

## **PENERAPAN KRIPTOGRAFI CAESAR CIPHER DAN VIGENERE CIPHER UNTUK MENGAMANKAN DATABASE BARANG BELTING PADA PT. MULTI MITRA USAHA BERSAMA**

**Muhammad Rizqi Zulfikar<sup>1\*</sup>, Sri Mulyati<sup>2</sup>**

<sup>1,2</sup>Fakultas Teknologi Informasi, Teknik Informatika, Universitas Budi Luhur, Jakarta, Indonesia

Email : <sup>1\*</sup>1711500940@student.budiluhur.ac.id, <sup>2</sup>sri.mulyati@budiluhur.ac.id  
(\* : corresponding author)

**Abstrak**-Privasi juga dikenal sebagai “confidentially”, dapat dipahami sebagai kerahasiaan sistem informasi perusahaan, tidak mengizinkan pihak-pihak yang tidak berwenang untuk mengakses. Kerahasiaan harus didefinisikan dengan jelas dan prosedur untuk menjaga kerahasiaan informasi harus dipertimbangkan dengan hati-hati. . Data yang bersifat rahasia tersebut perlu dibuatkan sistem keamanan yang baik, jauh dari jangkauan orang yang tidak berwenang. Bebas dari ruang lingkup secara fisik dan secara sistem. Agar tidak untuk di baca oleh pihak-pihak yang tidak berwenang pada saat data tersebut di simpan di dalam database. PT Multi Mitra Usaha Bersama mempunyai data mitra/partner, barang bersifat penting dalam bertransaksi disimpan kedalam database sistem PT Multi Mitra Usaha Bersama. Namun jika data tersebut hanya di simpan didalam database, tanpa adanya pengamanan data yang baik, maka data tersebut rentan terhadap pencurian atau pengubahan data oleh pihak yang tidak diinginkan. Oleh karena itu penerapan keamanan basis data mencegah orang yang berkepentingan mencuri data yang tersimpan dalam database dan penerapan algoritma 2 (dua) metode sangat penting untuk dapat mengamankan record database. Penerapan algoritma metode kriptografi dalam penelitian akan difokuskan bagaimana cara kerja kriptografi bisa mengamankan data teks yang disimpan didalam database menjadi aman dari pihak-pihak yaitu oleh orang yang tidak berkepentingan. Dan aplikasi kriptografi ini, diharapkan informasi data barang, supplier, customer dan data transaksi akan aman dan tidak tersebar oleh pihak yang tidak bertanggung jawab. Berdasarkan implementasi dan pengujian program, dan mampu menjaga, melindungi kerahasiaan data informasi. Serta dapat memberikan manfaat bagi pihak PT. Multi Mitra Usaha Bersama dalam menjalankan tugas pokoknya, fungsi, dan peran dalam keamanan teknologi.

**Kata Kunci:** caesar cipher, vigenere cipher, kriptografi database

### **APPLICATION OF CAESAR CIPHER AND VIGENERE CIPHER METHODS TO SECURE DATABASE OF BELTINGS AT PT. MULTI JOINT BUSINESS PARTNER**

**Abstract**-Privacy is known as confidentially, and can be understood as the confidentiality of the company's information system, not allowing unauthorized parties to access it. Confidentiality should be clearly defined, and procedures for maintaining the confidentiality of information should considered carefully. Such confidential data needs to be made into a good security system and away from the reach of unauthorized persons. Free from physical and system scope so that it is not read by unauthorized parties when the data stored in the database. PT Multi Mitra Usaha Bersama has partner data, goods are important in transactions stored in the PT Multi Mitra Usaha Bersama database system. However, if the data is stored only in the database, without good data security, then the data is vulnerable to theft or alteration of data by unwanted parties. Because the implementation of database security prevents interested persons from stealing data stored in the database and the application of 2 (two) methods of an algorithm is very important to be able to secure database records. The application of the cryptographic method algorithm in this study will focus on how cryptography works and can secure text data stored in the database to be safe from parties, namely unauthorized persons. And this cryptographic application, expects the information on goods, suppliers, customers, and transaction data to be safe and not spread by irresponsible parties. Based on the implementation and testing of the program, and able to maintain, and protect the confidentiality of information data. And can provide benefits for PT. Multi-Joint Venture Partners in carrying out their main duties, functions, and roles in technology security.

**Keywords:** vigenere cipher,, caesar cipher, database cryptography.

---

## **1. PENDAHULUAN**

Privasi juga dikenal sebagai “confidentially”, dapat dipahami sebagai kerahasiaan sistem informasi perusahaan, tidak mengizinkan pihak-pihak yang tidak berwenang untuk mengakses. Kerahasiaan harus didefinisikan dengan jelas dan prosedur untuk menjaga kerahasiaan informasi harus dipertimbangkan dengan hati-

hati. Data yang bersifat rahasia tersebut perlu dibuatkan sistem keamanan yang baik, jauh dari jangkauan orang yang tidak berwenang. Bebas dari ruang lingkup secara fisik dan secara sistem. Agar tidak untuk di baca oleh pihak-pihak yang tidak berwenang pada saat data tersebut di simpan di dalam database.

PT Multi Mitra Usaha Bersama adalah perusahaan yang telah berdiri sejak tahun 2012. Perusahaan ini bergerak dibidang mesin - mesin dan perlengkapannya, tekstil dan belting. Perusahaan kami berlokasi di Ciputat, kami siap bersaing dengan perusahaan lainnya di Indonesia dengan menawarkan kualitas dan harga produk yang cukup bersaing serta bergaransi. PT Multi Mitra Usaha mempunyai data mitra/parner, barang bersifat penting dalam bertransaksi untuk disimpan kedalam database sistem PT Multi Mitra Usaha. Namun jika data tersebut hanya di simpan didalam database, tanpa adanya keamanan data yang baik, maka data tersebut sangat rentan terhadap pencurian atau pengubahan data oleh pihak yang tidak diinginkan. Oleh karena penerapan keamanan basis data mencegah orang yang berkepentingan mencuri data yang tersimpan dalam database dan penerapan algoritma 2 (dua) metode sangat penting untuk dapat mengamankan record database. Penerapan algoritma metode kriptografi dalam penelitian akan difokuskan bagaimana cara kerja kriptografi bisa mengamankan data teks yang disimpan didalam database menjadi aman dari pihak ketiga yaitu oleh orang yang berkepentingan.

Banyak teknik yang dapat digunakan untuk mengamankan data diantaranya adalah kriptografi. Teknik tersebut memiliki fungsi masing masing, kriptografi yang bertujuan untuk menyamarkan suatu pesan menjadi suatu pesan yang sulit dibaca atau dimengerti.

Berdasarkan kenyataan diatas perlu ada suatu sistem pengamanan informasi *database* saat menginput data kedalam *database*. Untuk melakukan hal ini ada suatu cara yang biasa disebut penyandian data. Dalam penelitian ini akan mencoba mengimplementasikan suatu cabang ilmu matematika yang disebut dengan kriptografi. Dengan kriptografidata dapat di ubah menjadi sandi-sandi yang tidak dimengerti oleh sembarang orang serta mengembalikannya kebentuk semula, proses ini disebut enkripsi dan dekripsi.

## 2. METODOLOGI PENELITIAN

### 2.1 Data Penelitian

Data Penelitian berupa data barang yang di dapatkan melalui tempat penelitian PT. Multi Mitra Usaha Bersama, data barang terdiri dari kode barang, nama barang, kode supplier, supplier seperti Tabel 1:

**Tabel 1.** Data Barang

No.	Kode Barang	Nama Barang	Kode Supplier	Supplier
1.	20871	OPTI 150L*13	S0114	UD. HARAPAN JAYA
2.	20872	T.B-250DS8M-1760	S0291	TALI AGUNG
3.	20910	MITSUBOSHI ZR 285L*20	S0114	UD. HARAPAN JAYA
4.	20911	MITSUBOSHI 1800-8M*30	S0114	UD. HARAPAN JAYA
5.	20921	FG 1000 X 25 X 10MM GREEN	S0600	FOSHAN AOLIDA TRANSMISSION
6.	20922	FG 1540 X 25 X 8MM GREEN	S0600	FOSHAN AOLIDA TRANSMISSION
7.	20923	FG 1550 X 25 X 8MM GREEN	S0600	FOSHAN AOLIDA TRANSMISSION
8.	20952	GREEN SPONGE 8MMT 3X0.3	S0548	AMERICA ULIFLEX INDUSTRY BELT
9.	20953	BLACK PONGE+BLUE FAB.6MMT 3.3X1.3M	S0548	AMERICA ULIFLEX INDUSTRY BELT
10.	20954	BLACK PONGE+BLUE FAB.10MMT 3.3X1.3M	S0548	AMERICA ULIFLEX INDUSTRY BELT
11.	20955	BV/2 EM 8-00+12 AG-AS 3.0MM	S0448	INO BELT
12.	20956	BV/3 EM 12-00+10 AG AS 4.0MM	S0448	INO BELT
13.	20957	GREEN SPONGE 10MMT 3X0.3M	S0548	AMERICA ULIFLEX INDUSTRY BELT
14.	20961	ALLIGATOR 7-12 (1BOX=8PC)	S0646	FLEXCO
15.	20971	TB-1800-8M-30	S0114	UD. HARAPAN JAYA
16.	20972	TB-2400-8M-30	S0114	UD. HARAPAN JAYA
17.	20975	SPEED BELT 775X30	S0114	UD. HARAPAN JAYA

18.	20976	TB-1760-8M-30	S0114	UD. HARAPAN JAYA
19.	20977	BELT TWIST 5M	S0505	DWIDAYA INTRANUSA
20.	20978	ROLLER CURVE COMPLETE	S0505	DWIDAYA INTRANUSA
21.	20988	TC-35/25LK	S0585	JIANGYIN SEJONE BELTECH
22.	20992	TB-1200-S8M-30	S0114	UD. HARAPAN JAYA
23.	20993	TB-1000-8M-30	S0114	UD. HARAPAN JAYA
24.	21003	TB-330 H 100	S0140	JAYA ABADI
25.	21004	SPC-3000	S0114	UD. HARAPAN JAYA
26.	21017	PB-30DG(PVC-3.0MM)	S0562	GUANGZHOU LIBO INDUSTRIAL
27.	21018	TB.1640-S8MX35	S0114	UD. HARAPAN JAYA
28.	21019	TB.880-8MX20	S0114	UD. HARAPAN JAYA
29.	21020	FEP 20 (PFA FILM)	S0402	JIANGSU VEIK TECHNOLOGY

## 2.2 Metode Pembeding

Hasil tinjauan pustaka dapat disimpulkan perbedaan penelitian dengan penelitian sebelumnya, yaitu:

- Penelitian sebelumnya menerapkan data file dokumen dan email proses enkripsi dan dekripsi, sedangkan penelitian saat ini hanya enkripsi dan dekripsi data teks.
- Penelitian sebelumnya hanya menggunakan kata kunci yang sama terhadap enkripsi dan dekripsi, sedangkan penelitian saat ini menggunakan kunci berbeda-beda pada saat enkripsi dan dekripsi
- Penelitian sebelumnya tidak menggunakan waktu enkripsi dan dekripsi, penelitian saat ini menggunakan waktu enkripsi dan dekripsi untuk mengetahui kecepatan proses.

## 2.3 Penerapan Metode

Dalam penerapan metode peneliti akan menjelaskan langkah penyelesaian metode dan formula yang digunakan :

### 2.3.1 Metode Caesar Cipher

Algoritma caesar cipher adalah algoritma klasik dengan langkah-langkah logis berikut ini:

- Menghitung panjang karakter yang dimasukkan dalam teks biasa.
- Setiap karakter diubah menjadi kode ASCII dalam proses perulangan.
- Untuk melakukan proses *encode*, kode ASCII digeser dengan menambahkan lebih banyak shift. Misalnya, memindahkan 3 huruf maka kode ASCII ditambah sebanyak 3.
- Jika spasi (ASCII=32), maka tidak perlu menambahkannya.
- Hasil pergeseran bilangan ASCII dikembalikan dalam bentuk huruf / karakter.

### 2.3.2 Metode Vigenere Cipher

Vigenere cipher menggunakan kunci dengan panjang tertentu, panjang kunci bisa kurang dari atau sama dengan panjang teks asli. Jika panjang kunci kurang dari panjang teks asli, maka kunci diulang sampai panjang kunci tersebut sama dengan panjang teks aslinya.

Algoritma enkripsi vigenere cipher:

$$C_i = (P_i + K_i) \bmod 95 \quad (1)$$

Algoritma dekripsi vigenere cipher

$$P_i = (C_i - K_i) \bmod 95 \quad (2)$$

Dimana:

$C_i$  = nilai decimal karakter *ciphertext* ke- $i$

$P_i$  = nilai decimal karakter *plaintext* ke- $i$

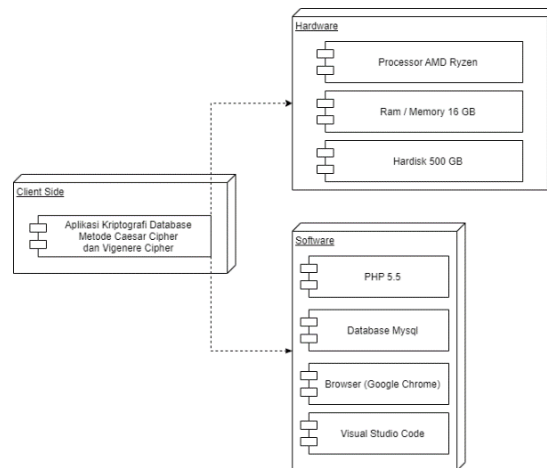
$K_i$  = nilai decimal karakter kunci ke- $i$

## 3. HASIL DAN PEMBAHASAN

### 3.1 Lingkungan Percobaan

Pengimplementasian aplikasi ini memerlukan kelengkapan *hardware* dan *software* pendukung.

Pembahasannya meliputi, diperlihatkan pada Gambar 1:



**Gambar 1.** Lingkungan Percobaan

### 3.2 Implementasi Metode

Berikut adalah langkah-langkah untuk menerapkan metode *Caesar Cipher* dan *Vigenere Cipher*

#### 3.2.1 Proses Enkripsi Data Barang

Untuk melakukan proses encrypt data barang atau transaksi, admin user terlebih dahulu memilih menu “Barang” lalu tekan button tambah barang, kemudian mengisi beberapa form, seperti deskripsi memilih supplier, kode, nama, satuan, dan harga yang wajib untuk tidak dikosongkan, setelah admin user menginput semua data barang, admin user menekan tombol submit, lalu semua data input akan terenkripsi dan masuk kedalam Database. Kemudian didalam aplikasi ini disediakan 2 tombol yaitu tombol “Cancel” dan tombol “Submit”, tombol cancel berfungsi untuk mencancel isi form client, dan tombol submit berfungsi untuk melanjutkan proses enkripsi data kedalam record database. seperti Gambar 2 berikut :



**Gambar 2.** Tampilan Layar Tambah Barang Proses Encrypt

Setelah muncul notifikasi input data barang berhasil terenkripsi oleh aplikasi ini, maka seluruh data akan masuk kedalam database dengan bentuk *atau* huruf acak algoritma *Caesar Cipher* dan *Vigenere Cipher*. Seperti Gambar 3.3 berikut ini:

barang_kode	barang_nama	barang_satuan	barang_harga	time_encrypt	time_decrypt
XOLI	E1MFDDLIYEMXVvPkTNLrTNLrTL==	FPYE	YELhXOLh	4.0054321289062E-5	5.1021575927734E-5
YvM5YFM=	FGxGG1HOF1ZUEENmGuMkAPHYwvUIUOMsUOMsUOMsUM==	GSZI	ZFMiYPMi	7.2956085205078E-5	9.0122222900391E-5
HeV5HOZ=	OPgPP1QXO1IDNNVsJYVrGOclFeHrDXvbDXvBvDXvBvDXvBvDX...	PBlu	IOVrHYVr	4.5061111450195E-5	0.00021219253540039
IfW5IfA=	NgycIPWsiYXUEZE1EBccIPXJPOXDQgRBPeWcEYW=	QCJv	JPWsiZWz	8.6069107055664E-5	0.00015997886657715
IfW5IfE=	NgycIPQ0iYXUEZE1EBccKA1JEAzONQRKEYWcEYWc	QCJv	JPWsiZWz	5.4121017456055E-5	8.702278137207E-5

**Gambar 3.** Tampilan Layar Tambah Barang Proses *Encrypt*

### 3.2.2 Proses Dekripsi Data Barang

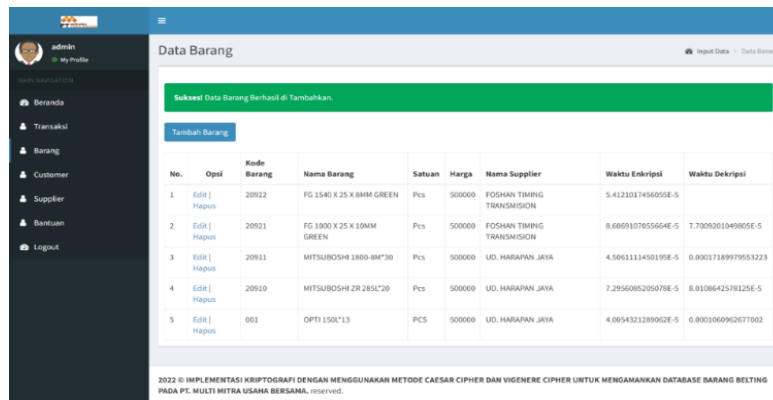
Jika data barang ingin dikembalikan menjadi text asli (*plaintext*) dan proses ini akan melalui proses dekritpsi pada sistem. Untuk melihat proses dekritpsi dapat dilihat pada Gambar 4 dan 5 berikut ini:

```

pages > barang.php
57 <tbody>
58 <tr>
59 <td>
60 <div style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;">
61 <pre>
62 <code><?php
63 $i = 1;
64 $db->connect();
65 $db->sql('SELECT A.*, B.*, A.time_encrypt as b_time_encrypt,
66 A.time_decrypt as b_time_decrypt FROM barang A
67 LEFT JOIN supplier B ON A.supplier_id = B.id_supplier
68 ORDER BY id_barang DESC');
69
70 $res = $db->getResult();
71
72 foreach ($res as $k => $val) {
73 $time_start = microtime(true);
74 $decrypt_kode = vigenerecipher_decrypt($cipher->decrypt($val['barang_kode'], $val['barang_key']));
75 $decrypt_nama = vigenerecipher_decrypt($cipher->decrypt($val['barang_nama'], $val['barang_key']));
76 $decrypt_satuan = vigenerecipher_decrypt($cipher->decrypt($val['barang_satuan'], $val['barang_key']));
77 $decrypt_harga = vigenerecipher_decrypt($cipher->decrypt($val['barang_harga'], $val['barang_key']));
78 $decrypt_s_nama = vigenerecipher_decrypt($cipher->decrypt($val['supplier_nama'], $val['supplier_key']));
79
80 </code>
81 </pre>
82 </div>
83 </td>
84 </tr>
85 </tbody>
86 </table>
87 </div>
88 </div>
89 </div>
90 </div>
91 </div>
92 </div>
93 </div>
94 </div>
95 </div>
96 </div>
97 </div>
98 </div>
99 </div>
100 </div>

```

Gambar 4. Tampilan Layar Proses Dekripsi Data Barang



Gambar 5. Tampilan Layar Data Barang yang telah Menjadi Tesk Asli

a. Algoritma Proses Sistem Enkripsi Algoritma *Caesar Cipher*

Algoritma enkripsi ini menerangkan bagaimana proses algoritma *Caesar Cipher* melakukan proses enkripsi sehingga berhasil mendapatkan *ciphertext*. Selama proses ini dilakukan, *plaintext* diinterpretasikan menjadi *chipertext* yang kemudian dilakukan proses menggunakan algoritma *Caesar Cipher*. Diperlihatkan pada gambar 6:

1. Masukkan plaintext
2. len = Panjang plaintext
3. P = Plaintext; S = Shift; C = Ciphertext4. i 4. = 0
5. for (i < len) do
6. ((P[i]+S) mod26)
7. i++
8. End For
9. write (ciphertext)

Gambar 6. Algoritma Proses Enkripsi Ceasar Cipher

b. Algoritma Proses Sistem Dekripsi Algoritma *Caesar Cipher*

Algoritma dekripsi ini menerangkan bagaimana proses algoritma *Caesar Cipher* melakukan proses dekripsi sehingga berhasil mendapatkan teks asli atau *plaintext*. Diperlihatkan pada gambar 7:

```

1. Masukkan kunci
2. len = Panjang ciphertext
3. P = Plaintext; S = Shift; C = Ciphertext
4. for (I < len) do
5.     P[i] = ((C[i]-S) mod26)
6.     i++
7. end for
8. write (plaintext)

```

**Gambar 7.** Algoritma Proses Dekripsi Ceasar Cipher

c. Algoritma Proses Sistem Enkripsi *Vigenere Cipher*

Algoritma proses enkripsi ini menerangkan bagaimana proses algoritma *Vigenere Cipher* melakukan proses enkripsi sehingga berhasil mendapatkan *ciphertext*. Pada proses ini akan menerangkan *plaintext* menjadi *chiphertext* yang nantinya akan dilakukan proses menggunakan algoritma *Vigenere Cipher*. Diperlihatkan pada gambar 8:

```

1. Masukkan plaintext
2. Masukkan kunci
3. P = Plaintext; C = Ciphertext; K = Kunci; len = Panjang Plaintext
4. i = 0
5. num;
6. for (i < len(P)) do
7.     num = tmod(num(C[i]) - num(K[i % strlen(K)]), 26)
8.     C[i] = chr(num + ord('A'))
9.     i++
10. end for
11. Return (C)
12. Tampilkan hasil
13. Selesai

```

**Gambar 8.** Algoritma Proses Enkripsi *Vigenere Cipher*

d. Algoritma Proses Sistem Dekripsi Algoritma *Vigenere Cipher*

Algoritma proses dekripsi ini menerangkan bagaimana proses dekripsi algoritma *Vigenere Cipher* melakukan proses dekripsi sehingga berhasil mendapatkan *chiphertext* atau *plaintext*. Diperlihatkan pada gambar 9:

```

1. Masukkan kunci
2. P = Plaintext; C = Ciphertext; K = Kunci; len = Panjang Plaintext
3. i = 0
4. num;
5. for (i < len(C)) DO
6.     num = tmod(num(C[i]) - num(K[i%len(K)]), 26)
7.     P[i] = chr(num + ord('a'))
8. end for
9. return (P)
10. Tampilkan hasil
11. Selesai

```

**Gambar 9.** Algoritma Proses Dekripsi *Vigenere Cipher*

### 3.3 Analisa dalam Penjabaran Pengujian

Pengujian di lakukan menggunakan memastikan semua fitur enkripsi dan dekripsi sudah berjalan dengan sesuai:

- a. Fitur enkripsi di proses pada saat melakukan tambah data dan ubah data

- b. Fitur dekripsi di proses pada saat melakukan tampil data
- c. Semua fitur tambah tampil ubah dan hapus pada menu transaksi, barang, supplier, dan customer pada pengujian enkripsi dan dekripsi berjalan sesuai

### 3.3.1 Tampilan Layar Login

Berikut adalah Tampilan Layar Halaman Login saat pertama user akses aplikasi, diperlihatkan pada Gambar 10:



Gambar 10. Tampilan Login

### 3.3.2 Tampilan Layar Beranda

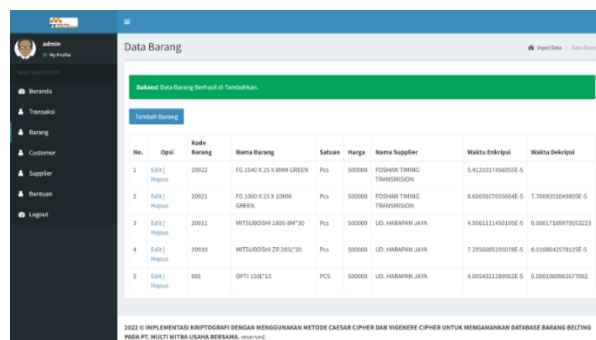
Berikut adalah Tampilan Layar Halaman Barang yaitu Halaman utama setelah user berhasil login, diperlihatkan pada Gambar 11:



Gambar 11. Tampilan Beranda

### 3.3.3 Tampilan Layar Tampil Barang

Berikut adalah Tampilan Layar Barang yaitu tampil data barang yang sudah di proses dekripsi dari table barang, lalu menampilkan data kode barang, nama barang, satuan, harga dan nama supplier, diperlihatkan Gambar 12 :



No.	Opsi	Kode Barang	Nama Barang	Satuan	Harga	Nama Supplier	Waktu Enkripsi	Waktu Dekripsi
1	SDR1 Majelis	20022	FG 124X125 X 8MM GREEN	Pcs	500000	FGSIHAN THINGING TRANSMESION	5.4122221436030E-5	
2	SDR1 Majelis	20021	FG 120X125 X 12MM GREEN	Pcs	500000	FGSIHAN THINGING TRANSMESION	8.6868017055564E-5	1.7089201044800E-5
3	SDR1 Majelis	20011	MITSUBISHI 1200 8M*20	Pcs	500000	UD HARAPAN JAYA	4.0361114519330E-5	0.006173897953223
4	SDR1 Majelis	20010	MITSUBISHI 20 20X120	Pcs	500000	UD HARAPAN JAYA	1.2956851200170E-5	0.0108642516123E-5
5	SDR1 Majelis	800	OPTI 120X13	PCS	500000	UD HARAPAN JAYA	4.0554211238026E-5	0.0053000824750E2

Gambar 12. Tampilan Data Barang

### 3.3.4 Tampilan Layar Tambah Barang

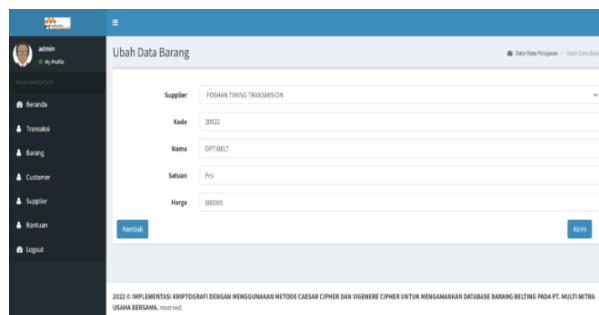
Berikut adalah Tampilan Layar Tambah Barang yaitu form tambah data barang untuk memproses enkripsi dengan cara user memasukan data barang lalu sistem mengenkripsi data barang, diperlihatkan Gambar 13:



**Gambar 13.** Tampilan Layar Tambah Barang

### 3.3.5 Tampilan Layar Ubah Barang

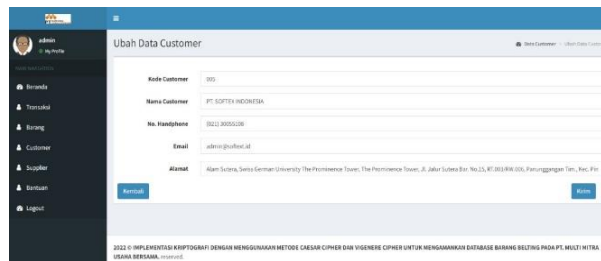
Berikut adalah Tampilan Layar Ubah Barang yaitu form ubah data barang untuk memproses enkripsi dengan cara user mengubah data barang lalu sistem mengenkripsi data barang, diperlihatkan Gambar 14:



**Gambar 14.** Tampilan Layar Ubah Barang

### 3.3.6 Tampilan Layar Ubah Data Customer

Berikut adalah Tampilan Layar Ubah Data *Customer* yaitu form ubah data customer untuk memproses enkripsi dengan cara user mengubah data *customer* lalu sistem mengenkripsi data *Customer*, diperlihatkan pada Gambar 15:



**Gambar 15.** Ubah Data *Customer*

### 3.3.7 Tampilan Layar Customer

Berikut adalah Tampilan Layar Customer yaitu tampil data barang yang sudah di proses dekripsi dari table *customer*, lalu menampilkan data kode customer, nama *customer*, email *customer* dan phone customer, dan alamat *customer*, diperlihatkan pada Gambar 16:

No.	Kode Customer	Nama	PPhone	Email	Alamat	WhatsApp	WhatsApp
1	001	PT. SOFTEX INDONESIA	082120303208	admin@softex.id	Alam Satria, Setia Gemari University The Performance Tower, The Performance Tower, Jl. Jabur Suban Bin No.12, RT.003 RW.001, Panunggapan Tem, Kec. Plo, Kota Suban, Setia Gemari, Indonesia	0 0850192068427	0 08502916885208
2	004	PT. AND INDONESIA	021231201980	admin@and.id	J. Hesper Vt pr (L), Karamong	6 380144307656	6 020008384930362
3	003	PT. JINDAL CRI Company Ltd.	813920	admin@jindalcri.com	J. Road Green Wagar Kulam, 17 P. 3, RT. 006, 2, Bantoran, Kec. Kudu, Kota Jabana Barat, Daerah Khusus Ibukota Jakarta 13132	6 08511381708676	6 0201950263977058
4	002	PT. MARIKA INDO	021231201980	admin@marika.com	J. Trusmi Raya Km 21 - 23, Jakarta Barat	6 380144307656	6 020008384930362
5	001	PT. ANDHICO CPT. PT. ANDHICO INDONESIA, Tbk	021231201980	admin@andhico.com	J. Habis No. 81, RT.001 RW.01, Tanah Barak, Kec. Tanah Barak, Kota Wajir, Jawa Barat 4013	6 380144307656	6 0201950263977058

**Gambar 16.** Tampil *Customer*



#### 4. KESIMPULAN

Berdasarkan analisis yang telah dilakukan dari pengumpulan data serta informasi, dengan pemecahan masalah sehingga pengembangan aplikasi ini, maka dapat membuat kesimpulan dan saran yang perlu diperhatikan agar sistem ini dapat berjalan dengan baik.

- a. Dibutuhkan suatu percobaan penerapan metode konversi pada teks dan pada video.
- b. Aplikasi yang telah di implementasikan dapat berguna dan dipakai sistem keamanannya oleh PT Multi Mitra Usaha Bersama.
- c. Diimplementasikan menggunakan bahasa pemrograman *PHP* dengan menggunakan algoritma *Caesar Cipher*, dan *Vigenere Cipher* untuk melakukan enkripsi dan dekripsi.

Untuk pengembangan lebih lanjut agar aplikasi ini dapat menjadi lebih baik lagi, adapun saran yang diberikan antara lain:

- a. Adanya pengembangan sistem aplikasi berbasis mobile menggunakan algoritma yang sama, dan percobaan metode konversi teks pada gambar video.
- b. Sistem masih sangat sederhana, diharapkan untuk dapat ditambah beberapa fitur seperti laporan penjualan dan laporan pembelian.
- c. Untuk ke depannya aplikasi ini bisa disempurnakan, serta diperbaharui setiap item yang tersedia dalam sistem aplikasi sehingga dapat mengikuti perkembangan zaman.

#### DAFTAR PUSTAKA

- [1] Marsian, E. S., Setiadi, I., & Cahyo, A. *Implementasi Sistem Keamanan Aes 256-Bit Gcm Guna Mengamankan Data Pribadi, JRKT: Jurnal Rekayasa Komputasi Terapan*, vol. 1, no. 2, pp. 108-114, 2021.
- [2] Hermawan, A., & Erik, I. *Implementasi Enkripsi Data Menggunakan Kombinasi AES dan RSA, Jurnal Nasional Informatika dan Teknologi Jaringan*, vol. 5, no. 2, pp. 326-330, 2021.
- [3] Fadlan, M., Haryansyah, & Rosmini, "Perpaduan Algoritma Kriptografi Atbash dan Autokey Cipher dalam Mengamankan Data," *Jurnal Media Informatika Budidarma*, vol. 5, no. 3, pp. 806-812, 2021.
- [4] Nugraha, A. P., & Gunandhi, E., "Penerapan Kriptografi BASE64 Untuk Keamanan URL (Uniform Resource Locator) Website dari Serangan SQL Injection," *Jurnal Algoritma*, vol. 13, no. 2, pp. 491-498, 2019.
- [5] N. B. Nugroho, Z. Azmi, & S. N. Arif, "Aplikasi Keamanan Email Menggunakan Algoritma RC4," *Jurnal Ilmiah SAINTIKOM*, vol. 15, no. 3, pp. 81-88, 2016.
- [6] M. D. Ramadhan, et al, "Rancang Bangun Sistem Keamanan Data Dengan Menerapkan Modifikasi Penggabungan Algoritma AES 256 dan BASE64," pp. 1-8, 2018.
- [7] Siswanto, Anif, M., & Gata, W., "Penerapan Algoritma Kriptografi Tea dan Base64 Untuk Mengamankan Email," *Jurnal ELTIKOM*, vol. 2, no. 1, pp. 34-41 (2018).
- [8] S. Siswanto, et al, "Penerapan Algoritma Kriptografi Twofish Untuk Mengamankan Data File," *Jurnal BIT*, vol. 18, no. 1, pp. 09-18, 2021.
- [9] Wahdani, S. V., Hartama, D., Okta Kirana, I., Poningsi, & Sumarno, "Pengamanan Data Pelanggan dan Penjualan Menggunakan Implementasi Kriptografi Metode RSA," *Journal of Informatics Management and Information Technology*, vol. 5, 1, pp. 101-107, 2021.
- [10] Putri, Y. D., Rosihan, & Lutfi, S., "Penerapan Kriptografi Caesar Cipher Pada Fitur Chatting Sistem Informasi Freelance," *Jurnal Informatika dan Ilmu Komputer (JIKO)*, vol. 2, no. 2, pp. 87-94, 2019.