Penerapan Kriptografi Menggunakan Caesar Cipher Dan Vigenere Cipher

Gracia Barbara Minarto[*1], Muhammad Qadafi Khairuzzaman[2]
[1,2]Jurusan Teknik Informatika; STMIK Pontianak. Jl. Merdeka No.372 Pontianak, 0561-735555
e-mail: [*1]graciablue28@gmail.com, m.qadafi.k@gmail.com

Abstrak

Dalam menjamin kerahasian dan keamanan suatu data diperlukan metode kriptografi, yang merupakan metode untuk menjaga kerahasian pada informasi. Pada dasarnya data tersebut tanpa ada melakukan pengamanan terhadap data yang diberikan, sehingga ketika dilakukan penyadapan terhadap alur pengirimanya maka data yang diambil tidak dapat langsung dibaca oleh penyadap. Untuk itu dibutuhkan perangkat lunak sebagai penunjang metode tertentu sehingga pesan terkirim tersebut menjadi lebih aman. Dalam penelitian ini penulis menggunakan bentuk penelitian studi literatur dan eksperimen. Sedangkan metode perancangan perangkat lunak menggunakan metode Prototype karena proses perkembangan perangkat lunak ini menekankan pada siklus perkembangan yang singkat. Adapun teknik pengumpulan data menggunakan studi dokumentasi dan observasi untuk memperoleh teori Caesar Cipher dan Vigenere Cipher. Penggunaan metode Caesar Cipher dan Vigenere Cipher termasuk cukup cepat dalam melakukan proses enkripsi dan dekripsi pada sebuah data penjulan. Perancangan perangkat lunak menggunakan bahasa pemrograman NetBeans IDE hasil perancangan didapatkan dalam penelitian ini bisa dilihat pada bab hasil penelitian yang akan menampilkan semua proses pada aplikasi ini.

Kata kunci : *Kriptografi, Caesar Cipher, Vigenere Cipher, NetBeans.*

Abstract

In ensuring the confidentiality and security of a data cryptographic method is needed, which is a method for maintaining confidentiality of information. Basically the data without any security to the data provided, so that when tapping the flow of the sender, the data taken cannot be read directly by the tappers. For this reason, software is needed to support certain methods so that the sent message becomes safer. In this study the author uses a form of literature study and experiment research. While the software design method uses the Prototype method because the software development process emphasizes a short development cycle. The data collection technique uses documentation and observation studies to obtain the theory of Caesar Cipher and Vigenere Cipher. The use of Caesar Cipher and Vigenere Cipher methods is quite fast in the process of encryption and decryption in a data collection. Software design using the NetBeans IDE programming language design results obtained in this study can be seen in the research results chapter which will show all the processes in this application.

Keywords : *cryptography, Caesar Cipher, Vigenere Cipher, NetBeans.*

1. PENDAHULUAN

Informasi penjualan sangatlah penting bagi perusahaan karena kunci kesuksesan dalam mengelola bisnis adalah dengan lebih mengandalkan data. Perusahaan biasa memberikan data barang yang akan dijual ke konsumen. Cara memberikan data pada setiap perusahaan berbeda-beda. Salah satu caranya adalah dengan memberikan data yang disimpan di flash disc. Pada saat kepala perusahaan memberikan data akan melewati staff atau karyawan perusahaan dan kemudian baru sampai ditangan konsumen. Akan tetapi, dikhawatirkan terjadinya pengubahaan pada data saat memberikan ke konsumen maka diperlukan pengenkripsi dan dekripsi pada data. Untuk menjamin kerahasiaan suatu informasi, dapat dilakukan dengan menggunakan kriptografi. Salah satunya kriptografi yang digunakan adalah caesar cipher dan vigenere cipher.

Penelitian yang berkaitan dengan kriptografi ialah [1] implementasi kombinasi caesar cipher dan affine cipher untuk keamanan data teks disimpulkan bahwa hasil penelitian menunjukkan kombinasi Caesar cipher dan Affine cipher dapat membantu meningkatkan keamanan data, jika dibandingkan hanya menggunakan satu buah metode saja. Sedangkan penelitian yang tentang [2] "implentasi enkripsi data dengan algoritma vigenere cipher" dapat meningkatkan tingkat keamanan pendataan penjualan, khususnya pada data harga. Kemudian penelitian untuk [3]menjamin kerahasiaan suatu informasi, dapat dilakukan dengan menggunakan kriptografi. Kriptografi Metode WAKE merupakan salah satu metode yang telah digunakan secara komersial. WAKE merupakan singkatan dari Word Auto Key Encryption dan merupakan salah satu algoritma stream cipher yang cepat dalam implementasinya dalam perangkat lunak. Metode ini menggunakan kunci 128 bit, plaintext 32 bit dan sebuah tabel 256 x 32 bit. Dalam algoritmanya, metoda ini menggunakan operasi XOR, AND, OR dan Shift Right. Inti dari metode WAKE terletak pada proses pembentukan tabel S-Box dan proses pembentukan kunci. Tabel S-Box dari metode WAKE bersifat fleksibel dan berbeda-beda untuk setiap putaran. Perangkat lunak ini menunjukkan setiap langkah dan tahapan proses-proses(proses pembentukan table S-Box, proses pembentukan kunci, proses enkripsi dan proses dekripsi) yang terdapat di dalam kriptografi metode WAKE, sehingga dapat membantu pemahaman atau pembelajaran prosedur kerja atau algoritma dari metode kriptografi tersebut. Semakin banyak putaran dari proses pembentukan kunci, maka keamanan data akan semakin terjamin.

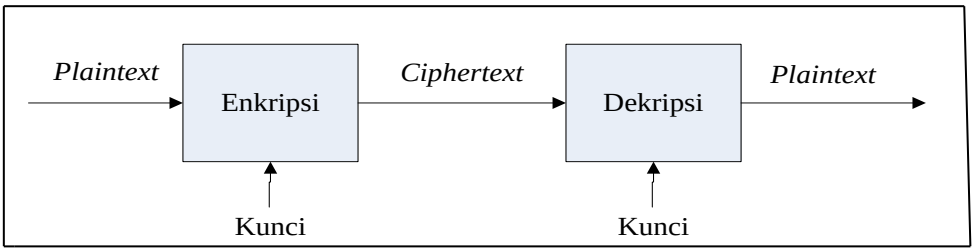
Kriptografi dapat pula diartikan sebagai ilmu atau seni untuk menjaga keamanan pesan. Terdapat empat tujuan dasar dari kriptografi yang menjadi aspek keamanan informasi dah harus diperhatikan dalam penggunaan kriptografi sebagai berikut [4]:

1. Kerahasiaan (*Confidentiality*) adalah layanan yang digunakan untuk menjaga isi informasi dari siapapun kecuali yang memiliki kunci rahasia atau otoritas untuk membuka informasi yang telah disandikan.
2. Integrasi data (*Data Integrity*) berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk dapat untuk menjaga dari integrasi data, suatu sistem harus memiliki kemampuan untuk mendeteksi manipulasi data yang dilakukan pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan dan pendistribusian data lain ke dalam data asli.
3. Otentikasi (*Authentification*) berhubungan dengan identifikasi, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan harus diotentifikasi keasliannya, isi datanya, waktu pengiriman dan lain sebagainya.
4. Non-repudasi (*Non-repudation*) merupakan usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman atau terciptanya suatu informasi oleh yang mengirimkan atau membuat.

Dalam era teknologi informasi sekarang ini, mekanisme yang sama masih digunakan tetapi tentunya implementasi sistemnya berbeda. Sebelum membahas lebih jauh mekanisme kriptografi modern,berikut ini diberikan beberapa istilah yang umum digunakan dalam pembahasan kriptografi [5] :

1. Plaintext (*message*) merupakan pesan asli yang ingin dikirimkan dan dijaga keamanannya. Pesan ini tidak lain dari informasi tersebut.
2. Chipertext merupakan pesan yang telah dikodekan (disandikan) sehingga siap untuk dikirimkan.
3. Cipher merupakan algoritma matematis yang digunakan untuk proses Enkripsi plaintext menjadi ciphertext.
4. Enkripsi (*encryption*) merupakan proses yang dilakukan untuk menyandikan plaintext sehingga menjadi chipertext.
5. Dekripsi (*decryption*) merupakan proses yang dilakukan untuk memperoleh kembali plaintext dari chipertext.
6. Kriptosistem merupakan sistem yang dirancang untuk mengamankan suatu sistem informasi dengan memanfaatkan kriptografi.

Kriptografi modern selain memanfaatkan algoritma juga menggunakan kunci (*key*) untuk memecahkan masalah tersebut. Proses enkripsi dan dekripsi dilakukan dengan menggunakan kunci ini. Setiap anggota memiliki kuncinya masing-masing yang digunakan untuk proses enkripsi dan dekripsi yang akan dilakukannya(yang didapat lihat pada gambar 1).



Gambar 1 Kriptografi Berbasis Kunci

Sandi Caesar diambil dari nama kaisar romawi Julius Caesar, dalam mengirimkan pesan Julius Caesar mengamankannya dengan cara isi pesan yang ada disandikan dengan mengganti posisi setiap huruf yang ada pada pesan dengan huruf lain yang memiliki posisi selisih huruf yang lain dari urutan alfabet[6]. Adapun langkah – langkah yang dilakukan adalah sebagai berikut :

1. Menentukan besarnya jumlah pergeseran huruf yang akan diganti
2. Mengganti setiap huruf yang ada pada pesan sesuai dengan jumlah pergeseran huruf yang ditentukan.
3. Merangkai kembali jumlah huruf sesuai dengan susunan pesan awal

Tabel 1 Susunan Abjad

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Untuk menyandikan suatu pesan cukup mengganti huruf yang ada pada pesan dengan huruf sandi sesuai dengan jumlah pergeseran huruf yang diinginkan. Contoh Enkripsi Caesar :

Teks Awal : PESAN INI SANGAT RAHASIA

Jumlah geser (Key) : 12
Teks Sandi : BQEMZ UZU EMZSMF DMTMEUM

Sandi Vigenere adalah suatu algoritma yang digunakan untuk Enkripsi data atau pesan dengan cara data atau pesan akan disandikan dengan menggunakan sebuah kata kunci (Key) yang berupa kata atau paduan kata[6]. Setiap huruf yang ada pada data atau pesan dipasangkan tepat dengan huruf yang terdapat pada kata kunci yang ditentukan, lalu kemudian dilakukan proses Enkripsi yaitu enkripsi. Contoh penggunaan sandi Vigenere :

Teks Awal : PESAN INI SANGAT RAHASIA
Kata Kunci : ARMADA
Teks Sandi : PVEAQ INZ EAQGAK DAKASZM

2. METODE PENELITIAN

Bentuk penelitian yang penulis gunakan dalam penelitian ini adalah metode studi literatur dan perancangan eksprimen. Studi literatur merupakan studi yang bisa dijadikan sebagai bahan untuk mengumpulkan dan mengkaji data dengan membaca berbagai literatur seperti buku, skripsi, jurnal maupun bentuk tulisan lainnya yang isinya berkaitan dengan masalah yang akan diteliti sebagai bahan referensi tertulis. Eksperimen dilakukan dengan cara melakukan perancangan, implementasi sistem untuk membuat gambaran yang jelas dari masalah yang dihadapi. Metode penelitian yang digunakkan adalah metode prototype karena metode ini mengusulkan sebuah pendekataan perkembangan perangkat lunak yang baik yang dimulai pada tingkat dan kemajuan. Ada dua jenis data yang digunakan dalam penelitian ini adalah data primer dan data sekunder.

Ada empat langkah yang diuraikan Prototype sebagai berikut [7]:

1. Mengidentifikasi kebutuhan pengguna.
   Pengembangan mewawancarai pengguna untuk mendapatkan ide mengenai apa yang diminta dari sistem.
2. Mengembangkan prototype.
   Pengembangan mempergunakan satu alat prototyping atau lebih untuk membuat atau mengembangkan prototype.
3. Menentukan apakah prototype dapat diterima atau tidak.
   Pengembang mendemotrasikan prototype kepada para pengguna untuk mengetahui apakah telah memberikan hasil yang memuaskan, jika sudah, langkah keempat akan diambil. Jika tidak, prototype direvisi dengan mengulang langkah satu, dua dan tiga dengan pemahaman yang lebih baik mengenai kebutuhan pengguna.
4. Menggunakan prototype.
   Prototype ini menjadi sistem operasional.

3. HASIL DAN PEMBAHASAN

3.1 Sandi Caesar

Terdapat suatu data atau pesan yang akan disandikan dengan menggunakan algoritma Caesar. Teks data atau pesan awal yang akan di sandikan yaitu PESAN INI SANGAT RAHASIA. Berikut adalah proses Enkripsi dengan menggunakan algoritma Caesar.

Teks awal : PESAN INI SANGAT RAHASIA
Key : 12
Proses enkripsi :
Rumus : E(P)=C, C=P+K Mod 26
Keterangan:

E(P) : Enkripsi
P : Plaintext (Teks Awal)
K : Key (Jumlah Pergeseran)

Teks / pesan sandi (Ciphertext) : BQEMZ UZU EMZSMF DMTMEUM
Proses dekripsi :
Rumus : D(C)=P, P=C-K mod 26
Keterangan:
D(C) : Dekripsi
C : Ciphertext (Teks akhir)
K : Key (Jumlah Pergeseran)

Teks/pesan sandi (Ciphertext) : BQEMZ UZU EMZSMF DMTMEUM
Teks/pesan awal (Plaintext) : PESAN INI SANGAT RAHASIA

3.2 Sandi Vigenere

Terdapat suatu data atau pesan yang akan disandikan dengan menggunakan algoritma Vigenere. Teks data atau pesan awal yang akan di sandikan yaitu PESAN INI SANGAT RAHASIA dengan kunci ARMADA. berikut adalah proses Enkripsinya dengan algoritma vigenere.
Teks awal (Hasil dari Enkripsi Caesar)= PESAN INI SANGAT RAHASIA
Kunci (Key) = ARMADA

Proses Enkripsi :

Tabel 2 Tabel Enkripsi Vigenere Cipher

Plaintext	P	E	S	A	N	I	N	I	S	A	N	G	A	T	R	A	H	A	S	I	A
Posisi abjad	15	4	18	0	13	8	13	8	18	0	13	6	0	19	17	0	7	0	18	8	0
Kunci	A	R	M	A	D	A	A	R	M	A	D	A	A	R	M	A	D	A	A	R	M
Posisi abjad	0	17	12	0	3	0	0	17	12	0	3	0	0	17	12	0	3	0	0	17	12
	15	21	30	0	16	8	13	25	30	0	16	6	0	36	29	0	10	0	18	25	12
Cipher text	P	V	E	A	Q	I	N	Z	E	A	Q	G	A	K	D	A	K	A	S	Z	M

Hasil Enkripsi :
PVEAQ INZ EAQGAK DAKASZM

Proses dekripsi :
Rumus : D(C)=P, P=C-K mod 26
D(C) : Dekripsi
C : Ciphertext (Teks akhir)
K : Key (Kata / Kalimat)

Tabel 3 Tabel Dekripsi Vigenere Cipher

Plaintext	P	V	E	A	Q	I	N	Z	E	A	Q	G	A	K	D	A	K	A	S	Z	M
Posisi	1	2	4	0	1	8	1	2	4	0	1	6	0	1	3	0	1	0	1	2	1

abjad	5	1			6		3	5			6			0			0		8	5	2
Kunci	A	R	M	A	D	A	A	R	M	A	D	A	A	R	M	A	D	A	A	R	M
Posisi abjad	0	17	12	0	3	0	0	17	12	0	3	0	0	17	12	0	3	0	0	17	12
	15	4	-8	0	13	8	13	8	-8	0	13	6	0	-7	-9	0	7	0	18	8	0
Cipher text	P	E	S	A	N	I	N	I	S	A	N	G	A	T	R	A	H	A	S	I	A

3.3 Kombinasi Sandi Caesar dan Vigenere

Jika algoritma Caesar dan Vigenere kita kombinasikan, maka akan menghasilkan kekuatan enkripsi yang cukup kuat karena apabila terjadi penyadapan pesan hasil penyadapan tersebut masih dalam keadaan terenkripsi. Berikut contoh kombinasi dari sandi Caesar dan sandi Vigenere :

1. Contoh enkripsi pertama

   Pesan akan disandikan : DATA PENJUALAN

   a. Enkripsi dengan sandi Caesar

   Teks Awal : DATA PENJUALAN

   Kunci (Key) : 12

   Cipher Text : PMFM BQZVGMXMZ

   Rumus enkripsi : E(P)=C, C=P+K Mod 26

   Proses Enkripsi sandi Caesar :

Tabel 4 Enkripsi Plainteks Caesar Contoh 1

Plainteks	D	A	T	A		P	E	N	J	U	A	L	A	N
Posisi abjad	3	0	19	0		15	4	13	9	20	0	11	0	13
Kunci (Key)	12	12	12	12		12	12	12	12	12	12	12	12	12
	15	12	31	12		27	16	25	21	32	12	23	12	25
Cipherteks	P	M	F	M		B	Q	Z	V	G	M	X	M	Z

Hasil Enkripsi dengan sandi Caesar kemudian menjadi pesan awal yang akan disandikan kembali dengan sandi Vigenere.

b. Enkripsi dengan sandi Vigenere

Teks Awal : PMFM BQZVGMXMZ

Key : PERMATA

Cipher Text : EQWY BJZKKDJMS

Rumus enkripsi : E(P)=C, C=P+K Mod 26

Proses Enkripsi sandi Vigenere :

Tabel 5 Enkripsi Plainteks Vigenere Contoh 1

Planteks	P	M	F	M		B	Q	Z	V	G	M	X	M	Z

Posisi abjad	15	12	5	12		1	16	25	21	6	12	23	12	25
Kunci (Key)	P	E	R	M		A	T	A	P	E	R	M	A	T
Posisi abjad	15	4	17	12		0	19	0	15	4	17	12	0	19
	30	16	22	24		1	35	25	36	10	29	35	12	44
Cipherteks	E	Q	W	Y		B	J	Z	K	K	D	J	M	S

Hasil akhir yang diperoleh adalah berupa pesan yang telah disandikan dengan sandi Vigenere.

2. Contoh enkripsi kedua
   a. Enkripsi dengan sandi Caesar
      Teks Awal : CAESAR DAN VIGENERE
      Kunci (Key) : 8
      Cipher Text : KIMAIZ LIV DQOMVMZM
      Rumus enkripsi : E(P)=C, C=P+K Mod 26
      Proses Enkripsi sandi Caesar :

Tabel 6 Enkripsi Plainteks Caesar Contoh 2

Plainteks	C	A	E	S	A	R		D	A	N		V	I	G	E	N	E	R	E
Posisi abjad	2	0	4	18	0	17		3	0	13		21	8	6	4	13	4	17	4
Kunci (Key)	8	8	8	8	8	8		8	8	8		8	8	8	8	8	8	8	8
	10	8	12	26	8	25		11	8	21		29	16	14	12	21	12	25	12
Ciphertek s	K	I	M	A	I	Z		L	I	V		D	Q	O	M	V	M	Z	M

   b. Enkripsi dengan sandi Vigenere
      Teks Awal : KIMAIZ LIV DQOMVMZM
      Key : ABCDE
      Cipher Text : KJODMZ MKY HQPOYQZN
      Rumus enkripsi : E(P)=C, C=P+K Mod 26
      Proses Enkripsi sandi Vigenere :

Tabel 7 Enkripsi Plainteks Vigenere Contoh 2

Plainteks	K	I	M	A	I	Z		L	I	V		D	Q	O	M	V	M	Z	M

Posisi abjad	10	8	12	0	8	25		11	8	21		3	16	14	12	21	12	25	12
Kunci (Key)	A	B	C	D	E	A		B	C	D		E	A	B	C	D	E	A	B
Posisi abjad	0	1	2	3	4	0		1	2	3		4	0	1	2	3	4	0	1
	10	9	14	3	12	25		12	10	24		7	16	15	14	24	16	25	13
Ciphertek s	K	J	O	D	M	Z		M	K	Y		H	Q	P	O	Y	Q	Z	N

Kemudian hasil proses dari kombinasi dengan sandi Caesar dan Vigenere pesan sudah siap dikirimkan.

Untuk penerima pesan yang telah disandikan tersebut, harus melakukan proses dekripsi atau mengembalikan pesan yang tersandikan menjadi pesan awal sebelum kombinasi Enkripsi pesan dilakukan sehingga isi pesan tersebut dapat dibaca dan dipahami. Berikut adalah proses dekripsinya.

3. Ciphertext diambil dari contoh pertama hasil dari sandi Vigenere.
   Rumus dekripsi : D(C)=P, P=C-K mod 26
   a. Dekripsi dengan sandi Vigenere
      Cipher Text : EQWY BJZKKDJMS
      Key : PERMATA
      Plaintext : PMFM BQZVGMXMZ

Tabel 8 Dekripsi Plainteks Vigenere pada Contoh 1

Plainteks	E	Q	W	Y		B	J	Z	K	K	D	J	M	S
Posis abjad	4	16	22	24		1	9	25	10	10	3	9	12	18
Kunci (key)	P	E	R	M		A	T	A	P	E	R	M	A	T
Posisi abjad	15	4	17	12		0	19	0	15	4	17	12	0	19
	-11	12	5	12		1	-10	25	-5	6	-14	-3	12	-1
Cipherteks	P	M	F	M		B	Q	Z	V	G	M	X	M	Z

   b. Dekripsi dengan sandi Caesar
      Rumus dekripsi : D(C)=P, P=C-K mod 26
      Cipher Text : PMFM BQZVGMXMZ
      Key : 12

Plaintext : DATA PENJUALAN

Tabel 9 Dekripsi Plainteks Caesar pada Contoh 1

Plainteks	P	M	F	M		B	Q	Z	V	G	M	X	M	Z
Posisi abjad	15	12	5	12		1	16	25	21	6	12	23	12	25
Kunci (Key)	12	12	12	12		12	12	12	12	12	12	12	12	12
	3	0	-7	0		-11	4	13	9	-6	0	11	0	13
Cipherteks	D	A	T	A		P	E	N	J	U	A	L	A	N

4. Contoh dekripsi kedua
   a. Dekripsi dengan sandi Vigenere
      Cipher Text : KJODMZ MKY HQPOYQZN
      Key : ABCDE
      Plaintext : KIMAIZ LIV DQOMVMZM

Tabel 10 Dekripsi Plainteks Vigenere pada Contoh 2

Plainteks	K	J	O	D	M	Z		M	K	Y		H	Q	P	O	Y	Q	Z	N
Posisi abjad	10	9	14	3	12	25		12	10	24		7	16	15	14	24	16	25	13
Kunci (Key)	A	B	C	D	E	A		B	C	D		E	A	B	C	D	E	A	B
Posisi abjad	0	1	2	3	4	0		1	2	3		4	0	1	2	3	4	0	1
	10	8	12	0	8	25		11	8	21		3	16	14	12	21	12	25	12
Ciphertek s	K	I	M	A	I	Z		L	I	V		D	Q	O	M	V	M	Z	M

   b. Dekripsi dengan sandi Caesar
      AAAAA
      Cipher Text : KIMAIZ LIV DQOMVMZM
      Key : ABCDE
      Plaintext : CAESAR DAN VIGENERE

Tabel 11 Dekripsi Plainteks Caesar pada Contoh 2

Plainteks	K	I	M	A	I	Z		L	I	V		D	Q	O	M	V	M	Z	M

Posisi abjad	10	8	12	0	8	25		11	8	21		3	16	14	12	21	12	25	12
Kunci (Key)	8	8	8	8	8	8		8	8	8		8	8	8	8	8	8	8	8
	2	0	4	-8	0	17		3	0	13		-5	8	6	4	13	4	17	4
Ciphertek s	C	A	E	S	A	R		D	A	N		V	I	G	E	N	E	R	E

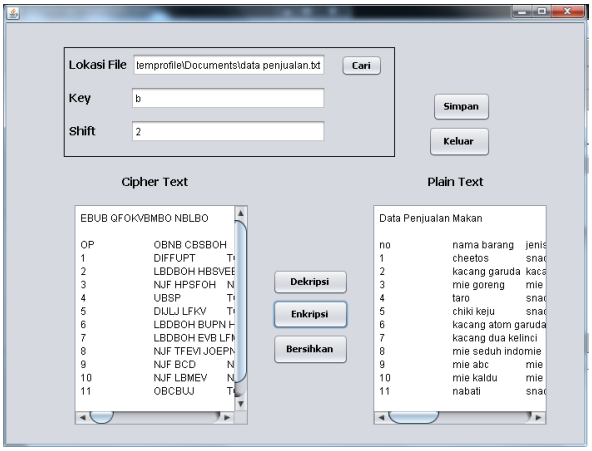
Pesan yang telah di dekripsi dari kombinasi sandi vigenere dan Caesar sudah dapat di baca dan di pahami oleh penerima pesan. Kerahasiaan dan keaslian pesan terjaga sampai kepada penerima.

3.4 Tampilan Aplikasi

Setelah diketahui bagaimana proses Enkripsi dengan mengkombinasikan kedua algoritma yaitu algoritma Caesar dan algoritma Vigenere secara tertulis, maka perlu ditransformasikan kedalam bahasa pemprograman agar pemanfaatannya menjadi lebih mudah. Berikut adalah Tampilan aplikasi dari algoritma Caesar dan Algoritma Vigenere.

Gambar 2 Tampilan Aplikasi Awal

Pada gambar 2 merupakan tampilan form menu pada form ini mengambarkan fitur-fitur dan tombol-tombol yang ada, di form ini pengguna memilih data yang akan dienkripsi atau dekripsi dan juga memasukkan kunci.



Gambar 3 Tampilan Akhir

Pada gambar 3 merupakan hasil setelah file dibuka dan telah mengisi kunci dan telah selesai enkripsi.

4. KESIMPULAN

Dari hasil analisis dan perancangan perangkat lunak kriptografi pada suatu data penjualan dengan menggunakan vigenere cipher dan caesar cipher yang telah di lakukan dapat diambil kesimpulan sebagai berikut yaitu file yang di enkripsi dan dekripsi hanya bisa .txt. Perangkat lunak telah dilakukan pengujian dan cukup baik dalam pengenkripsi dan mendekripsi data dengan baik. Efisiensi waktu yang ditempuh dalam proses enkripsi dan dekripsi relatif cepat dalam mengenkripsi dan dekripsi 2000 karakter. Penyimpanan hasil enkripsi dan dekripsi berjalan dengan cukup baik. Program aplikasi yang dirancang dapat membantu seseorang yang ingin mengenkripsi dan dekripsi yang tidak ingin datanya dipublikasi atau diketahui siapapun selain penerima.

5. SARAN

Penulis menyadari bahwa perangkat lunak kriptografi yang dibuat ini belum sepenuhnya sempurna. Penulis berharap agar pembaca dan programmer yang lebih handal dapat mengembangkan dan menyenmpurnakan kekurangan dari perangkat lunak ini. Beberapa saran yang dapat diberikan untuk penelitian lebih lanjut ialah penelitian selanjutnya dapat mengembangkan dan memodifikasi metode caesar cipher dan vigenere cipher guna untuk menjaga kerahasiaan data kemudian perangkat lunak ini dapat dikembangkann dengan menambah format file yang lebih banyak seperti doc, docx dan xlsx dan terakhir disarankan untuk merancang tampilan (interface) kembali agar aplikasi lebih menarik.

UCAPAN TERIMA KASIH

Dalam penyusunan jurnal ini penulis telah mendapatkan bantuan, nasihat, bimbingan dan pengarahan serta dorongan dari berbagai pihak. Oleh karena itu, dengan segala kerendahan hati dan penuh rasa hormat penulis ingin menyampaikan terima kasih yang tak terhingga kepada Bapak Sandy Kosasi, SE., MM., M.Kom., selaku Ketua Sekolah Tinggi Manajemen Informatika dan Komputer Pontianak waktunya untuk memberikan petunjuk, bimbingan dan pengarahan. Ibu Susanti MK., S.Kom., M.Kom., selaku Pembantu Ketua I Sekolah Tinggi Manajemen Informatika dan Komputer Pontianak dan selaku Dosen Pembimbing Akademik yang memberikan masukkan. Bapak David, S.Kom., M.Cs., M.Kom., Selaku Pembantu Ketua III STMIK Pontianak. Bapak Gat, S.Kom., M.Kom., selaku Ketua Jurusan Teknik Informatika

Sekolah Tinggi Manajemen Informatika dan Komputer Pontianak. Orang tua dan keluarga, yang telah memberikan dukungan baik moral maupun materil kepada penulis untuk selalu berusaha mencapai hasil yang baik. Dan orang-orang disekitar saya yang telah memberikan dukungan yang memberikan masukkan dalam penulisan jurnal ini.

DAFTAR PUSTAKA

[1] Rachmawati, Dian dan Candra, Ade., 2015, *Implementasi Kombinasi Caesar dan Affine Cipher untuk keamanan Data Teks,* Jurnal Edukasi dan Penelitian Informatika (JEPIN), Nomor 2, Volume(1):60-63.

[2] Arjana, Putu H, dkk, 2012, *Implentasi Enkripsi Data dengan Algoritma Vigenere Cipher*, Seminar Nasional Teknologi dan Komunikasi (SENTIKA). Maret.

[3] Eddy dan Mohammad Reza Pahlevi, 2014, *Pembelajaran Enkripsi Metode Word Auto Key Encryption*, Sisfotenika, Vol. 4, No. 1, Januari., ISSN : 2087-7897.

[4] Wahyuni. Ana, 2010, *Aplikasi Kriptosistem dengan Algoritma Mc Elliece*, Majalah Ilmiah Informatika, Vol. 1, 1 Januari.

[5] Munir Rinaldi, 2006, Kriptografi, Penerbit Informatika, Bandung.

[6] Bishop, David, *Introduction to Cryptography with Java Applets*. Grinnell College. 2003.

[7] McLeod dan Schell, 2010, *Sistem Informasi Manajemen*. Jakarta: Indeks