

Kombinasi Algoritma *Gronsfeld* Dan Feal Dalam Kerahasiaan Database Penggajian Guru Pada Smp Hang Tuah-2 Medan

A Combination Of The Gronsfeld And Feal Algorithms In The Confidentiality Of The Payroll Database Of Teachers At Smp Hang Tuah-2 Medan

Romanus Repair Ponse sarumaha^{a,1}, Mutiara Sovina^{b,2}

^{a,b}Program Studi Sistem Informasi Universitas Potensi Utama

^{a,b}Universitas Potensi Utama, K.L. Yos Sudarso KM 6,5 No. 3A Tj. Mulia - Medan

Email : romanussarumaha123@gmail.com¹, mutiarasovina@gmail.com²

ABSTRAK

Salah satu ilmu pengamanan data yang terkenal adalah kriptografi. Kriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan, data, atau informasi dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna. Dalam kriptografi, terdapat 2 proses utama, enkripsi dan dekripsi. Enkripsi adalah proses penyandian pesan asli atau plainteks menjadi cipherteks (teks tersandi). Sedangkan dekripsi adalah proses penyandian kembali cipherteks menjadi plainteks (Sari, D. N, 2022).

SMP Hang Tuah-2 Medan merupakan salah satu lembaga pendidikan yang telah berkembang di Kota Medan. SMP Hang Tuah-2 Medan saat ini memiliki sistem pendataan penggajian guru belum menggunakan sistem informasi dengan menggunakan database sebagai penyimpanan data penggajian guru dimana dalam setiap transaksi penggajian guru yang dilakukan diinputkan dalam lembar kerja Microsoft Excel dan disimpan didalam komputer dalam bentuk file sehingga sistem yang ada tersebut mengakibatkan rentan terjadinya pencurian data, manipulasi data yang berdampak buruk terhadap kerahasiaan data penggajian. Berdasarkan permasalahan yang ada saat ini maka penulis akan merancang sebuah sistem informasi menggunakan database dalam penyimpanan data distribusi dimana data yang tersimpan nantinya telah dilakukan teknik enkripsi dengan menggunakan algoritma Gronsfeld Cipher dan FEAL Cipher.

Kata Kunci : Kriptografi, Enkripsi, Dekripsi, Gronsfeld Cipher, FEAL Cipher.

ABSTRACT

One well-known data security discipline is cryptography. Cryptography is the science and art of maintaining the confidentiality of messages, data, or information by disguising them in a meaningless, encrypted form. In cryptography, there are two main processes: encryption and decryption. Encryption is the process of encoding an original message, or plaintext, into ciphertext (encrypted text). Decryption is the process of re-encoding ciphertext into plaintext (Sari, D.N., 2022).

SMP Hang Tuah-2 Medan is one of the developing educational institutions in Medan City. Currently, SMP Hang Tuah-2 Medan's teacher payroll data system does not utilize an information system that uses a database to store teacher payroll data. Each teacher payroll transaction is entered into a Microsoft Excel spreadsheet and stored on the computer as a file. This leaves the system vulnerable to data theft and data manipulation, which negatively impacts payroll data confidentiality. Based on the current problems, the author will design an information system using a database for distributed data storage. The stored data will be encrypted using the Gronsfeld Cipher and FEAL Cipher algorithms.

Keywords: Cryptography, Encryption, Decryption, Gronsfeld Cipher, FEAL Cipher

Info Artikel :

Disubmit: 11 September 2025

Disubmit: 11 September 2025

Disubmit: 11 September 2025

Copyright © 2025 – senadimu. All rights reserved.

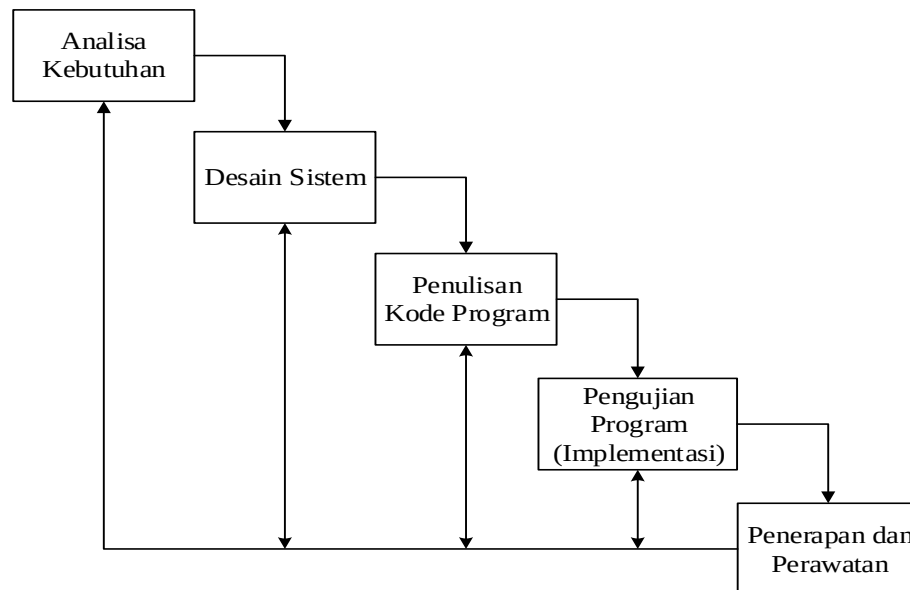
1. PENDAHULUAN

SMP Hang Tuah-2 Medan merupakan salah satu lembaga pendidikan yang telah berkembang di Kota Medan. SMP Hang Tuah-2 Medan saat ini memiliki sistem pendataan penggajian guru belum menggunakan sistem informasi dengan menggunakan database sebagai penyimpanan data penggajian guru dimana dalam setiap transaksi penggajian guru yang dilakukan diinputkan dalam lembar kerja Microsoft Excel dan disimpan didalam komputer dalam bentuk file sehingga sistem yang ada tersebut mengakibatkan rentan terjadinya pencurian data, manipulasi data yang berdampak buruk terhadap kerahasiaan data penggajian.

Keamanan adalah kondisi yang menunjukkan berada dalam keadaan bebas dari ancaman. Keamanan pesan (data atau informasi) dapat diartikan sebagai perlindungan data atau informasi dalam sebuah sistem dari akses yang tidak sah, perubahan, atau kerusakan terhadap data atau informasi tersebut [1]. kriptografi adalah suatu ilmu pengetahuan yang dapat dipelajari pemakaian persamaan matematika dalam melakukan penyandian data [2]. Kriptografi merupakan seni dan ilmu penyandian pesan sehingga tidak dapat lagi dipahami. Metode ini menjaga kerahasiaan pesan. Keamanan data adalah masalah kriptografi. Hal ini mencakup pembuatan proses berbasis algoritma matematika yang menyediakan sejumlah fungsi keamanan informasi utama [3]. Kriptografi adalah cabang ilmu yang memanfaatkan persamaan matematis untuk melakukan enkripsi dan dekripsi data. Teknik ini digunakan untuk mengubah data menjadi kode tertentu, sehingga informasi yang disimpan atau dikirim melalui jaringan yang tidak aman, seperti internet, tidak dapat dibaca oleh pihak yang tidak berwenang [4]. kriptografi merupakan teknik pengamanan informasi yang dilakukan dengan cara mengolah informasi awal (plaintext) dengan suatu kunci tertentu menggunakan suatu metode enkripsi tertentu sehingga menghasilkan informasi baru (ciphertext) yang tidak dapat dibaca secara langsung. Ciphertext tersebut dapat dikembalikan menjadi informasi awal (plaintext) melalui proses deskripsi. [5]. Kriptografi adalah seni dan ilmu untuk mengamankan data yang akan dikirim, dengan menjadikannya kode tertentu dan hanya ditunjukkan kepada orang yang memiliki sebuah kunci untuk mengubah struktur kode itu kembali, yang berfungsi dalam menjaga kerahasiaan data atau pesan [6]. Kriptografi adalah sebuah seni yang berfokus pada menyembunyikan dan mengirimkan pesan secara diam-diam. Banyak sandi yang digunakan sepanjang sejarah, banyak diantaranya sekarang dianggap tidak aman menurut standar modern. Nyatanya, baru pada pertengahan abad ke-20 kriptografi berubah dari seni menjadi sebuah sains [7]. Enkripsi adalah proses dimana informasi atau data sebelum ditransmisikan, diubah menjadi bentuk yang hampir tidak dapat dikenali sebagai informasi awalnya menggunakan algoritma tertentu. [8]. deskripsi, adalah rangkaian proses yang mengeksekusi ciphertext menggunakan kunci rahasia untuk menghasilkan teks asli atau plaintext. [9]. Enkripsi merupakan sebuah proses yang melibatkan penggunaan algoritma khusus untuk mengubah data atau informasi menjadi suatu format yang hampir tidak dapat dikenali atau diidentifikasi sebagai informasi aslinya.[10]. Enkripsi adalah proses pencampuran pesan asli ke dalam pesan lain yang tidak dapat diuraikan seperti pesan aslinya [11]. Gronsfeld merupakan algoritma penyandian yang hanya menggunakan numeric sebagai key. Key tersebut ditetapkan oleh programmer. Cara kerjanya menyerupai sandi Vigenere, dimana akan pengulangan secara periodik untuk kunci dengan tujuan agar panjang plaintek dan kunci sama [12]. . FEAL merupakan enkripsi tipe simetris *block chippers*. FEAL mempunyai panjang blok 64 bit, panjang kunci 64 bit, dan memiliki iterasi sebanyak 8 ronde [13].

2. METODE

Penelitian ini akan melalui beberapa tahapan. Tahapan dalam penelitian ini dapat di modelkan pada diagram *waterfall* yang ditunjukkan pada gambar I.1.



Gambar 1. Diagram Analisa Rancangan dengan *Waterfall*

1. Tahap Analisa Kebutuhan
Spesifikasi *hardware* yang dibutuhkan adalah:
 - a. *Personal Computer*.
 - b. *Harddisk* minimal 320 GB.
 - c. RAM minimal 2 MB.
 - d. *Mouse* dan *Keyboard*.Software yang digunakan adalah *Visual Studio 2010* yang digunakan sebagai penulisan *coding* dan *Microsoft SQL Server 2008 R2*.
2. Tahap Desain Sistem
Pada tahap ini, penulis melakukan perancangan atau desain antar muka aplikasi yang diusulkan menggunakan *Unified Modelling Language (UML)* meliputi rancangan *output*, rancangan *input*, rancangan stuktur data yang digunakan, rancangan struktur sistem dan algoritma sistem.
3. Tahap Penulisan Kode Program
Bahasa pemrograman yang digunakan pada bagian ini yaitu bahasa pemrograman *Visual Studio 2010* dan database *SQL Server 2008 R2*.
4. Tahap Pengujian Program (Implementasi)
Pengujian *software* dilakukan menggunakan *black box* untuk memastikan bahwa sistem yang dibuat telah sesuai dengan desainnya dan semua fungsi dapat dipergunakan dengan baik tanpa ada kesalahan.
5. Tahap Penerapan dan Perawatan
Pada tahapan ini dilakukan monitoring proses, evaluasi dan perubahan (perbaikan) bila diperlukan. Sistem di-*install* dan digunakan secara praktikal. Pemeliharaan meliputi perbaikan kesalahan yang tidak diketahui pada tahapan sebelumnya, memperbaiki implementasi unit sistem dan meningkatkan layanan sistem ketika terdapat kebutuhan baru.

3. HASIL DAN PEMBAHASAN

Bagian hasil dan pembahasan merupakan komponen utama yang menggambarkan *output*

3.1. Penerapan Metode

Berikut ini adalah rumus dan langkah dari metode *Gronsfeld* dan *FEAL Cipher* beserta contoh perhitungannya:

Tabel 1. Daftar Gaji Guru

No	Nama	Jabatan	Status	Gaji Pokok
1	Lasniar MHP Simbolon, S.Pd	Kepsek	Honor	1480000
2	Farida Mariani S, S.pd	PKS-1	Honor	925000
3	Drs. Jamaluddin	PKS-2	Honor	925000
4	Isma Aulia, S.Pdi	PKS-3	Honor	962000
5	Zulfida Ariani, S.Pdi	Guru	Honor	666000

3.2 Proses Enkripsi

1. Enkripsi Algoritma Gronsfeal

$$C_i = (P_i + K_i) \bmod 256 \dots \dots \dots (3.1)$$

Dimana:

C : *Ciphertext* hasil proses enkrip

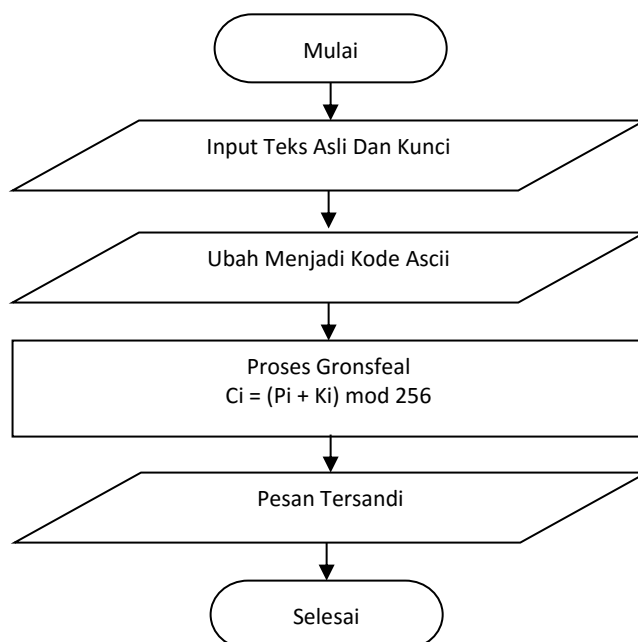
P : *Plaintext* untuk proses enkrip

K : *Key* untuk proses enkrip

mod : Sisa bagi

256 : Total ASCII pada *keyboard*

Flowchart enkrip metode Gronsfeal:



Gambar 2. Flowchart Algoritma Metode Gronsfeal

Data : Lasniar MHP Simbolon, S.Pd

Kunci : 4

$$C1 = (P1+K) \bmod 256$$

$$= (L+4) \bmod 256$$

$$= (76+4) \bmod 256$$

$$= 80 \bmod 256$$

$$= 80$$

$$= P$$

$$C2 = (P2+K) \bmod 256$$

$$= (a+4) \bmod 256$$

$$= (97+4) \bmod 256$$

$$= 101 \bmod 256$$

$$= 101$$

$$= e$$

$$C3 = (P3+K) \bmod 256$$

$$= (s+4) \bmod 256$$

$$= (115+4) \bmod 256$$

$$= 119 \bmod 256$$

$$= 119$$

$$= w$$

$$C4 = (P4+K) \bmod 256$$

$$= (n+4) \bmod 256$$

$$= (110+4) \bmod 256$$

$$= 114 \bmod 256$$

$$= 114$$

$$\begin{aligned} &= r \\ C5 &= (P5+K) \text{ Mod } 256 \\ &= (i+4) \text{ Mod } 256 \\ &= (105+4) \text{ Mod } 256 \\ &= 109 \text{ Mod } 256 \\ &= 109 \\ &= m \\ C6 &= (P5+K) \text{ Mod } 256 \\ &= (a+4) \text{ Mod } 256 \\ &= (97+4) \text{ Mod } 256 \\ &= 101 \text{ Mod } 256 \\ &= 101 \\ &= e \\ C7 &= (P7+K) \text{ Mod } 256 \\ &= (r+4) \text{ Mod } 256 \\ &= (114+4) \text{ Mod } 256 \\ &= 118 \text{ Mod } 256 \\ &= 118 \\ &= v \\ C8 &= (P8+K) \text{ Mod } 256 \\ &= (\text{Space}+4) \text{ Mod } 256 \\ &= (32+4) \text{ Mod } 256 \\ &= 36 \text{ Mod } 256 \\ &= 36 \\ &= \$ \\ C9 &= (P9+K) \text{ Mod } 256 \\ &= (M+4) \text{ Mod } 256 \\ &= (77+4) \text{ Mod } 256 \\ &= 81 \text{ Mod } 256 \\ &= 81 \\ &= Q \\ C10 &= (P10+K) \text{ Mod } 256 \\ &= (H+4) \text{ Mod } 256 \\ &= (72+4) \text{ Mod } 256 \\ &= 76 \text{ Mod } 256 \\ &= 76 \\ &= L \\ C11 &= (P11+K) \text{ Mod } 256 \\ &= (P+4) \text{ Mod } 256 \\ &= (80+4) \text{ Mod } 256 \\ &= 84 \text{ Mod } 256 \\ &= 84 \\ &= T \\ C12 &= (P12+K) \text{ Mod } 256 \\ &= (\text{Space}+4) \text{ Mod } 256 \\ &= (32+4) \text{ Mod } 256 \\ &= 36 \text{ Mod } 256 \\ &= 36 \\ &= \$ \\ C13 &= (P13+K) \text{ Mod } 256 \\ &= (S+4) \text{ Mod } 256 \\ &= (83+4) \text{ Mod } 256 \\ &= 87 \text{ Mod } 256 \\ &= 87 \end{aligned}$$

$$\begin{aligned} &= W \\ C14 &= (P14+K) \text{ Mod } 256 \\ &= (i+4) \text{ Mod } 256 \\ &= (105+4) \text{ Mod } 256 \\ &= 109 \text{ Mod } 256 \\ &= 109 \\ &= m \\ C15 &= (P15+K) \text{ Mod } 256 \\ &= (m+4) \text{ Mod } 256 \\ &= (109+4) \text{ Mod } 256 \\ &= 113 \text{ Mod } 256 \\ &= 113 \\ &= q \\ C16 &= (P16+K) \text{ Mod } 256 \\ &= (b+4) \text{ Mod } 256 \\ &= (98+4) \text{ Mod } 256 \\ &= 102 \text{ Mod } 256 \\ &= 102 \\ &= f \\ C17 &= (P17+K) \text{ Mod } 256 \\ &= (o+4) \text{ Mod } 256 \\ &= (111+4) \text{ Mod } 256 \\ &= 115 \text{ Mod } 256 \\ &= 115 \\ &= s \\ C18 &= (P18+K) \text{ Mod } 256 \\ &= (l+4) \text{ Mod } 256 \\ &= (108+4) \text{ Mod } 256 \\ &= 112 \text{ Mod } 256 \\ &= 112 \\ &= p \\ C19 &= (P19+K) \text{ Mod } 256 \\ &= (n+4) \text{ Mod } 256 \\ &= (110+4) \text{ Mod } 256 \\ &= 114 \text{ Mod } 256 \\ &= 114 \\ &= r \\ C20 &= (P20+K) \text{ Mod } 256 \\ &= (,+4) \text{ Mod } 256 \\ &= (44+4) \text{ Mod } 256 \\ &= 48 \text{ Mod } 256 \\ &= 48 \\ &= 0 \\ C21 &= (P2110+K) \text{ Mod } 256 \\ &= (\text{Space}+4) \text{ Mod } 256 \\ &= (32+4) \text{ Mod } 256 \\ &= 36 \text{ Mod } 256 \\ &= 36 \\ &= \$ \\ C22 &= (P22+K) \text{ Mod } 256 \\ &= (S+4) \text{ Mod } 256 \\ &= (83+4) \text{ Mod } 256 \\ &= 87 \text{ Mod } 256 \\ &= 87 \end{aligned}$$

$$\begin{aligned}
 &= W \\
 C23 &= (P23+K) \text{Mod } 256 \\
 &= (.+4) \text{Mod } 256 \\
 &= (45+4) \text{Mod } 256 \\
 &= 49 \text{ Mod } 256 \\
 &= 49 \\
 &= 1 \\
 C24 &= (P24+K) \text{Mod } 256 \\
 &= (P+4) \text{Mod } 256 \\
 &= (80+4) \text{Mod } 256 \\
 \text{Ciphertext} &: \text{Pewrmev\$QLT\$Wmqfspr0\$W1Th}
 \end{aligned}$$

2. Enkripsi Algoritma *Fast Encryption Algorithm* (FEAL)

$$C_i = (P_i + K) \text{ mod } 256 \dots\dots\dots(3.2)$$

Ket:

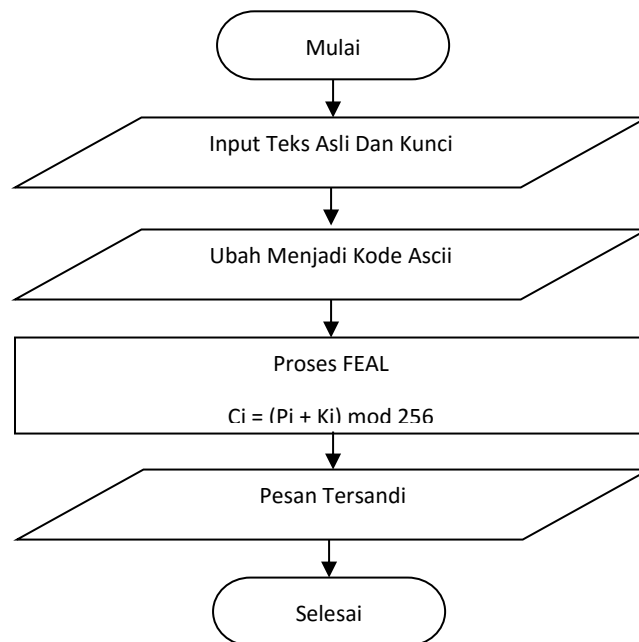
C_i : Ciphertext merupakan pesan yang disandikan, dimana $i = \{1,2,3,4,\dots,n\}$

P_i : Plaintext adalah pesan asli, dengan $i = \{1,2,3,4,\dots,n\}$

K : Kunci parameter untuk transformasi enchipering R Fadillah · 2022

Sebelum melakukan proses penerapan metode atau algoritma dalam penyelesaian masalah, hal yang pertama dilakukan ialah menganalisa sehingga bisa diuraikan permasalahan endskripsi, mengurangi ukuran dan dekripsi data teks hingga ke bentuk semula.

Flowchart enkrip metode FEAL :



Gambar 3. Flowchart Algoritma Metode FEAL

Langkah penyelesaiannya :

Plaintext : Pewrmev\\$QLT\\$Wmqfspr0\\$W1Th

$$\begin{aligned}
 \text{Kunci : } 4 & \\
 C1 &= (P1+K) \text{Mod } 256 \\
 &= (P+4) \text{Mod } 256 \\
 &= (80+4) \text{Mod } 256 \\
 &= 84 \text{ Mod } 256 \\
 &= 84 \\
 C2 &= (P2+K) \text{Mod } 256 \\
 &= (e+4) \text{Mod } 256 \\
 &= (101+4) \text{Mod } 256 \\
 &= 105 \text{ Mod } 256 \\
 &= 105
 \end{aligned}$$

$$\begin{aligned} &= i \\ C3 &= (P3+K) \text{ Mod } 256 \\ &= (w+4) \text{ Mod } 256 \\ &= (119+4) \text{ Mod } 256 \\ &= 123 \text{ Mod } 256 \\ &= 123 \\ &= \{ \\ C4 &= (P4+K) \text{ Mod } 256 \\ &= (r+4) \text{ Mod } 256 \\ &= (114+4) \text{ Mod } 256 \\ &= 118 \text{ Mod } 256 \\ &= 118 \\ &= v \\ C5 &= (P5+K) \text{ Mod } 256 \\ &= (m+4) \text{ Mod } 256 \\ &= (109+4) \text{ Mod } 256 \\ &= 113 \text{ Mod } 256 \\ &= 113 \\ &= q \\ C6 &= (P5+K) \text{ Mod } 256 \\ &= (e+4) \text{ Mod } 256 \\ &= (101+4) \text{ Mod } 256 \\ &= 105 \text{ Mod } 256 \\ &= 105 \\ &= i \\ C7 &= (P7+K) \text{ Mod } 256 \\ &= (v+4) \text{ Mod } 256 \\ &= (118+4) \text{ Mod } 256 \\ &= 122 \text{ Mod } 256 \\ &= 122 \\ &= z \\ C8 &= (P8+K) \text{ Mod } 256 \\ &= (\$+4) \text{ Mod } 256 \\ &= (36+4) \text{ Mod } 256 \\ &= 40 \text{ Mod } 256 \\ &= 40 \\ &= (\\ C9 &= (P9+K) \text{ Mod } 256 \\ &= (Q+4) \text{ Mod } 256 \\ &= (81+4) \text{ Mod } 256 \\ &= 85 \text{ Mod } 256 \\ &= 85 \\ &= U \\ C10 &= (P10+K) \text{ Mod } 256 \\ &= (L+4) \text{ Mod } 256 \\ &= (76+4) \text{ Mod } 256 \\ &= 80 \text{ Mod } 256 \\ &= 80 \\ &= P \\ C11 &= (P11+K) \text{ Mod } 256 \\ &= (T+4) \text{ Mod } 256 \\ &= (84+4) \text{ Mod } 256 \\ &= 88 \text{ Mod } 256 \end{aligned}$$

$$\begin{aligned} &= 88 \\ &= X \\ C12 &= (P12+K) \text{ Mod } 256 \\ &= (\$+4) \text{ Mod } 256 \\ &= (36+4) \text{ Mod } 256 \\ &= 40 \text{ Mod } 256 \\ &= 40 \\ &= (\\ C13 &= (P13+K) \text{ Mod } 256 \\ &= (W+4) \text{ Mod } 256 \\ &= (87+4) \text{ Mod } 256 \\ &= 91 \text{ Mod } 256 \\ &= 91 \\ &= [\\ C14 &= (P14+K) \text{ Mod } 256 \\ &= (m+4) \text{ Mod } 256 \\ &= (109+4) \text{ Mod } 256 \\ &= 113 \text{ Mod } 256 \\ &= 113 \\ &= q \\ C15 &= (P15+K) \text{ Mod } 256 \\ &= (q+4) \text{ Mod } 256 \\ &= (113+4) \text{ Mod } 256 \\ &= 117 \text{ Mod } 256 \\ &= 117 \\ &= u \\ C16 &= (P16+K) \text{ Mod } 256 \\ &= (f+4) \text{ Mod } 256 \\ &= (102+4) \text{ Mod } 256 \\ &= 106 \text{ Mod } 256 \\ &= 106 \\ &= j \\ C17 &= (P17+K) \text{ Mod } 256 \\ &= (s+4) \text{ Mod } 256 \\ &= (115+9) \text{ Mod } 256 \\ &= 119 \text{ Mod } 256 \\ &= 119 \\ &= w \\ C18 &= (P18+K) \text{ Mod } 256 \\ &= (p+4) \text{ Mod } 256 \\ &= (112+4) \text{ Mod } 256 \\ &= 116 \text{ Mod } 256 \\ &= 116 \\ &= t \\ C19 &= (P19+K) \text{ Mod } 256 \\ &= (r+4) \text{ Mod } 256 \\ &= (114+4) \text{ Mod } 256 \\ &= 118 \text{ Mod } 256 \\ &= 118 \\ &= v \\ C20 &= (P20+K) \text{ Mod } 256 \\ &= (0+4) \text{ Mod } 256 \\ &= (44+4) \text{ Mod } 256 \\ &= 52 \text{ Mod } 256 \end{aligned}$$

$$\begin{aligned}
 &= 52 \\
 &= 4 \\
 C21 &= (P21+K) \text{Mod } 256 \\
 &= (5+4) \text{Mod } 256 \\
 &= (36+4) \text{Mod } 256 \\
 &= 40 \text{ Mod } 256 \\
 &= 40 \\
 &= (\\
 C22 &= (P22+K) \text{Mod } 256 \\
 &= (W+4) \text{Mod } 256 \\
 &= (87+4) \text{Mod } 256 \\
 &= 91 \text{ Mod } 256 \\
 &= 91 \\
 &= [\\
 C23 &= (P23+K) \text{Mod } 256 \\
 &= (1+4) \text{Mod } 256 \\
 \text{Ciphertext} &: \text{Ti}\{\text{vqiz}*\text{UPX}*\text{[qujwrv4}\{[\text{5Xl} \\
 &= (49+4) \text{Mod } 256 \\
 &= 53 \text{ Mod } 256 \\
 &= 53 \\
 &= 5 \\
 C24 &= (P24+K) \text{Mod } 256 \\
 &= (T+4) \text{Mod } 256 \\
 &= (84+4) \text{Mod } 256 \\
 &= 88 \text{ Mod } 256 \\
 &= 88 \\
 &= X \\
 C25 &= (P25+K) \text{Mod } 256 \\
 &= (h+4) \text{Mod } 256 \\
 &= (104+4) \text{Mod } 256 \\
 &= 108 \text{ Mod } 256 \\
 &= 108 \\
 &= 1
 \end{aligned}$$

Tabel 2. Hasil Enkripsi Daftar Gaji Guru

No	Nama	Jabatan	Status	Gaji Pokok
1	Ti{vqiz(UPX([qujwrv4([5Xl	Smx{ms	Pwvwz	9<@8888
2	Nizqli(Uizqivq([4([6xl	XS[59	Pwvwz	A:=888
3	Lz{6(Riuit}llqv	XS[5:	Pwvwz	A:=888
4	Q{ui(l}tqi4([6Xlq	XS[5;	Pwvwz	A>:888
5	b}tnqli(Izqivq4([6Xlq	O}z}	Pwvwz	>>>888

3.3 Proses Dekripsi

1. Dekripsi Algoritma *Fast Encryption Algorithm* (FEAL)

$$Ci = (Pi - K) \text{ mod } 256 \dots\dots\dots(3.3)$$

Ket:

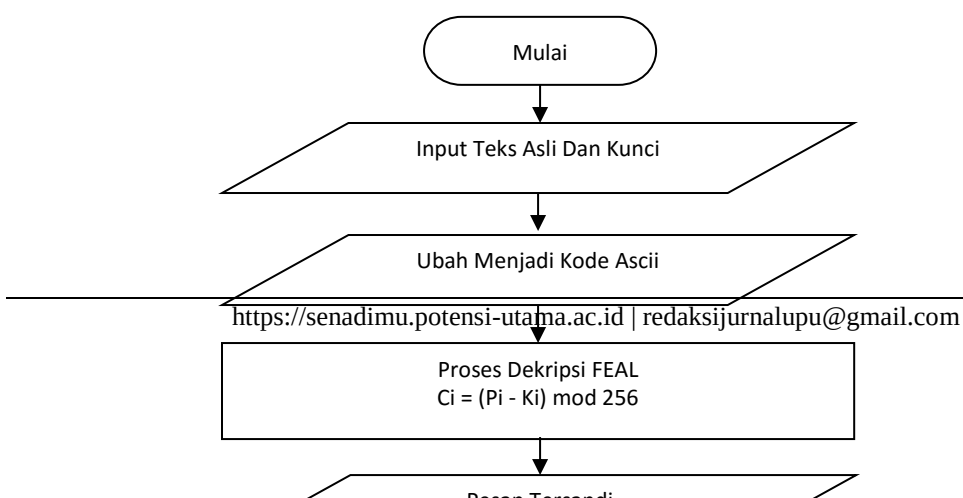
Ci : Ciphertext merupakan pesan yang disandikan, dimana $i = \{1, 2, 3, 4, \dots, n\}$

Pi : Plaintext adalah pesan asli, dengan $i = \{1, 2, 3, 4, \dots, n\}$

K : Kunci parameter untuk transformasi enchipering R Fadillah · 2022

Sebelum melakukan proses penerapan metode atau algoritma dalam penyelesaian masalah, hal yang pertama dilakukan ialah menganalisa sehingga bisa diuraikan permasalahan endskripsi, mengurangi ukuran dan dekripsi data teks hingga ke bentuk semula.

Flowchart Dekripsi metode FEAL :



Gambar 4. Flowchart Dekripsi Algoritma Metode FEAL

Langkah penyelesaiannya :

Plaintext : Ti{vqiz(UPX([qujwv4([5Xl

Kunci : 4

C1	=	$(P1-K) \text{ Mod } 256$	=	101
	=	$(T-4) \text{ Mod } 256$	=	e
	=	$(84-4) \text{ Mod } 256$	C7	= $(P7-K) \text{ Mod } 256$
	=	$80 \text{ Mod } 256$		= $(z-4) \text{ Mod } 256$
	=	80		= $(122-4) \text{ Mod } 256$
	=	P		= $118 \text{ Mod } 256$
C2	=	$(P2-K) \text{ Mod } 256$		= 118
	=	$(i-4) \text{ Mod } 256$		= v
	=	$(105-4) \text{ Mod } 256$	C8	= $(P8-K) \text{ Mod } 256$
	=	$101 \text{ Mod } 256$		= $((-4) \text{ Mod } 256)$
	=	101		= $(40-4) \text{ Mod } 256$
	=	e		= $36 \text{ Mod } 256$
C3	=	$(P3-K) \text{ Mod } 256$		= 36
	=	$(\{-4\} \text{ Mod } 256)$		= &
	=	$(123-4) \text{ Mod } 256$	C9	= $(P9-K) \text{ Mod } 256$
	=	$119 \text{ Mod } 256$		= $(U-4) \text{ Mod } 256$
	=	119		= $(85-4) \text{ Mod } 256$
	=	w		= $81 \text{ Mod } 256$
C4	=	$(P4-K) \text{ Mod } 256$		= 81
	=	$(v-4) \text{ Mod } 256$		= Q
	=	$(118-4) \text{ Mod } 256$	C10	= $(P10-K) \text{ Mod } 256$
	=	$114 \text{ Mod } 256$		= $(P-4) \text{ Mod } 256$
	=	114		= $(80-4) \text{ Mod } 256$
	=	r		= $76 \text{ Mod } 256$
C5	=	$(P5-K) \text{ Mod } 256$		= 76
	=	$(q-4) \text{ Mod } 256$		= L
	=	$(113-4) \text{ Mod } 256$	C11	= $(P11-K) \text{ Mod } 256$
	=	$109 \text{ Mod } 256$		= $(X-4) \text{ Mod } 256$
	=	109		= $(88-4) \text{ Mod } 256$
	=	m		= $84 \text{ Mod } 256$
C6	=	$(P6-K) \text{ Mod } 256$		= 84
	=	$(i-4) \text{ Mod } 256$		= T
	=	$(105-4) \text{ Mod } 256$	C12	= $(P12-K) \text{ Mod } 256$
	=	$101 \text{ Mod } 256$		= $((-4) \text{ Mod } 256)$

$$\begin{aligned}
 &= (40-4) \text{Mod } 256 \\
 &= 36 \text{ Mod } 256 \\
 &= 36 \\
 &= \$ \\
 \text{C13} &= (P13-K) \text{Mod } 256 \\
 &= ([-4) \text{Mod } 256 \\
 &= (91-4) \text{ Mod } 256 \\
 &= 87 \text{ Mod } 256 \\
 &= 87 \\
 &= W \\
 \text{C14} &= (P14-K) \text{ Mod } 256 \\
 &= (q-4) \text{ Mod } 256 \\
 &= (113-4) \text{ Mod } 256 \\
 &= 109 \text{ Mod } 256 \\
 &= 109 \\
 &= m \\
 \text{C15} &= (P15-K) \text{ Mod } 256 \\
 &= (u-4) \text{ Mod } 256 \\
 &= (117-4) \text{ Mod } 256 \\
 &= 113 \text{ Mod } 256 \\
 &= 113 \\
 &= q \\
 \text{C16} &= (P16-K) \text{ Mod } 256 \\
 &= (j-4) \text{ Mod } 256 \\
 &= (106-4) \text{ Mod } 256 \\
 &= 102 \text{ Mod } 256 \\
 &= 102 \\
 &= f \\
 \text{C17} &= (P17-K) \text{ Mod } 256 \\
 &= (w-4) \text{ Mod } 256 \\
 &= (119-4) \text{ Mod } 256 \\
 &= 115 \text{ Mod } 256 \\
 &= 115 \\
 &= s \\
 \text{C18} &= (P18-K) \text{ Mod } 256 \\
 &= (t-4) \text{ Mod } 256 \\
 &= (116-4) \text{ Mod } 256 \\
 &= 112 \text{ Mod } 256 \\
 &= 112 \\
 &= p \\
 \text{C19} &= (P19-K) \text{Mod } 256 \\
 \text{Plaintext FEAL} &: \text{Pewrmev\$QLT\$Wmqfspr0\$W1Th}
 \end{aligned}$$

$$\begin{aligned}
 &= (v-4) \text{Mod } 256 \\
 &= (118-4) \text{Mod } 256 \\
 &= 114 \text{ Mod } 256 \\
 &= 114 \\
 &= r \\
 \text{C20} &= (P20-K) \text{Mod } 256 \\
 &= (4-4) \text{Mod } 256 \\
 &= (52-4) \text{Mod } 256 \\
 &= 48 \text{ Mod } 256 \\
 &= 48 \\
 &= 0 \\
 \text{C21} &= (P21-K) \text{Mod } 256 \\
 &= ((-4) \text{Mod } 256 \\
 &= (40-4) \text{Mod } 256 \\
 &= 36 \text{ Mod } 256 \\
 &= 36 \\
 &= \$ \\
 \text{C22} &= (P22-K) \text{Mod } 256 \\
 &= ([-4) \text{Mod } 256 \\
 &= (91-4) \text{Mod } 256 \\
 &= 87 \text{ Mod } 256 \\
 &= 87 \\
 &= W \\
 \text{C23} &= (P23-K) \text{Mod } 256 \\
 &= (5-4) \text{Mod } 256 \\
 &= (53-4) \text{Mod } 256 \\
 &= 49 \text{ Mod } 256 \\
 &= 49 \\
 &= 1 \\
 \text{C24} &= (P24-K) \text{Mod } 256 \\
 &= (X-4) \text{Mod } 256 \\
 &= (88-4) \text{Mod } 256 \\
 &= 84 \text{ Mod } 256 \\
 &= 84 \\
 &= T \\
 \text{C25} &= (P25-K) \text{Mod } 256 \\
 &= (l-4) \text{Mod } 256 \\
 &= (108-4) \text{Mod } 256 \\
 &= 104 \text{ Mod } 256 \\
 &= 104 \\
 &= h
 \end{aligned}$$

2. Dekripsi Algoritma Gronsfeal

$$C_i = (P_i - K_i) \text{ mod } 256 \dots\dots\dots(3.4)$$

Ket:

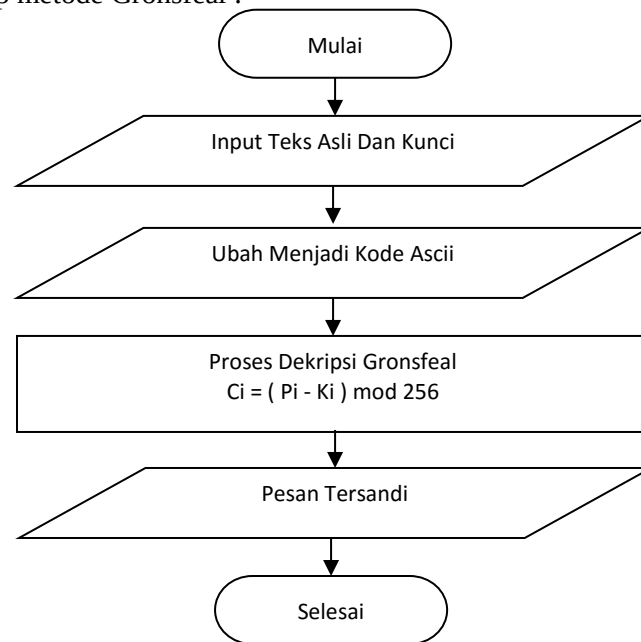
C_i : Ciphertext merupakan pesan yang disandikan, dimana $i = \{1, 2, 3, 4, \dots, n\}$

P_i : Plaintext adalah pesan asli, dengan $i = \{1, 2, 3, 4, \dots, n\}$

K : Kunci parameter untuk transformasi enchipering R Fadillah · 2022

Sebelum melakukan proses penerapan metode atau algoritma dalam penyelesaian masalah, hal yang pertama dilakukan ialah menganalisa sehingga bisa diuraikan permasalahan endskripsi, mengurangi ukuran dan dekripsi data teks hingga ke bentuk semula.

Flowchart enkrip metode Gronsfeal :



Gambar 5. Flowchart Algoritma Metode Gronsfeal

Langkah penyelesaiannya :

Chipertext : Pewrmev\$QLT\$Wmqfspr0\$W1Th

Kunci : 4

$$\begin{aligned} C1 &= (P1-K) \text{ Mod } 256 \\ &= (P-4) \text{ Mod } 256 \\ &= (80-4) \text{ Mod } 256 \\ &= 76 \text{ Mod } 256 \\ &= 76 \\ &= L \end{aligned}$$

$$\begin{aligned} C2 &= (P2-K) \text{ Mod } 256 \\ &= (e-4) \text{ Mod } 256 \\ &= (101-4) \text{ Mod } 256 \\ &= 97 \text{ Mod } 256 \\ &= 97 \\ &= a \end{aligned}$$

$$\begin{aligned} C3 &= (P3-K) \text{ Mod } 256 \\ &= (w-4) \text{ Mod } 256 \\ &= (119-4) \text{ Mod } 256 \\ &= 115 \text{ Mod } 256 \\ &= 115 \\ &= s \end{aligned}$$

$$\begin{aligned} C4 &= (P4-K) \text{ Mod } 256 \\ &= (r-4) \text{ Mod } 256 \\ &= (114-4) \text{ Mod } 256 \\ &= 110 \text{ Mod } 256 \\ &= 110 \\ &= n \end{aligned}$$

$$\begin{aligned} C5 &= (P5-K) \text{ Mod } 256 \\ &= (m-4) \text{ Mod } 256 \\ &= (109-4) \text{ Mod } 256 \\ &= 105 \text{ Mod } 256 \\ &= 105 \\ &= i \end{aligned}$$

$$\begin{aligned} C6 &= (P5-K) \text{ Mod } 256 \\ &= (e-4) \text{ Mod } 256 \\ &= (101-4) \text{ Mod } 256 \\ &= 97 \text{ Mod } 256 \\ &= 97 \\ &= a \end{aligned}$$

$$\begin{aligned} C7 &= (P7-K) \text{ Mod } 256 \\ &= (v-4) \text{ Mod } 256 \\ &= (118-4) \text{ Mod } 256 \\ &= 114 \text{ Mod } 256 \\ &= 114 \\ &= r \end{aligned}$$

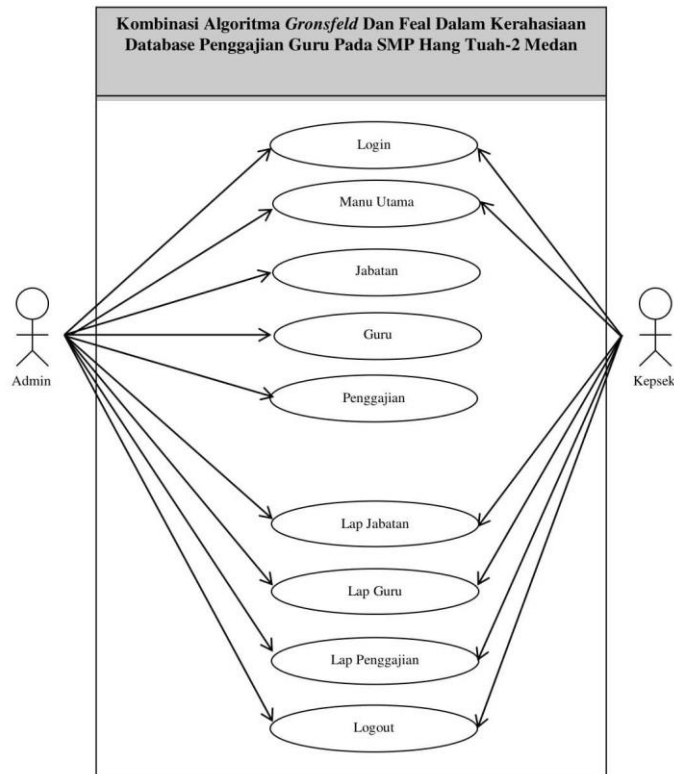
$$\begin{aligned} C8 &= (P8-K) \text{ Mod } 256 \\ &= (\$-4) \text{ Mod } 256 \\ &= (36+4) \text{ Mod } 256 \\ &= 32 \text{ Mod } 256 \\ &= 32 \\ &= \text{SPACE} \end{aligned}$$

C9	= (P9-K)Mod 256	= 111 Mod 256
	= (Q -4)Mod 256	= 111
	= (81-4)Mod 256	= 0
	= 77 Mod 256	C18 = (P18-K) Mod 256
	= 77	= (p -4) Mod 256
	= M	= (112-4) Mod 256
C10	= (P10-K)Mod 256	= 108 Mod 256
	= (L -4)Mod 256	= 108
	= (76-4) Mod 256	= l
	= 72 Mod 256	C19 = (P19-K)Mod 256
	= 72	= (r -4)Mod 256
	= H	= (114-4)Mod 256
C11	= (P11-K)Mod 256	= 110 Mod 256
	= (T -4)Mod 256	= 110
	= (84-4) Mod 256	= n
	= 80 Mod 256	C20 = (P20-K)Mod 256
	= 80	= (0-4)Mod 256
	= P	= (48-4)Mod 256
C12	= (P12-K)Mod 256	= 44 Mod 256
	= (\$-4)Mod 256	= 44
	= (36-4)Mod 256	= ,
	= 32 Mod 256	C21 = (P2110-K)Mod 256
	= 32	= (\$-4)Mod 256
	= SPACE	= (36-4)Mod 256
C13	= (P13- K)Mod 256	= 32 Mod 256
	= (w-4)Mod 256	= 32
	= (87-4) Mod 256	= SPACE
	= 83 Mod 256	C22 = (P22-K)Mod 256
	= 83	= (W-4)Mod 256
	= s	= (87-4)Mod 256
C14	= (P14-K) Mod 256	= 83 Mod 256
	= (m-4) Mod 256	= 83
	= (109-4) Mod 256	= S
	= 105 Mod 256	C23 = (P23-K)Mod 256
	= 105	= (1-4)Mod 256
	= i	= (49-4)Mod 256
C15	= (P15-K) Mod 256	= 45 Mod 256
	= (q-4) Mod 256	= 45
	= (113-4) Mod 256	= .
	= 109 Mod 256	C24 = (P24-K)Mod 256
	= 109	= (T -4)Mod 256
	= m	= (84-4)Mod 256
C16	= (P16-K) Mod 256	= 80 Mod 256
	= (f-4) Mod 256	= 80
	= (102-4) Mod 256	= P
	= 98 Mod 256	C25 = (P25-K)Mod 256
	= 98	= (h -4)Mod 256
	= b	= (104-4)Mod 256
C17	= (P17-K) Mod 256	= 100 Mod 256
	= (s-4) Mod 256	= 100
	= (115-4) Mod 256	= d

Plaintext Grosfeld : Lasniar MHP Simbolon, S.Pd

3.3. Desain Sistem

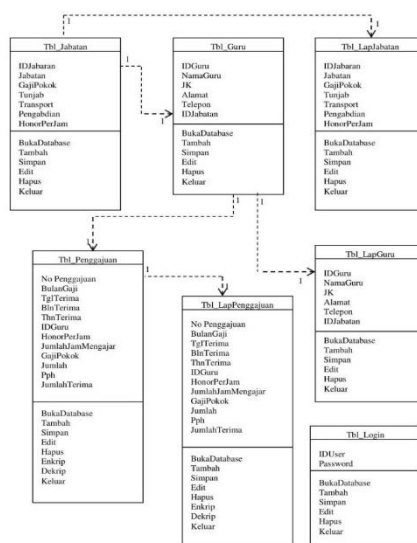
1 Use Case Diagram



Gambar 6. Use Case Diagram Kombinasi Algoritma Gronsfeld Dan Feal Dalam Kerahasiaan Database Penggajian Guru Pada SMP Hang Tuah-2 Medan

2. Class Diagram

Diagram ini digunakan untuk menggambarkan perbedaan yang mendasar antara *class-class*, hubungan antar-*class*, di mana sub-sistem *class* tersebut. Pada *class diagram* terdapat nama *class*, *attributes*, *operations*, serta *association* (hubungan antar-*class*). Adapun bentuk *class diagram* yang penulis rancang dapat dilihat pada gambar 7 sebagai berikut :



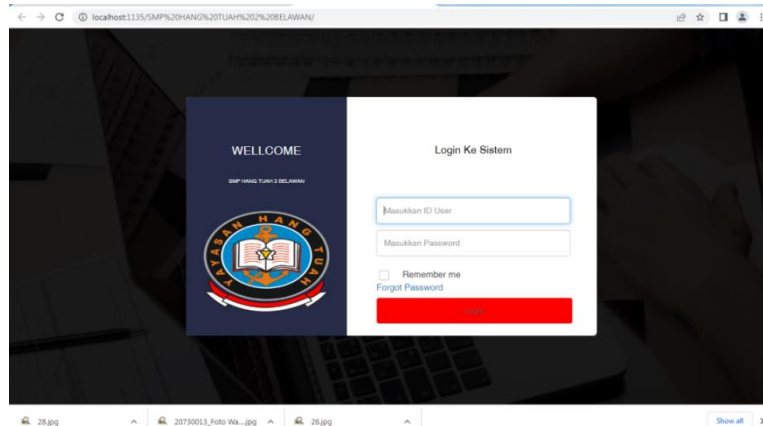
Gambar 7. Class Diagram

Kombinasi Algoritma Gronsfeld Dan Feal Dalam Kerahasiaan Database Penggajian Guru Pada SMP Hang Tuah-2 Medan

3.4 Tampilan Hasil

1. Tampilan Menu *Login*

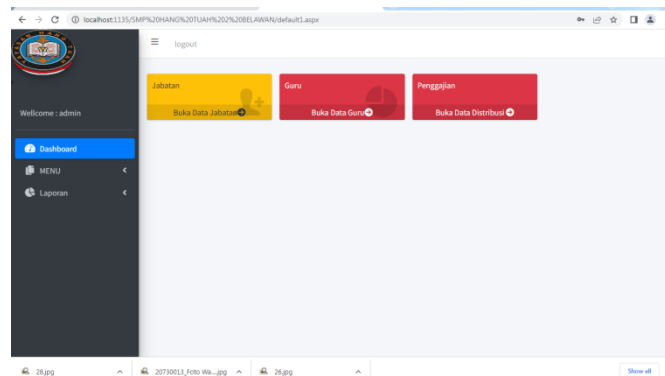
Tampilan *Login* merupakan tampilan yang pertama kali muncul ketika program dijalankan. Berfungsi sebagai *form input username* dan *password* admin program. Gambar tampilan *login* dapat ditunjukkan pada gambar 8:



Gambar 8. Tampilan *Form Login*

2. Tampilan Menu Utama

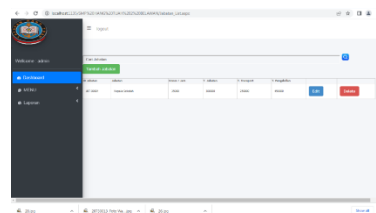
Tampilan ini merupakan tampilan menu utama yang berfungsi untuk mengetahui dan menampilkan sub menu yang ada dalam aplikasi yang dirancang. Adapun gambar menu utama ditunjukkan pada gambar 9 :



Gambar 9. Tampilan Menu Utama

3. Tampilan halaman *List Jabatan*

Tampilan ini merupakan tampilan halaman *list* jabatan yang berfungsi untuk menampilkan data jabatan yang ada di SMP Swasta Hangtuh 2 Belawan. Adapun gambar tampilan halaman *list* data jabatan ditunjukkan pada gambar 10 :



Gambar 10. Tampilan *Form List Jabatan*

4. Tampilan halaman Input Jabatan

Tampilan ini merupakan tampilan halaman input jabatan yang berfungsi untuk menginput data jabatan. Adapun gambar tampilan *form input* data jabatan ditunjukkan pada gambar 11 :

Gambar 11. Tampilan *Form Input Jabatan*5. Tampilan halaman *List Guru*

Tampilan ini merupakan tampilan halaman *list* guru yang berfungsi untuk menampilkan data guru. Adapun gambar tampilan halaman *list* data guru ditunjukkan pada gambar 12 :

NIK	Nama	Tpt Lahir	Tgl Lahir	Bln Lahir	Thn Lahir	JK	Status	ID Jabatan	Alamat
NIK-00001	Lamstar MHP Sembolan	Lamstar MHP Sembolan	1	Januari	1972	Laki-Laki	Honor	JBT-00001	Belawan

Gambar 12. Tampilan *Form List Guru*

6. Tampilan halaman Input Guru

Tampilan ini merupakan tampilan halaman input guru yang berfungsi untuk menginput data guru. Adapun gambar tampilan *form input* data guru ditunjukkan pada gambar 13 :

Gambar 13. Tampilan *Form Input Guru*

7. Tampilan halaman *List* Enkripsi Penggajian

Tampilan ini merupakan tampilan halaman *list* enkripsi penggajian yang berfungsi untuk menampilkan data penggajian dan melakukan proses enkripsi data penggajian. Adapun gambar tampilan halaman *list* data penggajian ditunjukkan pada gambar 14 :

[illegible]

Gambar 14. Tampilan *Form List Enkripsi Penggajian*

8. Tampilan halaman Input Penggajian

Tampilan ini merupakan tampilan halaman input penggajian yang berfungsi untuk menginput data penggajian. Adapun gambar tampilan *form input* data penggajian ditunjukkan pada gambar 15 :

The screenshot shows the 'Pengisian Simpanan' form in the SIMPANG2020 application. The form is titled 'Pengisian Simpanan' and contains the following fields:

- No. Rekening:** PGU-00002
- Tanggal:** 1 Januari
- Jenis Simpanan:** Tabungan
- Jumlah Simpanan:** (Empty field)
- Jangka Waktu:** Tidak Ada

The form is submitted via a 'Simpan' button.

Gambar 15. Tampilan *Form* Input Penggajian

9. Tampilan halaman Dekripsi Penggajian

Tampilan ini merupakan tampilan halaman input dekripsi penggajian yang berfungsi untuk dekripsi data penggajian. Adapun gambar tampilan *form input* data penggajian ditunjukkan pada gambar 16 :

[illegible]

Gambar 16. Tampilan *Form* Dekripsi Penggajian

4. KESIMPULAN

Dari hasil penelitian penulis, maka dapat diambil beberapa kesimpulan antara lain :

1. Terciptanya aplikasi dalam kerahasiaan database penggajian guru Pada SMP Hang Tuah-2 Medan *yang* mengakibatkan rentan terjadinya pencurian data, manipulasi data yang berdampak buruk terhadap kerahasiaan data penjualan perusahaan.
2. Terciptanya aplikasi dengan memanfaatkan algoritma kriptografi yang digunakan untuk keamanan kerahasiaan database penggajian guru Pada SMP Hang Tuah-2 Medan.

UCAPAN TERIMA KASIH

Penulis dengan tulus mengucapkan rasa terima kasih yang sebesar-besarnya kepada Universitas Potensi Utama atas bantuan yang diberikan dalam menyelesaikan karya tulis ilmiah ini.

REFERENSI

- [1] Risqiati, R. (2021). Penerapan metode single exponential smoothing dalam peramalan penjualan benang. *Smart Comp: Jurnalnya Orang Pintar Komputer*, 10(3), 154-159.
- [2] Roban, R. (2024). PERAMALAN KEBUTUHAN KCI PADA GUDANG BAHAN BAKU PT. PUPUK KUJANG CIKAMPEK DENGAN PERBANDINGAN METODE SINGLE EXPONENTIAL SMOOTHING DAN WEIGHTED MOVING AVERAGE. *Jurnal Media Teknologi*, 11(1), 53-62.
- [3] Rizal, M., Indah, D. R., & Meutia, R. (2021). Analisis Peramalan Produksi Menggunakan Trend Moment Pada Kilang Padi Do'a Ibu Diperlak Kecamatan Pereulak. *Jurnal Samudra Ekonomika*, 5(2), 161-168.
- [4] Sudarsono, A. (2016). Jaringan Syaraf Tiruan Untuk Memprediksi Laju Pertumbuhan Penduduk Menggunakan Metode Bacpropagation (Studi Kasus Di Kota Bengkulu). *Jurnal Media Infotama*, 12(1).
- [5] Utami, M. M., Sunarso, S., & Sumaryanto, S. (2024). Analisis Perbandingan Metode Exponential Smoothing dan Least Square pada Peramalan Penjualan Produk Smartphone Merek Vivo di Solusi Cash & Kredit Cabang Karanganyar. *Jurnal Manajemen Riset Inovasi*, 2(4), 107-116.
- [6] Eriva, C. Y., Arfiani, M., Ramadhan, R., Fauziah, S. R., & Paramita, S. (2023). Penerapan Anggaran Penjualan Menggunakan Metode Trend Moment Pada UD. Meudang Perkasa. *Jurnal Ilmiah Akuntansi*, 10(02), 65-70.
- [7] Tahirs, J. P. (2023). ANALISIS RAMALAN PENJUALAN KOPI PADA PT. SULOTCO JAYA ABADI KECAMATAN BITTUANG KABUPATEN TANA TORAJA. *Jurnal Darma Agung*, 31(1), 860-868.
- [8] Pengelolaan Persediaan Bahan Baku di Sun Cafe. *Jurnal EMBA: Jurnal Riset Ekonomi, Manajemen, Bisnis Dan Akuntansi*, 11(4), 483-490.
- [9] Gea, Y. J., Zai, K. S., Telaumbanua, E., & Gea, J. B. I. J. (2023). Analisis Peramalan Penjualan Dalam Pengelolaan Persediaan Bahan Baku di Sun Cafe. *Jurnal EMBA: Jurnal Riset Ekonomi, Manajemen, Bisnis Dan Akuntansi*, 11(4), 483-490.
- [10] Deni, D. R., & Barata, M. A. (2023). FORECASTING METODE SINGLE EXPONENTIAL SMOOTHING DALAM MERAMALKAN PENJUALAN BARANG. *Jurnal Informatika Polinema*, 9(4), 435-444.

- [11] Marlim, Y. N., & Hajjah, A. (2023). Analisis Kuantatif Penjualan Menggunakan Metode Single Exponential Smoothing. *JOISIE (Journal Of Information Systems And Informatics Engineering)*, 6(2), 111-116.
- [12] Maulana, A. Y., Pranoto, Y. A., & Ariwibisono, F. X. (2023). Peramalan Penjualan Thrift Pada Toko Klasswear Menggunakan Metode Regresi Linear Berbasis Website. *JATI (Jurnal Mahasiswa Teknik Informatika)*, 7(4), 2175-2181
- [13] Febrian, M. T., Manurung, N., & Putri, P. (2024). SISTEM PERAMALAN PENJUALAN PARFUM PADA FIONA PERFUME DENGAN METODE SINGLE EXPONENTIAL SMOOTHING (SES). *JSiI (Jurnal Sistem Informasi)*, 11(2), 104-111.
- [14] Shobori, I., Khairil, K., & Suryana, E. (2024). PREDIKSI PENJUALAN BARANG MENGGUNAKAN METODE SINGLE EXPONENTIAL SMOOTHING PADA DUO SISTER HIJAB BENGKULU. *JOURNAL OF SCIENCE AND SOCIAL RESEARCH*, 7(4), 1493-1498.
- [15] Audinasyah, C. S. (2024). Sistem Forecasting Perencanaan Produksi dengan Metode Single Exponential Smoothing Pada Home Industry Tempe Putera Sejahtera. *Jurnal EMT KITA*, 8(3), 845-853.