ZONAsi Jurnal Sistem Informasi
ZONAsi VOL. 2 NO. 1 MARET 2020
Halaman 61 - 72
ISSN: 2656-7407 (Online)
2656-7393 (Cetak)

KEAMANAN DATA PADA PENGARSIPAN SURAT MENGGUNAKAN METODE KRIPTOGRAFI KLASIK VIGENERE CIPHER DAN SHIFT CIPHER

Gyna Rahmi Fajri[1], Sya'banu Ahmad[2], Refnaldi Kurniawan Saputra[3], Ewa Haris Sembiring[4] , Mhd Arief Hasan[5]

[1,2,3,4,5]Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Lancang Kuning

[1,2,3,4,5]Jl. Yos Sudarso KM. 8 Rumbai, Pekanbaru, Riau, Telp. 0811 753 2015

e-mail: [1]gynarahmi@gmail.com, [2]syachan3@gmail.com, [3]aldigul56@gmail.com, [4]ewaharis@gmail.com , [5]m.arif@unilak.ac.id

Abstrak

Pengarsipan surat adalah suatu kegiatan penyimpanan dokumen atau berbagai catatan informasi yang dibuat perorangan atau kelompok organisasi, lembaga, perusahaan dalam rangka kebutuhan tanda untuk kegiatan pelaksanaan yang dilakukan. pada saat ini keamanan sistem pengarsipan surat masih rentan dalam pencurian data. Oleh karena itu dibutuhkan sebuah sistem keamanan data untuk mengamankan informasi yang ada. Dengan penelitian ini yaitu pengamanan data pada sisi database, teknik pengamanan data ini menggunakan teknik kriptografi klasik. Dengan menggunakan gabungan dari metode vigenere cipher dan shift cipher/Caesar cipher. Hasil dari penelitian ini adalah memiliki kemampuan lebih dalam record database karena menggunakan 2 metode yaitu vigenere dan shift, sehingga sangat sulit untuk dibaca isi dari record tersebut dan untuk kekurangan nya untuk menampilkan waktu dalam proses enkripsi.

Kata kunci : *kriptografi, vigenere cipher, shift cipher, database.*

Abstract

Letter filing is an activity to keep documents or various information records made by individuals or groups of organizations, institutions, companies in the context of the need for signs for the implementation activities carried out. at this time the security of the letter filing system is still vulnerable to data theft. Therefore we need a data security system to secure existing information. With this research, namely data security on the database side, this data security technique uses classical cryptography techniques. By using a combination of the vigenere cipher method and shift cipher / Caesar cipher. The result of this research is to have more capability in the record database because it uses 2 methods, vigenere and shift, so it is very difficult to read the contents of the record and for its shortcomings to display the time in the encryption process.

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

1. PENDAHULUAN

Keamanan data merupakan sesuatu hal yang harus kita jaga saat ini karena menjaga data pribadi bisa mencegah seseorang untuk berpura-pura menjadi diri kita sendiri. Data - data yang berisikan informasi penting tidak boleh sampai tersebar karena bisa terjadi sampai di masa yang akan datang. Keamanan data menjadi hal sangat penting untuk diperhatikan karena kita harus menghindari hal-hal yang tidak diinginkan . Salah satu cara untuk mengatasi dan meningkatkan keamanan sebuah data dengan menggunakan metode enkripsi kriptografi, Metode enskripsi yang digunakan adalah sebagai perbandingan antara dua konsep kriptografi.

Database adalah kumpulan data yang disimpan secara sistematis didalam komputer dengan ketentuan dan aturan tertentu sehingga dapat diolah atau dimanipulasi menggunakan perangkat lunak (program aplikasi) untuk memperoleh informasi dari *database* tersebut. Database merupakan aspek yang sangat penting dalam sistem informasi karena *database* merupakan tempat penyimpanan data yang akan diolah lebih lanjut menjadi yang paling akurat. Untuk dapat mengakses kedalam *database* pengguna harus terkoneksi dengan jaringan komputer. Terkoneksinya jaringan komputer dapat menambah celah keamanan bagi database tersebut, salah satu cara untuk mengamankannya dengan menggunakan kriptografi.

Java adalah Bahasa pemograman serbaguna yang lahir pada saat penelitian yang dilakukan oleh sejumlah insinyur di sun California pada tahun 1991 dengan nama **oak** pada januari 1995. Nama oak dianggap kurang komersial , maka mereka mengubah namanya menjadi java Mereka membuat proyek pembuatan Bahasa pemograman yang dapat bejalan pada perangkat yang memiliki memori ukuran kecil

Menurut Indonesia (2018) dalam web nya berjudul *Kasus pencurian data terbesar yang terjadi di tahun 2017,* Kasus pencurian data semakin meningkat, dimana setiap harinya tercatat ada kasus pencurian dan kehilangan data seiring meningkatnya para pengguna aplikasi internet, maka meningkat pula kasus kejahatan internet menggunakan internet seperti *injection, Broken Authentication and Session Management, Cross-site Scripting.* kriptografi merupakan bidang ilmu untuk memberi keamanan pengiriman data dengan mengubah data menjadi kode kode secara acak dan hanya bisa dipecahkan oleh orang yang memiliki kata kunci untuk mengubah kode tersebut kembali menjadi sebuah data atau pesan.

Kriptografi adalah sebagai ilmu untuk menjaga sebuah kerahasiaan data, dan seperti authentikasi data. Namun pada pengertian modern kriptografi terdiri dari dua kegiatan yang saling berkaitan. dua proses tersebut disebut enkripsi dan deskripsi. Enkripsi adalah mengubah data atau yang disebut istilah plain text dalam kriptografi menjadi sebuah kode acak yang tidak dapat dibaca yang disebut cipher text.

Vigenere cipher merupakan algoritma kriptografi klasik yang dibuat pada abad ke-16 atau pada tahun 1986. Algoritma kriptografi sendiri ini dipublikasikan oleh seorang diplomat dan juga kriptologis yang berasal dari prancis, yaitu Blaise de Vigenere. Namun sebenarnya algoritma ini telah digambarkan sebelum nya pada buku La Cifra del sig (Bellaso, 1553). Cara kerja vigenere cipher ini mirip dengan Caesar cipher, yaitu mengenkripsi plaintext pada pesan dengan cara menggeser huruf pada pesan tersebut sejauh nilai kunci pada deret alphabet (Karman, 2009).

Shift cipher adalah salah satu teknik enkripsi paling sederhana dan paling dikenal luas. Ini adalah jenis sandi pengganti di mana setiap huruf dalam plaintext digantikan oleh huruf beberapa posisi tetap dibawah alphabet. Cara kerja shift cipher dimana susunan huruf ciphertext diperoleh dengan menggeser huruf huruf alphabet.

Pengarsipan surat adalah suatu proses kegiatan penyimpanan dan mengelola dokumen arsip tertentu untuk berbagai catatan informasi yang dibuat oleh individu atau kelompok, institusi. pada saat ini keamanan sistem pengarsipan surat masih rentan dalam pencurian data. Untuk menjaga keamanan data tersebut maka penulis membuat sistem keamanan menggunakan metode kriptografi agar data tidak dapat dicuri atau tidak mudah dibaca oleh orang- orang yang bertanggung jawab.

Rumusan masalah yang kami simpulkan adalah apa itu kriptografi? [1], Apa itu keamanan Data ? [2], Apa tujuan dari keamanan data pada pengarsipan surat? [3], Apa penyebab dari kasus pencurian data? [4]

Dari permasalahan yang penulis temukan , maka dapat simpulkan pengarsipan surat memerlukan suatu sistem untuk menjaga kerahasiaan data atau informasi yang ada agar terhindar dari hal hal yang tidak diinginkan, maka penulis melakukan penelitian yang berjudul **" *Keamanan data pribadi pada pengarsipan surat menggunakan metode kriptografi klasik vigenere cipher dan shift cipher"***

2. TINJAUAN PUSTAKA

Dalam peneletian ini akan digunakan sepuluh tinjauan studi yang akan menjadi rujukan dan juga nanti mendukung penelitian yang akan dilakukan, dimana tinjauan studi yang diambil adalah :

a. Oleh Joni Karman, Ahmad Nurhasan, dari Program Studi Sistem Informasi dan Informatika Universitas Bina Insan Lubuklinggau dengan judul Perancangan Sistem Keamanan Data *Inventory* Barang di Toko Nanda Berbasis Web Menggunakan Metode *Kriptografi Vigenere Cipher* untuk dapat membantu mengamankan data Toko Nanda serta mengetahui stok barang yang tersedia. Hasil dari penelitian ini adalah sebuah aplikasi berbasis *web* untuk keamanan data, yang menggunakan bahasa PHP, database menggunakan MySQL, dan untuk keamanan data nya menggunakan metode *kriptografi klasik* dengan algoritma *vigenere cipher*.
b. Oleh Mahya Azka dari Teknik Elektro Universitas Negeri Semarang dengan judul Implementasi Algoritma *Vigenere* dan *Columnar* Untuk Mengamankan Data Teks yang Disimpan di *Database MySQL*. Pada penelitian tersebut hasil enkripsi yang ada dalam bentuk file teks, yang didapat dari kombinasi algoritma columnar dan vigenere. Program tersebut menggunakan metode *waterfall* dan dibuat menggunakan bahasa pemrograman *PHP, HTML, CSS, Javascript* dan *MySQL*. Dari hasil penelitian ini didapatkan program tersebut dapat berjalan dengan baik, dan proses enkripsi dekripsinya juga baik.
c. Oleh Muhammad Andrian Nasuton, Edy Victor Haryanto, Alfa Saleh dengan judul Penerapan Metode *Hill Cipher dan Stream Cipher* Dalam mengamankan *Database MySQL*. Penelitian ini bertujuan mengamankan *database MySQL* dari para pencuri informasi. Pada penelitian ini menggunakan program aplikasi visual basic 2010 yang terhubung dengan database mysql, dan menggunakan metode enkripsi dekripsi hill cipher dikombinasikan dengan metode stream cipher.
d. Oleh Tomy Satria Alasi, Ahmad Taufik Al Afkari Siahaan dengan judul Algoritma *Vigenere Cipher* Untuk Penyandian Record Informasi Pada *Database.* Hasil dari penelitian ini adalah data yang tersimpan di database ter enkripsi dengan metode algoritma vigenere cipher.
e. Oleh Albi Dwi Haryono, Pipin Farida Ariyani dengan judul Aplikasi Pengaman Basis Data Pada Nuklindo Lab dengan *Algoritma Elgamal dan Affine Cipher.* Penelitian ini

memakai teknik kriptografi *Elgamal* Karena Keamanan *Elgamal* terletak terhadap sulitnya menghitung logaritma dan *Affine Cipher* dipilih dikarenakan perluasan berasal dari metode *Caesar Cipher*. Hasil penelitian ini membawa berlebihan record database dienkripsi benar-benar tinggi dikarenakan memakai 2 metode kriptografi, yaitu *Elgamal* dan *Affine Cipher* sehingga benar-benar sukar untuk dibaca isikan record tersebut serta kekurangannya hasil *text* hasil *enkripsi* bertambah panjang.

f. Oleh Adnan Buyung Nasution dengan judul Implementasi Pengamanan Data Dengan Menggunakan *Algoritma Caesar Cipher dan Transposisi Cipher*. Hasil dari penelitiani ini dengan proses penyandian dengan algoritma *Caesar Cipher* dan *Transposisi Cipher* berhasil digunakan untuk menyembunyikan pesan dan dapat mengembalikan pesan tersebut seperti semula. Program ini hanya bisa memproses karakter A hingga Z dikarenakan penggunaan angka 26.
g. Oleh Abduh Riski, Ahmad Kamsyakawuni, M. Ziaul Arif dari Program Studi Matematika FMIPA Universitas Jember dengan judul Implementasi *Vigenere Cipher* Pada Pengamanan Data Medis. Penelitian ini memperoleh hasil bahwa metode yang diambil dapat digunakanan untuk keamanan citra medis. Diperoleh NPCR sebesar 100% dengan rata-rata UACT 20% untuk citra RGB dan 43% untuk citra biner.
h. Oleh Agustin Siburian, Andy Paul Harianja dari Teknik Informatika UNIKA dengan judul Perancangan Aplikasi Pengamanan Basis Data Menggunakan Algoritma *Caesar Cipher*. Dipenelitian ini akan menggunakan cara dengan mengenkripsi plainteks dengan cara menggeser posisi plainteks sebanyak jumlah kunci. Hasil akhir dari penelitian ini memperoleh pengamanan data nilai pada basis data lebih terjamin keamanannya.
i. Oleh Ahmad Hanafi Sikumbang, Edy Victor Haryanto, Alfa Saleh dari Jurusan Teknik Informatika Universitass Potensi Utama dengan judul Kombinasi Metode *Stream Cipher* dan *Caesar Cipher* Dalam Pengamanan Data Kredit *Customer* (Studi Kasus : PT. ACE HARDWARE). Penelitian ini menggunakan pemrograman *visual basic 2010* dan menggunakan basis daa *SQL Server 2008*. Hasil dari penelitian ini dengan menggunakan metode *Stream Cipher dan Caesar Cipher* mendapatkan *Ciphertext* yang lebih baik dan lebih aman.
j. Oleh Safitri Jaya, Yane Arliana Kurniawati dari Sekolah Tinggi Teknologi Informasi NIIT I-Tech dengan judul Keamanan Data Pasien Baru Poliklinik Umum dengan Algoritma Sandi *Caesar*. Penelitian ini dibuat dengn menggunakan *MySQL* (sebagai databse) dan *Visual Studio 2010* yang dilengkapi dengan *function* algoritma sandi *Caesar* untuk mengenkripsi dan deskripsi data. Data yang sudah terenkripsi dengan aman pada database hanya dapat didekripsi oleh pengguna yang memiliki akses atau izin untuk melakukan dekripsi tersebut.

3. METODE PENELITIAN

3.1 Vigenere Cipher

Algoritma Vigenere Cipher adalah proses enkripsi yang hampir mirip dengan Caesar cipher / shift cipher yaitu dengan menggeser kuncinya, namun disini iya menggunakan tabel vigenere itu sendiri.

Plainteks diubah menjadi abjad yang lain dengan menggunakan kunci yang digeser sesuai dengan numeriknya.

Contoh :

A = 0, B = 1, C = 2 ……

Jika plainteks lebih panjang dari kunci, maka kunci digandakan hingga panjangnya sama dengan plainteks.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Gambar 1. Tabel Vigenere

Sebagai contoh pesan yang akan dienkripsi adalah FASILKOM dan kuncinya adalah AYAM. Hasil enkripsinya akan seperti ini.

Teks Asli	F	A	S	I	L	K	O	M
Kunci	A	Y	A	M	A	Y	A	M
Teks Cipher	F	Y	S	U	L	I	O	Y

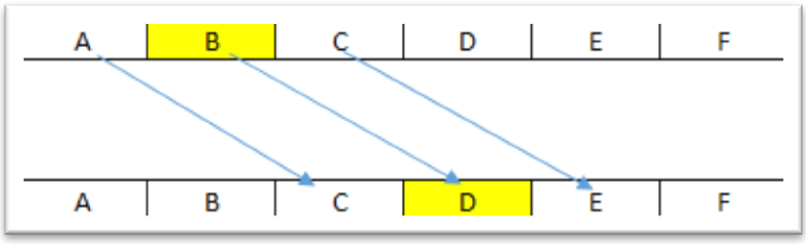
Cipher yang didapat adalah FYSULIOY, untuk persamaan enkripsi dan dekripsi dari vigenere dapat dituliskan seperti ini.

Enkripsi : $C_i = (p_i + ki) \bmod 26$ (1)

Dekripsi : $P_i = (c_i + k_i) \bmod 26$ (2)

3.2 Shift Cipher

Algoritma Shift Cipher adalah kode ini terdiri dari semua huruf pada plainteksnya dengan hasil cipher dengan selisih posisi tertentu. Proses shift cipher awalnya adalah menentukan berapa besar pemindahan atau penggeserannya. Sebagai contoh menggunakan penggeseran 2. Jadi, huruf A menjadi huruf C, huruf B menjadi D, dan seterusnya.



Gambar 2. Contoh Shift Cipher

Untuk persamaan yang digunakan adalah sebagai berikut.

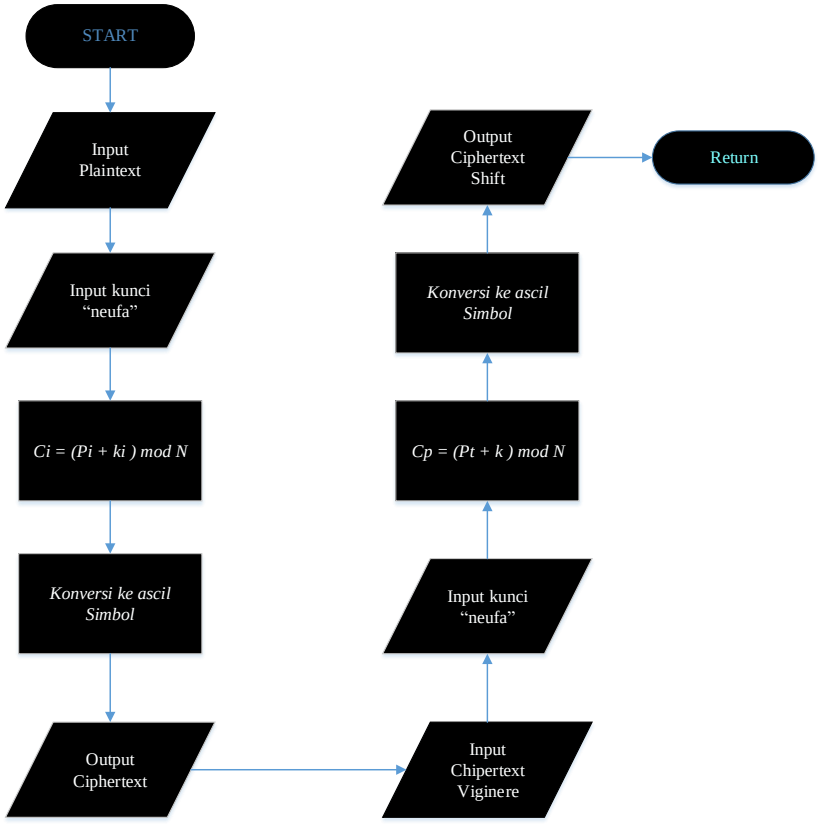
Enkripsi : $Cp = (Pt + k)\ Mod\ N$ (1)

Dekripsi : $Pt = (Cp - k)\ Mod\ N$ (2)

3.3 Flowchart Enkripsi Vigenere Cipher dan Shift Cipher

a. Flowchart Enkripsi Vigenere Cipher dan Shift Cipher

Dari Gambar 3 dibawah merupakan flowchart Enkripsi gabungan dari Viginere dan Shift Cipher dari gambar kita bisa lihat bahwa pertama kita melakukan input Plaintext , setelah kita meinputkan plaintext kita akan memasukan kata kunci nya yaitu “ neufa “ Setelah itu program akan melakukan scanner terhadap plaintext nya dengan kata kunci neufa, setelah program melakukan scanner akan keluar outputnya atau hasil dari plaintext nya yang disebut ciphertext karena ini merupakan dua metode yang digabungkan maka hasil dari viginere akan di ubah lagi ke shift cipher dengan cara yang sama

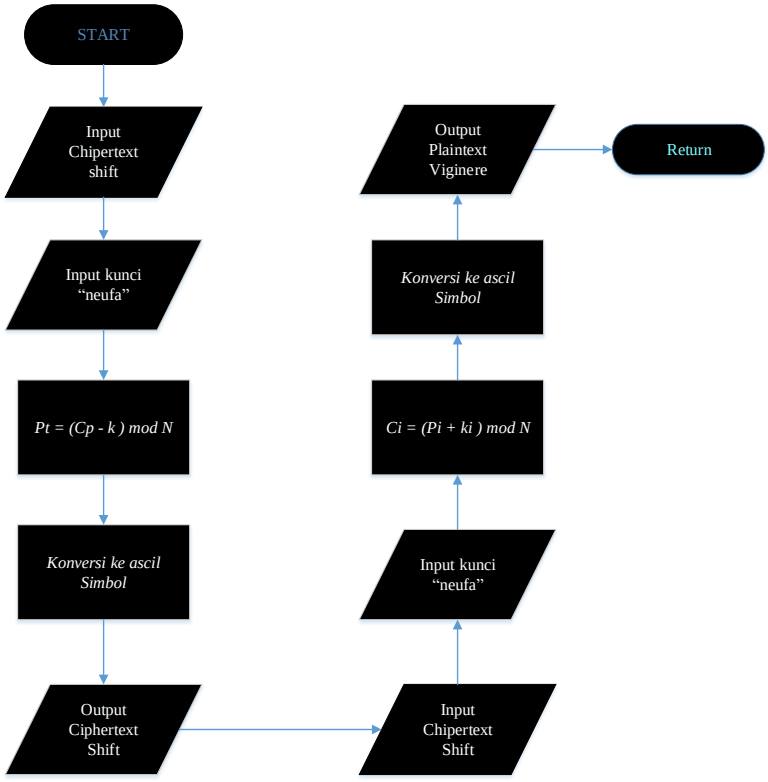


Gambar 3. Flowchart Enkripsi Viginere dan Shift Cipher

3.4 Flowchart Deskripsi Shift Cipher dan Viginere Cipher

a. Flowchart Deskripsi Shift Cipher

Dari Gambar 4 dibawah merupakan flowchart Deskripsi Shift Cipher gabungan Viginere cipher dari gambar dibawah jika kita ingin mengubah cipher teks dari shift cipher ke plaintext viginere cipher yang pertama kita lakuin adalah input cipher teks shift cipher tersebut setelah itu kita masukin kata kunci nya " neufa " dan program akan melakukan scanner dengan kata kunci tersebut dan akan keluar hasil dari cipher text shift dan kita kembali menginputkan hasil cipher text shift cipher untuk mendapatkan plaintext dari viginere cipher tersebut, setelah itu kita masukin kata kunci viginere cipher dan program akan melakukan scanner sehingga menghasil kan plaintext viginere



Gambar 4. Flowchart Deskripsi Shift cipher ke Viginere cipher

3.5 Source code Vigenere

Pada source code vigenere pesan didapatkan dari textfield password, dengan kunci "neufa". Ketika plainteks didapatkan maka selanjutnya scanner akan melakukan scan pada pesan, data huruf, dan kunci. Selanjutnya akan melakukan perhitungan untuk menampilkan hasil enkripsi.

```
//VIGENEKE
String dataHuruf = "1234567890-abcdefghijklmnopqrstuvwxyz .";

String pesan = "";
pesan = password.getText();
String kunci = "neufa";
String chiper = "";

ArrayList en = new ArrayList();
ArrayList de = new ArrayList();

Scanner s = new Scanner();
ArrayList sP = s.scannPesan(pesan, dataHuruf);
ArrayList sK = s.scannKuci(pesan, kunci, dataHuruf);

System.out.println("Enkripsi");
EnkripDekrip ed = new EnkripDekrip();
for (int i = 0; i < pesan.length(); i++) {
    int iP = Integer.parseInt(sP.get(i).toString());
    int iK = Integer.parseInt(sK.get(i).toString());
    int gE = ed.getEnkrip(iP, iK, dataHuruf);

    en.add(gE);

}
```

Gambar 5. Source Code Vigenere

3.6 Source code Shift

Setelah proses enkripsi dari vigenere selesai, maka selanjutnya proses dilanjutkan dengan enkripsi shift cipher. Pada enkripsi shift cipher data huruf yang digunakan adalah tabel ASCII, dengan shiftnya bernilai 1. Maksudnya adalah nilai pada plainteks akan ditambah satu, sebagai contoh apabila A maka akan menjadi B.

```
String isitext = vigenere.getText();
String out= "" ;
 for (int i = 0; i < isitext.length(); i++) {
    int index = isitext.charAt(i);
    char s = (char)(index+1) ;
    out = out+ String.valueOf(s);
 }
hasilvigeneredanshift.setText(out);
vigenere.setText("");
System.out.println("Hasli Enkripsi :" + out);
JOptionPane.showMessageDialog(null, "ENKRIPSI BERHASIL !\nSILAHKAN SAVE DATA ANDA");
```

Gambar 6. Source Code Shift

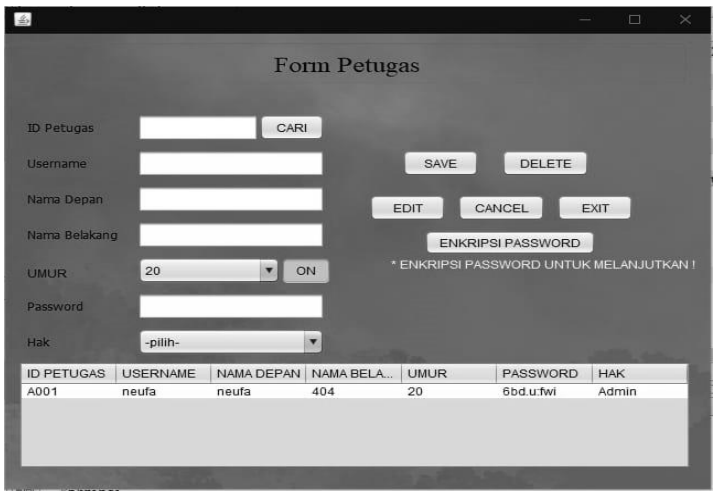
4. HASIL DAN PEMBAHASAN

4.1 Tampilan aplikasi

Tampilan berikut ini merupakan tampilan form fungsi utama yang digunakan dari aplikasi ini.

A. Tampilan form petugas

Pada tampilan ini petugas dapat menambahkan petugas baru, mengedit, atau menghapus data. Pada form ini enkripsi digunakan pada input password, ketika akan menyimpan ataupun mengedit data. Sebelum melakukan penyimpanan, diharuskan untuk enkripsi password terlebih dahulu.



Gambar 7. Form petugas

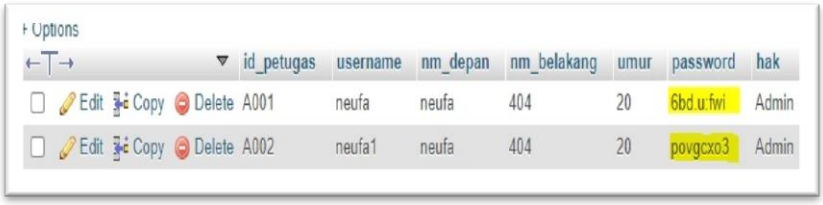
B. Tampilan form surat keluar

Form surat keluar berfungsi agar petugas mengetahui apakah surat telah dikirim atau tidak. Pada form ini yang di enkripsi adalah bagian perihal dari surat. Setelah petugas memasukkan perihalnya, maka secara otomatis akan berubah teksnya menjadi enkripsi dan akan tersimpan didatabase.

Gambar 8. Form surat keluar

C. Tampilan data base

Database ini menunjukkan adanya data yang telah dienkripsi. Terlihat pada tabel password teks yang tampil adalah teks acak.



Options

	id_petugas	username	nm_depan	nm_belakang	umur	password	hak
Edit Copy Delete	A001	neufa	neufa	404	20	6bd.u:fwi	Admin
Edit Copy Delete	A002	neufa1	neufa	404	20	povgcxo3	Admin

Gambar 9. Data base

4.2 Pengujian

pengujian ini dilakukan untuk mengetahui panjang teks awal dengan teks yang akan di hasilkan dengan proses enkripsi memiliki panjang yang sama dengan teks aslinya.

```
Output - pengarsipan_surat (run)
Enkripsi
Pesan  : iykwiml2
Kunci  : neufa
Hasli Enkripsi  :5ac-t9ev
Enkripsi
Pesan  : iykwiml23
Kunci  : neufa
Hasli Enkripsi  :5ac-t9evh
Hasli Enkripsi  :6bd.u:fwi
Enkripsi
```

Gambar 10. Pengujian enkripsi

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari Hasil Penelitian yang dilakukan, Penulis menemukan beberapa kesimpulan yaitu algoritma vigenere cipher merupakan algoritma dengan pengenkrisipan teks yang sangat sederhana dan mudah karena berdasarkan tabel yang sudah ada namun bisa menjaga kerahasiaan karena huruf plaintext yang dienkripsi tidak sama dengan ciphertext yang dihasilkan. Dari hasil percobaan diatas dapat disimpulkan juga bahwa keamanan data pribadi pada pengarsipan surat sudah terbilang aman karena algoritma vignere hasil dari pengenkripsian nya tidak sama dengan plaintext nya jadi sehingga bagi orang awam itu sudah sangat sulit jika karakter algoritma nya panjang.

5.2 Saran

Setelah menarik beberapa kesimpulan, didapatkan saran yang mungkin dapat digunakan sebagai pertimbangan dalam pengembangan system, diantaranya :

a. Diharapkan tampilan dari system tersebut dapat menunjukkan progress atau waktu lama dari enkripsinya.
b. Diharapkan adanya perkembangan system yang lebih baik, sehingga program ini dapat digunakan dalam waktu yang lama.
c. Diharapkan dilakukannya pelatihan terlebih dahulu dalam penggunaan program ini.

DAFTAR PUSTAKA

[1] T. S. Alasi, A. T. Al, and A. Siahaan, "Algoritma Vigenere Cipher Untuk Penyandian Record Informasi Pada Database," *J. Inf. Komput. Log.*, vol. 1, no. 4, 2020, [Online]. Available: http://ojs.logika.ac.id/index.php/jikl.

[2] J. Karman and A. Nurhasan, "Perancangan Sistem Keamanan Data Inventory Barang Di Toko Nanda Berbasis Web Menggunakan Metode Kriptografi Vigenere Cipher," *J. Teknol. Inf. MURA*, vol. 11, no. 1, pp. 29–36, 2019, doi: 10.32767/jti.v11i1.451.

[3] M. Z. A. ABDUH RISKI, AHMAD KAMSYAKAWUNI, "IMPLEMENTASI VIGENERE CIPHER PADA Pendahuluan Citra Digital," vol. 02, no. 01, pp. 23–30, 2018.

[4] M. Azka, "Columnar Untuk Mengamankan Data Teks," 2019.

[5] A. D. Haryono *et al.*, "Aplikasi Pengaman Basis Data Pada Nuklindo Lab," vol. 1, no. 1, pp. 186–192, 2018.

[6] A. H. Sikumbang *et al.*, "Kombinasi Metode Stream Cipher Dan Caesar Cipher Dalam Pengamanan Data Kredit Customer (Studi Kasus : PT . ACE HARDWARE)," pp. 693–706, 2020.

[7] S. Jaya and Y. A. Kurniawati, "KEAMANAN DATA PASIEN BARU POLIKLINIK UMUM dengan ALGORITMA SANDI CAESAR (Studi Kasus : RS Sentra Medika Cibinong)," vol. 12, no. 1, pp. 13–21, 2016.

[8] A. A and D. Dasril, "Perancangan Aplikasi Pengamanan Data Menggunakan Algoritma XOR," *J. IT*, vol. 8, no. 1, pp. 61–69, 2017.