses di antaranya adalah sebagai berikut :

a.Tambah User

Halaman tambah data user atau pengguna berfungsi untuk menambah data user atau pengguna yang akan diberikan hak akses pada aplikasi ini. Adapun tampilan dari halaman tambah data user baru dapat dilihat pada gambar 17.

Gambar 18 Halaman Tambah Data User



b.Edit

Halaman edit data user untuk melakukan koreksi data user yang telah di input sebelumnya. Adapun tampilan dari halaman edit data user dapat dilihat pada gambar 19.

Gambar 19 Halaman Edit Data User

Pengujian Sistem

Pengujian pada aplikasi keamanan database nilai penilaian kinerja pegawai pada Kantor Camat Teluk Segara Kota Bengkulu dilakukan menggunakan metode blackbox. Adapun hasil pengujian yang tersebut, seperti Tabel 5.

Tabel 5 Hasil Pengujian Sistem

No.	Komponen Yang Diuji	Skenario Pengujian	Hasil Yang Diharapkan	Hasil Pengujian
1.	Form Login	Memasukkan *username* dan *password* yang benar	Sistem berhasil menerima akses *login* tersebut dengan pesan berhasil dan menampilkan halaman menu utama	Sesuai harapan
		Memasukkan username atau password yang salah	Sistem berhasil menolak akses login tersebut dengan pesan kesalahan	Sesuai harapan
2.	Form Input Data Pegawai	menginputkan data pegawai pada *field* yang telah disediakan	Sistem berhasil menyimpan hasil input data pegawai dengan menampilkan pesan berhasil	Sesuai harapan

e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

No.	Komponen Yang Diuji	Skenario Pengujian	Hasil Yang Diharapkan	Hasil Pengujian
		proses enkripsi data pegawai	Sistem berhasil melakukan proses enkripsi data pegawai dan menyimpan data pegawai sebagai ciphertext (data yang sudah diacak)	Sesuai harapan
3	Form Input Data Penilaian Kinerja Pegawai	Menginputkan data pegawai pada *field* yang telah disediakan	Sistem berhasil menyimpan hasil input data pegawai dengan menampilkan pesan berhasil	Sesuai harapan
		Proses dekripsi data pegawai	Sistem berhasil melakukan proses dekripsi pegawai dengan mengubah data ciphertext menjadi data asli untuk memudahkan user mengolah data penilaian kinerja pegawai	Sesuai harapan

KESIMPULAN DAN SARAN

Kesimpulan

1. Aplikasi keamanan database nilai penilaian kinerja pegawai pada Kantor Camat Teluk Segara Kota Bengkulu dibuat menggunakan Bahasa Pemrograman PHP dan Database MySql.
2. Pada aplikasi ini telah diterapkan salah satu algoritma kriptografi Rail Fence Cipher untuk mengamankan isi record database, sehingga yang tersimpan di dalam database record yang telah diacak oleh algoritma tersebut.
3. Hasil enkripsi yang dihasilkan oleh Rail Fence Cipher tidak merubah hasil plaintext menjadi ciphertext jika kunci dari lebih besar atau banyak dari karakter plaintext.

Saran

1. Dapat menggunakan aplikasi ini dengan baik, menjaga data dan password (kunci) untuk keamanan data penilaian kinerja pegawai di Kantor Camat Teluk Segara Kota Bengkulu
2. Bagi peneliti selanjutnya yang akan mengambil penelitian dengan tema serupa atau sama diharapkan dapat lebih meningkatkan keaktifan, dan dapat menambahkan algoritma klasik yang lain atau algoritma modern untuk keamanan data yang lebih baik seperti algoritma Vigenere Cipher, Hill Cipher, DES, AES, Blowfish, RSA, dan lain-lain.

DAFTAR PUSTAKA

Handayani, V. R., Wijianto, R., & Anggoro, A. (2018). Sistem Informasi Pendaftaran Seleksi Kerja Berbasis Web Pada BKK (Bursa Kerja Khusus) Tunas Insan Karya SMK Negeri 2 Banyumas. Jurnal Evolusi, 76-84.

Hardiansyah, A., & Dewi, C. (2020). Perancangan Basis Data Sistem Informasi Perwira Tugas Belajar (Sipatubel) Pada Kementerian Pertahanan. SENAMIKA (Seminar Nasional Mahasiswa Bidang Ilmu Komputer dan Aplikasinya), 222-233.

Mubarak, A. (2019). Rancang Bangun Aplikasi Web Sekolah Menggunakan UML (Unified Modeling Language) Dan Bahasa Pemrograman PHP (Php Hypertext Preprocessor) Berorientasi Objek. JIKO (Jurnal Informatika dan Komputer), 19-25.Novendri, M. S., Saputra, A., & Firman , C. E.

(2019). Aplikasi Inventaris Barang Pada MTS Nurul Islam Dumai Menggunakan PHP Dan Mysql. Lentera Dumai, 46-57.

Nurmalasari, Anna, & Arissusand, R. (2019). Rancang Bangun Sistem Informasi Akuntansi Laporan Laba Rugi Berbasis Web Pada PT. United Tractors Pontianak. Evolusi: Jurnal Sains dan Manajemen, 6-14.

Nursyanti, R., Alamsyah, R. R., & Perdana, S. (2019). Perancangan Aplikasi Berbasis Web Untuk Membantu Pengujian Kualitas Kain Tekstil Otomotif (Studi Kasus Pada PT. Ateja Multi Industri). Explore – Jurnal Sistem Informasi dan Telematika, 153-159.

Pardede, A., Manurung, H., & Filina, D. (2017). Algoritma Vigenere Cipher Dan Hill Cipher Dalam Aplikasi Keamanan Data Pada File Dokumen. Jurnal Teknik Informatika Kaputama (JTIK), 26-33.

Rizki, M. A., & OP, A. (2021). Rancang Bangun Aplikasi E-Cuti Pegawai Berbasis Website (Studi Kasus : Pengadilan Tata Usaha Negara). Jurnal Teknologi dan Sistem Informasi (JTSI), 1-13.

Santoso, & Nurmalina, R. (2017). Perencanaan dan Pengembangan Aplikasi Absensi Mahasiswa Menggunakan Smart Card Guna Pengembangan Kampus Cerdas (Studi Kasus Politeknik Negeri Tanah Laut). Jurnal Integrasi, Vol.9 No.1 April 2017 e-ISSN : 2548-9828.

Siregar, R., Asih, M., & Wulan, N. (2019). Penerapan Algoritma Rc4 Dan Rail Fence Untuk Enkripsi Database Mahasiswa Pada Kampus Poltekkes Kemenkes Medan. JITEKH, 42-50.

Wahyuni, R., & Irawan, Y. (2020). Aplikasi E-Book Untukaturan Kerja Berbasis Web Di Pengadilan Negeri Muara Bulian Kelas II Jambi . Jurnal Ilmu Komputer, 20-26.

Yanti, Y., Munawir, Zulfan, & Erdiwansyah. (2017). Implementasi Sistem Keamanan Database Menggunakan Metode Triangle Chain. Serambi Engineering, 172-175.

Yazid, M., & Haryanto, E. (2021). Perancangan Aplikasi Penyandian File Teks Dengan Menggunakan Algoritma ROT13 Dan Rail Fence Cipher. Jurnal VOI (Voice Of Informatics), 65-77.

Yusfrizal. (2019). Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper Dan Rsa Berbasis Android. Jurnal Teknik Informatika Kaputama (JTIK), 29-37.