Djtechno : Jurnal Teknologi Informasi
Vol. 6, No. 2, Agustus 2025
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno

PENERAPAN ALGORITMA *GRONSFELD* DALAM PENGAMANAN DATA PENJUALAN SPAREPART SEPEDA MOTOR

Hendri Satrianto[1], Zulham[2], Amru Yasir [3]
1,3) Teknologi Informasi, Fakultas Teknik dan Ilmu Komputer, Universitas Dharmawangsa, Indonesia
2) Rekayasa Perangkat Lunak, Fakultas Teknik dan Ilmu Komputer, Universitas Dharmawangsa, Indonesia

Article Info

Article history:

Received: 16 Juli 2025
Revised: 28 Juli 2025
Accepted: 31 Juli 2025

ABSTRACT

Abstrak

Perkembangan teknologi informasi telah memungkinkan komunikasi dan pertukaran data tanpa batasan jarak dan waktu. Seiring dengan meningkatnya kebutuhan akan keamanan data, perlindungan terhadap kerahasiaan informasi menjadi sangat penting. Salah satu cara untuk menjaga kerahasiaan data adalah dengan menggunakan kriptografi, yang mencakup proses enkripsi dan dekripsi pesan. Dalam hal ini, algoritma Gronsfeld Cipher digunakan sebagai solusi untuk meningkatkan keamanan data penjualan pada PT. Buana Jaya Lestari, yang masih menggunakan sistem manual berbasis *Microsoft Excel* untuk menyimpan data penjualan sparepart sepeda motor. Sistem tersebut rentan terhadap pencurian dan manipulasi data. Penelitian ini bertujuan untuk merancang aplikasi berbasis web yang dapat mengamankan database penjualan dengan menerapkan algoritma Gronsfeld Cipher. Algoritma ini bekerja dengan menggantikan karakter plaintext menggunakan angka untuk mengenkripsi data, sehingga menghasilkan ciphertext yang lebih aman. Dengan penerapan algoritma ini, diharapkan dapat mengatasi masalah pencurian data dan memberikan solusi keamanan yang lebih baik untuk perusahaan. Penelitian ini juga memberikan kontribusi dalam meningkatkan pemahaman tentang penerapan kriptografi dalam melindungi data sensitif, khususnya di lingkungan bisnis.

Kata Kunci: Kriptografi, Gronsfeld Cipher, Keamanan Data, Penjualan Sparepart**.**

Abstract

The development of information technology has enabled communication and data exchange without the constraints of distance and time. As the need for data security increases, protecting information confidentiality becomes crucial. One way to maintain data confidentiality is through the use of cryptography, which encompasses the process of encrypting and decrypting messages. In this case, the Gronsfeld Cipher algorithm is used as a solution to improve sales data security at PT. Buana Jaya Lestari, which still uses a manual Microsoft Excel-based system to store motorcycle spare part sales data. This system is vulnerable to data theft and manipulation. This research aims to design a web-based application that can secure the sales database by implementing the Gronsfeld Cipher algorithm. This algorithm works by replacing plaintext characters with numbers to encrypt data, resulting in more secure ciphertext. The implementation of this algorithm is expected to address data theft issues and provide better security solutions for companies. This research also contributes to increasing understanding of the application of cryptography in protecting sensitive data, particularly in business environments.

Keywords: *Cryptography, Gronsfeld Cipher, Data Security, Spare Part Sales.*

Djtechno : Jurnal Teknologi Informasi
Vol. 6, No. 2, Agustus 2025
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno

Corresponding Author:
E-mail: hendri.satrianto@gmail.com

1. PENDAHULUAN

Perkembangan teknologi terkini telah memungkinkan orang untuk berkomunikasi dan bertukar data dan informasi tanpa batasan jarak atau waktu. Dengan meningkatnya tuntutan keamanan atas kerahasiaan informasi yang dipertukarkan, maka tuntutan akan ketersediaan data dan sistem keamanan informasi [1] yang lebih baik untuk melindungi data dari ancaman pencurian data.

Kriptografi adalah ilmu menjaga kerahasiaan pesan dengan cara menyandikannya dalam bentuk yang tidak dapat dipahami lagi. Dalam kriptografi terdapat dua proses yaitu enkripsi dan dekripsi. Pesan terenkripsi disebut plaintext [2] [3]. Disebut demikian karena informasi ini dapat dengan mudah dibaca dan dipahami oleh siapa saja. Algoritma yang digunakan untuk mengenkripsi dan mendekripsi plaintext melibatkan penggunaan beberapa bentuk kunci. Pesan eksplisit dengan ciphertext disebut ciphertext. Dalam pengkodean, kita sering menemukan istilah yang berbeda. [4]

PT. Buana Jaya Lestari memiliki sistem pendataan penjualan produk sparepart sepeda motor belum menggunakan sistem dengan menggunakan database sebagai penyimpanan data penjualan dimana dalam setiap transaksi penjualan sparepart sepeda motor yang dilakukan diinputkan dalam lembar kerja.

Perumusan masalah yang berdasarkan identifikasi masalah yang terdapat pada penelitian ini adalah sebagai berikut:

1. Bagaimana merancang sebuah aplikasi untuk kerahasiaan database penjualan produk sparepart sepeda motor honda berbasis web pada PT. Buana Jaya Lestari?
2. Bagaimana menerapkan algoritma *Gronsfeld* untuk kerahasiaan database penjualan produk sparepart sepeda motor ?

Tujuan penelitian ini adalah sebagai berikut:

1. Untuk merancang aplikasi kerahasiaan tabel penjualan produk sparepart sepeda motor honda berbasis web.
2. Untuk menerapkan algoritma *Gornsfeld* dalam Kerahasian tabel penjualan produk sparepart sepeda motor honda pada PT. Buana Jaya Lestari.

Djtechno : Jurnal Teknologi Informasi
Vol. 6, No. 2, Agustus 2025
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno

Disebabkan banyaknya permasalahan dan waktu yang terbatas, maka agar pembahasan masalah tidak melebar penulis membatasi masalah sebagai berikut:

1. Aplikasi Kerahasiaan database yang dirancang menggunakan algoritma *Gornsfeld*.
2. Data yang didapatkan dari PT. Buana Jaya Lestari diolah dengan menggunakan algoritma *Gornsfeld* untuk mendapatkan *Cipher* Teks.
3. Aplikasi yang digunakan adalah *Visual Stuido 2010* dengan Active Server Page (ASP).

Kriptografi adalah suatu Teknik penyembunyian pesan dimana pesan tersebut hanya bisa diketahui oleh orang tertentu dimana pesan itu seringkali disebut dengan enkripsi.[5] Saat ini enkripsi telah banyak dikembangkan salah satunya ialah metode Rivest Shamir Adleman (RSA) [6] yang memakai 2 kunci yaitu kunci publik serta kunci pribadi, dimana kunci tersebut bisa diatur dimana semakin panjang bit pembentukan kunci maka semakin sukar untuk dipecahkan sebab sulitnya memfaktorkan 2 bilangan yang sangat besar dan itu disebut aman meskipun tidak pernah dibuktikan aman tidaknya. Tujuan dari kriptografi adalah untuk kerahasiaan (confidentiality), untuk menjaga pesan agar tidak dibaca oleh pihak yang tidak bersangkutan. Integritas data (data integrity), menjamin bahwa pesan masih asli dan tidak diubah atau dimanipulasi selama proses pengiriman. Otenttikasi (authentication), untuk mengidetifikasi kebenaran dari pihak bersangkutan. Non-repudiation menjaga entitas yang bersangkutan melakukan suatu penyangkalan [7].

Gronsfeld merupakan algoritma penyandian yang hanya menggunakan numeric sebagai *key* [8]. *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.

Gronsfeld Cipher adalah bentuk dari cipher substitusi monoalfabetik yang menggunakan angka sebagai kunci enkripsi. Setiap digit dalam kunci menunjukkan seberapa banyak pergeseran huruf dalam alfabet [9].

a. Alfabet yang digunakan: A-Z (26 huruf)
b. Kunci: terdiri dari digit angka (0–9)
c. Huruf-huruf dalam pesan digeser ke kanan sesuai angka pada kunci
d. Jika panjang kunci lebih pendek dari pesan, kunci akan **diulang**

Djtechno : Jurnal Teknologi Informasi
Vol. 6, No. 2, Agustus 2025
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno

Karakteristik Gronsfeld Cipher cocok untuk alfabet Latin dan juga Termasuk cipher **simetris** (kunci enkripsi = kunci dekripsi). Gronsfeld Cipher tidak tahan terhadap serangan brute-force karena jumlah kemungkinan kuncinya relatif kecil (jika kunci pendek).

Sebagai contoh metode Gronsfield seperti berikut ini :

Pesan asli: HELLO

Kunci: 31415

Langkah-langkah:

Tabel 1.1 Cara kerja Metode Gronsfield

Huruf	Kunci	Pergeseran	Hasil
H	3	H → K	K
E	1	E → F	F
L	4	L → P	P
L	1	L → M	M
O	5	O → T	T

Algoritma enkripsi Gronsfeld Cipher :

Ci = (Pi + Ki) mod 256.....(1)

Contoh Proses Enkripsi :

Plaintext : GRO

Kunci : 734

G = 71

R = 82

O = 79

Key : 7,3,4

C1 = (G + k1) mod 256

= (71 + 7) mod 256

= 78 mod 256

= 78 = N

C2 = (R + k2) mod 256

= (82 + 3) mod 256

= 85 mod 256

= 85 = U

C3 = (O + k3) mod 256

Djtechno : Jurnal Teknologi Informasi
Vol. 6, No. 2, Agustus 2025
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno

= (79 + 4) mod 256

= 83 mod 256

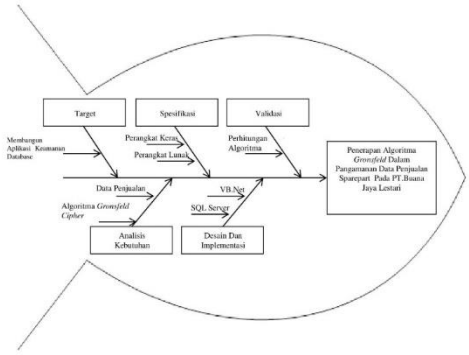
= 83 = S

Chipertext : NUS

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 penjualan perusahaan.

2. METODE PENELITIAN

Langkah-langkah yang dilakukan untuk mencapai tujuan perancangan adalah sebagai berikut:



Gambar 2.1. Prosedur Perancangan *Fishbone*

Keterangan :

1. Analisis Kebutuhan

   Adapun yang dibutuhkan dalam analisis data yaitu data aktual penjualan sparepart sepeda motor honda.

2. Studi Literatur

   Tahap ini merupakan tahap dimana penulis melakukan / mencari bahan bacaan tentang metode yang digunakan berupa referensi jurnal.

3. Desain Aplikasi

   Sistem yang akan dibangun dengan menggunakan *ASP.Net* [10].

4. Penulisan Kode

   Tahap ini membutuhkan perangkat lunak yang sesuai kebutuhan sistem dengan spesifikasi Perangkat lunak yang dibutuhkan antara lain: Microsoft Visual Studio 2010[11], *Sql Server 2008 R2*[12].

Djtechno : Jurnal Teknologi Informasi
Vol. 6, No. 2, Agustus 2025
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno

5. Uji Coba

   Uji coba sistem digunakan yaitu dengan menerapkan Blackbox

6. Implementasi

Pada tahap ini penerapan algoritma *Gornsfeld* [13] [14] dalam pengamanan database penjualan produk sparepart sepeda motor telah melewati tahap pengujian dan validasi sehingga dapat digunakan pada keamanan database penjualan produk sparepart.

2.1 Proses Enkripsi

1. Enkripsi Algoritma Gronsfeal

Ci = (Pi + Ki) mod 256.....(1)

Dimana:

C : *Ciphertext* hasil proses enkrip

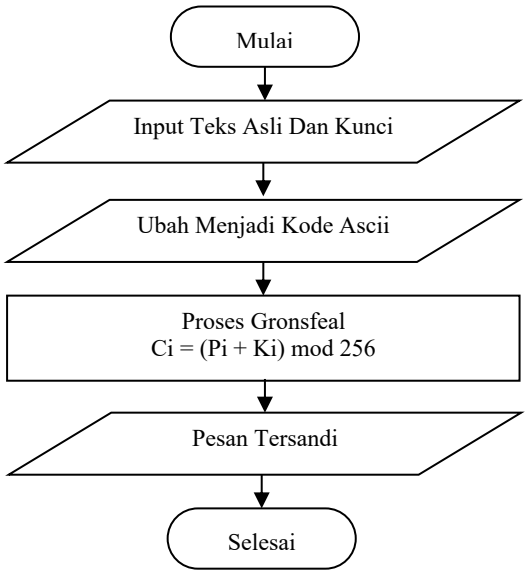
P : *Plaintext* untuk proses enkrip

K : *Key* untuk proses enkrip

mod : Sisa bagi

256 : Total ASCII pada *keyboard*

Flowchart enkrip metode Gronsfeal:



Gambar 2.2. Flowchart Algoritma Metode *Gronsfeal*

Data : Kanvas Rem

Kunci : 5

C1 = $(P1+K) Mod\ 256$
= (K+5) $Mod\ 256$
= (75+5) $Mod\ 256$
= 80 $Mod\ 256$
= 80
= P

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

Djtechno : Jurnal Teknologi Informasi
Vol. 6, No. 2, Agustus 2025
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno

= (a+5) Mod 256
= (97+5) Mod 256
= 102 Mod 256
= 102
= f

C3 = (P5+K) Mod 256
= (n+5) Mod 256
= (110+5) Mod 256
= 115 Mod 256
= 115
= s

C4 = (P4+K)Mod 256
= (v+5)Mod 256
= (118+5)Mod 256
= 123 Mod 256
= 123
= {

C5 = (P5+K) Mod 256
= (a+5) Mod 256
= (97+5) Mod 256
= 102 Mod 256
= 102
= f

C6 = (P5+K)Mod 256
= (s+5)Mod 256
= (115+5)Mod 256
= 120 Mod 256
= 120
= x

C7 = (P7+K)Mod 256
= (Spasi+5)Mod 256
= (32+5)Mod 256
= 37 Mod 256
= 37
= %

C8 = (P8+K)Mod 256
= (R+5)Mod 256
= (82+5)Mod 256
= 87 Mod 256
= 87
= W

C9 = (P9+K)Mod 256
= (e+5)Mod 256
= (101+5)Mod 256
= 106 Mod 256
= 106
= j

C10 = (P10+K)Mod 256
= (m+5)Mod 256
= (109+5)Mod 256
= 114 Mod 256
= 114
= r

Ciphertext : Pfs{fx%Wjr

2. Dekripsi Algoritma Gronsfeal

Ci = (Pi - Ki) mod 256 .....(2)

Ket:

Ci : Ciphertext merupakan pesan yang disandikan, dimana i ={1,2,3,4,….n}

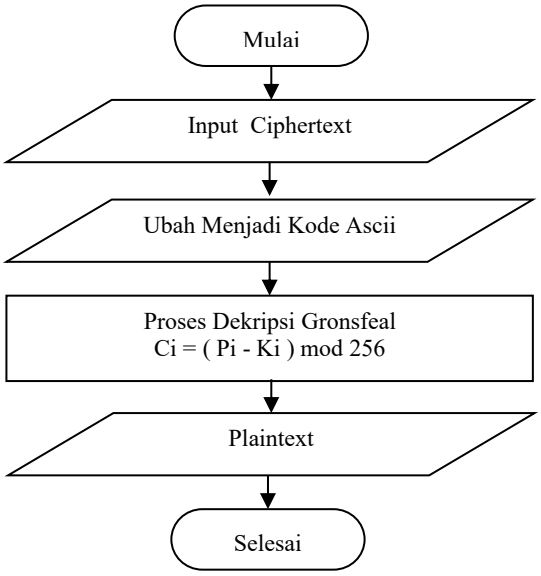
Pi : Plaintext adalah pesan asli, dengan i ={1,2,3,4,…n}

K : Kunci parameter untuk transformasi enchipering R Fadillah · 2022

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

Flowchart dekrip metode Gronsfeal :

Djtechno : Jurnal Teknologi Informasi
Vol. 6, No. 2, Agustus 2025
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno



Gambar 2.3. Flowchart Algoritma Metode Gronsfeal

Langkah penyelesaiannya :

Chipertext : Pfm{fx%Wjr

Kunci : 5

C1 = (P - k1) mod 256
= (80 - 5) mod 256
= 75 mod 256
= 75
= K
C2 = (f - 5) mod 256
= (102 - 5) mod 256
= 97 mod 256
= 97
= a
C3 = (s - 5) mod 256
= (115 - 5) mod 256
= 110 mod 256
= 110
= n
C4 = ({ - 5) mod 256
= (123 - 5) mod 256
= 118 mod 256
= 118
= v
C5 = (f - 5) mod 256
= (102 - 5) mod 256
= 97 mod 256
= 97
= a
C6 = (x - 5) mod 256
= (120 - 5) mod 256
= 115 mod 256
= 115
= s
C7 = (% - 3) mod 256
= (37 - 5) mod 256
= 32 mod 256
= 32
= Spasi
C7 = (W - 5) mod 256
= (87 - 5) mod 256
= 82 mod 256
= 82
= R
C8 = (j - 5) mod 256
= (106 - 5) mod 256
= 101 mod 256
= 101
= e
C9 = (r - 5) mod 256
= (114 - 5) mod 256

Djtechno : Jurnal Teknologi Informasi
Vol. 6, No. 2, Agustus 2025
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno

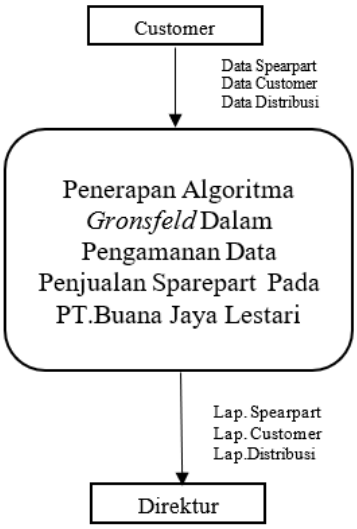
= 109 mod 256 = m
= 109 Plainttext : Kanvas Rem

3. HASIL DAN PEMBAHASAN

3.1 Rancangan Proses

Rancangan ini dimulai dari bentuk yang paling global yaitu Diagram Kontkes, kemudian *Diagram Konteks* ini diturunkan sampai bentuk yang paling detail. Pada gambar berikut dapat dilihat *Diagram Konteks* dari sistem yang dirancang.

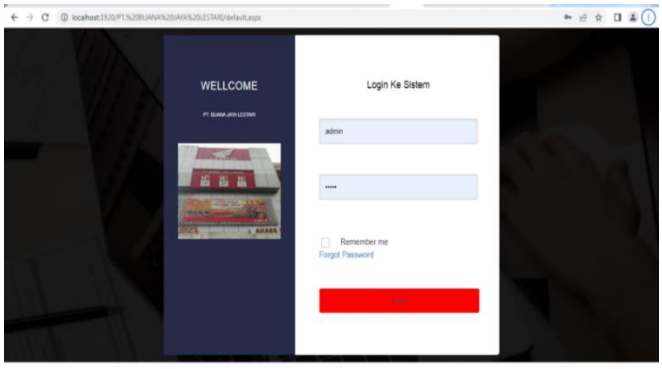
Diagram kontkes menggambarkan diagram utama dari sistem yang dirancang[15]. Berikut ini adalah bentuk *Diagram Konteks* dari sistem yang dirancang.



Gambar 3.1 *Diagram Konteks* Penerapan Algoritma *Gronsfeld*

3.2 Tampilan Halaman *Login*

Tampilan *Login* merupakan tampilan yang pertama kali muncul ketika website dijalankan. Berfungsi sebagai halaman pengisian *username* dan *password* admin program. Gambar tampilan halaman *login* dapat ditunjukkan pada gambar 3.2 :

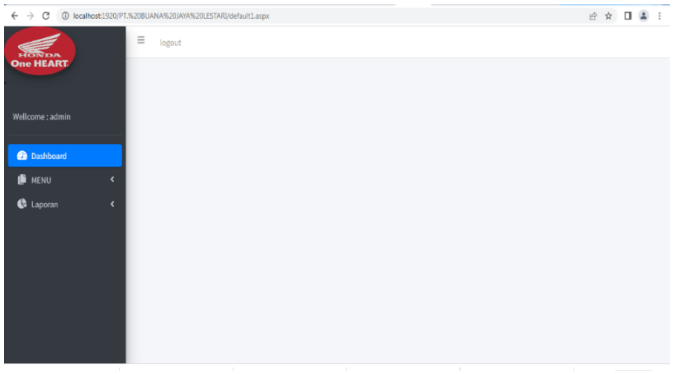


Gambar 3.2. Tampilan *Form Login*

Djtechno : Jurnal Teknologi Informasi
Vol. 6, No. 2, Agustus 2025
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno

3.3. Tampilan *Form Dashboard*

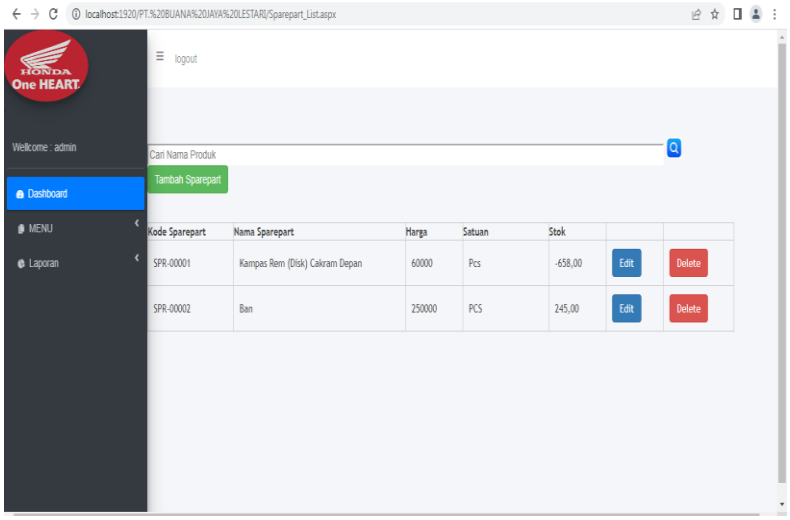
Tampilan ini merupakan tampilan data dashboard pada sistem yang dirancang. Halaman *dashboard* berfungsi untuk menampilkan semua pilihan inputan maupun laporan, Gambar tampilan *dashboard* ditunjukkan pada gambar 3.3 :



Gambar 3.3. Tampilan Halaman *Dashboard*

3.4 Tampilan Halaman *Input* Sparepart

Tampilan ini merupakan tampilan Halaman *Input* Sparepart digunakan untuk mengisi data sparepart dan disimpan ke database. Adapun tampilan halaman input sparepart pada gambar 3.4 :

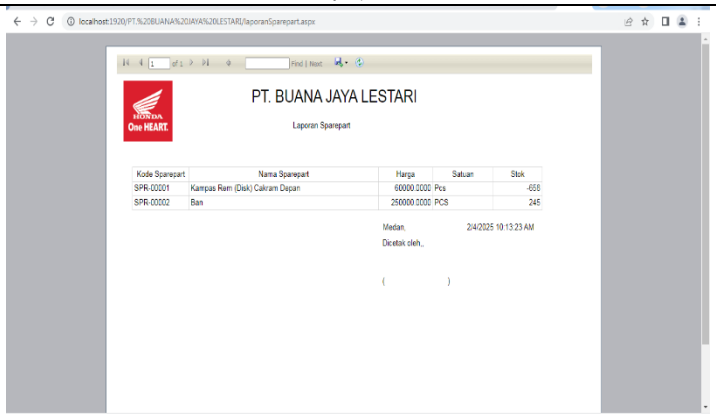


Gambar 3.4. Tampilan Halaman input Sparepart

3.5. Laporan

Halaman laporan sparepart ini berfungsi menampilkan laporan sparepart yang akan di cetak, ketika *admin* memilih laporan sparepart maka aplikasi akan menampilkan laporan data sparepart. Gambar tampilan *form* laporan sparepart dapat pada gambar 3.5 :

Djtechno : Jurnal Teknologi Informasi
Vol. 6, No. 2, Agustus 2025
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno



Gambar 3.5. Tampilan Halaman Laporan Sparepart

4. SIMPULAN

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

1. Terciptanya sebuah aplikasi yang dapat merahasiakan tabel penjualan tersimpan ke database dengan bentuk yang telah di enkripsi
2. Terciptanya sebuah aplikasi dengan menerapkan algoritma *Gronsfeal Cipher* Untuk Kerahasian tabel penjualan produk sparepart sepeda motor.

Berdasarkan hasil penelitian dan kesimpulan yang telah diuraikan di atas, maka ada beberapa saran yang dapat diberikan. Adapaun saran-saran yang dapat dikemukakan adalah sebagai berikut :

1. Sebaiknya PT. Buana Jaya Lestari merancang sistem yang dapat melakukan penyimpanan data penjualan ke database dengan bentuk yang telah di enkripsi.
2. Sebaiknya PT. Buana Jaya Lestari menerapkan algoritma *Gronsfeal Cipher* Untuk menjaga kerahasian Data penjualan produk sparepart sepeda motor.

REFERENCES

[1]. E. Novianto, E. H. Heri Ujianto, and R. Rianto, "KEAMANAN INFORMASI (INFORMATION SECURITY) PADA APLIKASI SISTEM INFORMASI MANAJEMEN SUMBER DAYA MANUSIA," *rabit*, vol. 8, no. 1, pp. 10–15, Jan. 2023, doi: 10.36341/rabit.v8i1.2966.

[2]. "992." Accessed: Aug. 01, 2025. [Online]. Available: https://dinastirev.org/JEMSI/article/view/992

[3]. "Azura et al. - 2023 - Penerapan Kemanan Data Text menggunakan Metode Kri."

[4]. "Azhari et al. - 2022 - Implementasi Pengamanan Data pada Dokumen Mengguna."

[5]. "81893." Accessed: Jul. 28, 2025. [Online]. Available: https://journal.ugm.ac.id/khazanah/article/view/81893

Djtechno : Jurnal Teknologi Informasi
Vol. 6, No. 2, Agustus 2025
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno
[6]. "Trisnawati et al. - 2023 - Penerapan Algoritma Rivest-Shamir-Adleman (RSA) pa."
[7]. "378686166_Implementasi_Aplikasi_Pencatatan_Data_Magang_Mahasiswa_Berbasis_Mobile_Menggunakan_Kodular_Menggunakan_Metode_Waterfall." Accessed: Jul. 28, 2025. [Online]. Available: https://www.researchgate.net/publication/378686166_Implementasi_Aplikasi_Pencatatan_Data_Magang_Mahasiswa_Berbasis_Mobile_Menggunakan_Kodular_Menggunakan_Metode_Waterfall
[8]. Sinaga et al. - 2020 - Pengamanan File Docx Menerapkan Algoritma Gronsfel."
[9]. "Safitri and Prihanto - 2019 - Modifikasi Cipher Kriptografi Caesar yang Dapat Di."
[10]. "Christanto and Wibowo - 2020 - ANALISIS KOMPARASI PERFORMA WEB APPLICATION STUDI."
[11]. "Rinaldi et al. - 2021 - Perancangan Sistem Informasi Indeks Penyakit Pasie."
[12]. "Sianturi - 2018 - ANALISA PENGARUH LOG TRANSAKSI PADA SISTEM KOMPUTE."
[13]. "Syahputri et al. - 2023 - Penerapan Algoritma Gronsfeld Dengan Pembangkit Ku."
[14]. "1+Wahyudi+et+al."
[15]. "Husna et al. - Analisis Bibliometrik Kiryoku Jurnal Studi Kejepa."