PEMBUATAN PERANGKAT LUNAK MEDIA PEMBELAJARAN KRIPTOGRAFI KLASIK

Abd. Hallim [1], Isbat Uzzin Nadhori [2], Setiawardhana[2]
Mahasiswa Jurusan Teknologi Informasi [1] , Dosen Pembimbing [2]
Politeknik Elektronika Negeri Surabaya
Institut Teknologi Sepuluh Nopember
Kampus PENS-ITS Keputih Sukolilo Surabaya 60111
Telp (+62)31-5947280, 5946114, Fax. (+62)31-5946114
Email : halim_cracker@yahoo.com

Abstrak

Perkembangan teknologi telah menjadikannya salah satu media utama pertukaran informasi. Tidak semua informasi bersifat terbuka untuk umum. Karena internet merupakan jaringan komputer yang bersifat publik, maka diperlukan suatu usaha untuk menjamin keamanan informasi tersebut. Di satu sisi, telah banyak usaha-usaha untuk menjamin keamanan suatu informasi. Di sisi lain, tetap saja ada pihak-pihak dengan maksud tertentu yang berusaha untuk menembus sistem keamanan tersebut. Oleh karena itu, peranan kriptografi sangat dibutuhkan untuk menjaga keamanan informasi tersebut. Dikarenakan peranan kriptografi yang penting, oleh karena itu di dalam dunia pendidikan diperlukan suatu aplikasi untuk mempelajari kriptografi secara visual dan interaktif. Di beberapa tempat kuliah dan belajar sering sekali ditemukan pembelajaran kriptografi yang masih menggunakan teori-teori tanpa langsung melihat apa yag terjadi di dalam proses kriptografi tersebut. Oleh karena itu, pada proyek akhir ini akan dibuat suatu perangkat lunak pembelajaran kriptografi klasik yang dapat mempermudah dalam mempelajari proses dari beberapa kriptografi klasik seperti caesar cipher, vigenere, autokey, reverse, column cipher, zig-zag cipher, segitiga cipher, super enkripsi dan enigma machine dengan visualisasi yang lebih detail dan proses dalam perubahan data secara bertahap.

***Kata Kunci** : Kriptografi Klasik , Caesar cipher, Vigenere cipher, Autokey cipher, Reverse cipher, Column cipher, Zig-zag cipher, Segitiga cipher, Super enkripsi dan Enigma machine*

Abstract

The development of the technology has making it as one of the main media of information changing. Not all the information is open for public. Because internet is a public-computer-network, then it needed an effort to keep the security of that information. On one side, there are so many efforts to keep the security of one information. On the other side, there are still some mean people that struggle to breach one security system. Because of that, the role of cryptography is needed to protect the information's safety. Because of cryptography role that is needed, therefore in the education the application for learning the cryptography visually and interactively is needed. In some college and education places, learning cryptography using theories without directly see the process of the cryptography itself always occurs. Based on that, on this final project an application for learning classical cryptography that could make easier learning process of few classical cryptography like a Caesar cipher, Vigenere cipher, Autokey cipher, Reverse cipher, Column cipher, Zig-zag cipher, Triangle cipher, Super encryptioni dan Enigma machine with more visual detail and process in data changing phasely.

***Key Word** : Classical cryptography, Caesar cipher, Vigenere cipher, Autokey cipher, Reverse cipher, Column cipher, Zig-zag cipher, Triangle cipher, Super encryptioni dan Enigma machine*

I. PENDAHULUAN

Keamanan data yang harus kita pertahankan semakin hari haruslah semakin secure dan data (informasi) yang bersifat rahasia harus diamankan terlebih dahulu dengan menggunakan metoda kriptografi sebelum dikirimkan untuk mencegah agar data (informasi) diketahui oleh orang lain yang tidak berkepentingan. Metoda yang digunakan untuk mengamankan data ada bermacam – macam. Masing – masing metoda memiliki kelebihan dan kekurangan tetapi sebelum mempelajari kriptografi yang lebih mendalam sebaiknya mempelajari kriptografi dasar yaitu kriptografi klasik.

Dalam dunia perkuliahan sering kita temui pembelajaran kriptografi hanya membahas teori mengenai kriptografi, kita hanya membahas tanpa lebih dalam lagi mengenai kriptografi dan kita tidak bisa mengetahui secara detail dari proses kriptografi yang sedang terjadi. Oleh karena itu, pembelajaran mengenai kriptografi kurang diminati.

Pada tugas akhir ini penulis mencoba membuat suatu Perangkat Lunak Media Pembelajaran Kriptografi Klasik untuk membantu dalam pembelajaran mengenai beberapa kriptografi klasik.

II. DASAR TEORI

2.1 Kriptografi

Kriptografi, secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita [bruce Schneier - *Applied Cryptography*] [4]. Dalam kriptografi, pesan atau informasi yang dapat dibaca disebut sebagai plaintext atau clear text. Proses yang dilakukan untuk mengubah plaintext ke dalam ciphertext disebut enkripsi. Pesan yang tidak dapat terbaca tersebut disebut ciphertext. Proses yang merupakan kebalikan dari enkripsi disebut sebagai dekripsi. Proses ekripsi dapat digunakan untuk membuat ciphertext kembali menjadi plaintext.

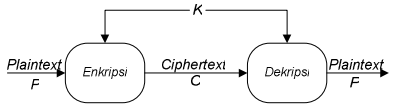
Ahli di bidang kriptografi disebut sebagai cryptographer. Cryptanalyst merupakan orang yang melakukan cryptanalysis, yaitu seni dan ilmu untuk meecahkan ciphertext menjadi plaintext tanpa melalui cara yang seharusnya (dekripsi) [1].

Terdapat dua jenis algoritma kriptografi berdasar jenis kuncinya [1] :

1. Algoritma Simetri (konvensional)
2. Algoritma Asimetri (kunci public)

Algoritma Simetri

Algoritma simetri disebut juga sebagai algoritma konvensional adalah algoritma yang menggunakan kunci enkripsi yang sama dengan kunci dekripsinya. Yang termasuk algoritma kunci simetri adalah OTP, DES, RC2, RC4, RC5, RC6, IDEA, Twofish, Magenta, FEAL, SAFER, LOKI, CAST, Rijndael (AES), Blowfish, GOST, A5, Kasumi dan lain-lain.



Gambar 1. Kriptografi konvensional

Orang sering menggunakan notasi matematika untuk mempermudah penulisan dan analisis, sehingga kriptografi modern selalu berhubungan dengan matematika. Dengan pesan asal P dan kode rahasia C yang diperoleh dari enkripsi dengan kunci K, kita dapat dituliskan sebagai berikut :

$$\mathbf{C = E_k\,(P)} \qquad \mathbf{(1)}$$

Pada proses dekripsi, dilakukan operasi sebaliknya, dan dapat dituliskan sebagai berikut :

$$\mathbf{P = D_k\,(P)} \qquad \mathbf{(2)}$$

Algoritma Asimetri

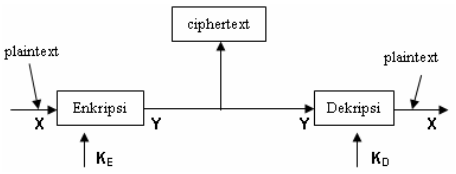
Algoritma asimetrik (juga disebut algoritma kunci public) didesain sedemikian sehingga kunci yang digunakan untuk enkripsi berbeda dari kunci yang digunakan untuk dekripsi.Enkripsi dengan kunci public ***Ke*** dinyatakan sebagai berikut :

$$\mathbf{E_{Ke}\,(M) = C} \qquad \mathbf{(1)}$$

$$\mathbf{D_{Kd}\,(C) = M} \qquad \mathbf{(2)}$$

2.2 Metoda Kriptografi Klasik

Algoritma Kriptografi dari setiap kriptografi klasik selalu terdiri dari dua bagian yaitu enkripsi dan dekripsi. Secara sederhana proses kriptografi dapat digambarkan sebagai berikut :



Gambar. 2.1. *Kriptografi Secara Umum*

Operasi enkripsi dan dekripsi dijelaskan secara umum sebagai berikut :

$$Y = E_{K_E}(X) \qquad \text{(enkripsi)} \quad (1)$$

$$X = D_{K_D}(Y) \qquad \text{(dekripsi)} \quad (2)$$

dimana:

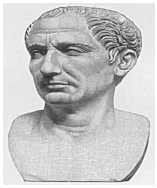
X = plaintext, Y = chipertext, K_E = key enkripsi, K_D = key dekripsi

Ada dua cara yang paling dasar pada kriptografi klasik. yaitu adalah Transposisi dan Subsitusi :

- Transposisi adalah mengubah susunan huruf pada plaintext sehingga urutannya berubah. Contoh yang paling sederhana adalah mengubah suatu kalimat dengan menuliskan setiap kata secara terbalik.
- Substitusi yaitu setiap huruf pada plaintext akan digantikan dengan huruf lain berdasarkan suatu cara atau rumus tertentu

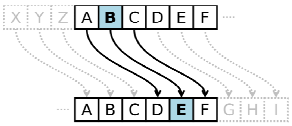
2.2 Caesar Cipher

Algoritma kriptografi yang mula-mula digunakan oleh kaisar Romawi, Julius Caesar (sehingga dinamakan juga caesar chiper), untuk menyandikan pesan yang dikirim kepada para gubernurnya.



Gambar. 2.2.1 *Julius Cesar*

- Caranya adalah dengan mengganti (mensubstitusi) setiap karakter dengan karakter lain dalam susunan abjad (alfabet).
- Misalnya, tiap huruf disubstitusi dengan huruf ketiga berikutnya dari susunan abjad. Dalam hal ini kuncinya adalah jumlah pergeseran huruf (yaitu k = 3).



Gambar. 2.2.2 *Pergeseran Huruf*

- Karena hanya ada 26 huruf abjad, maka pergeseran huruf yang mungkin dilakukan adalah dari 0 sampai 25. Secara umum, untuk pergeseran huruf sejauh k (dalam hal ini k adalah kunci enkripsi dan deksripsi), fungsi enkripsi dan dekripsi adalah
- ci = E(pi) = (pi + k) mod 26 (1)
- pi = D(ci) = (ci – k) mod 26 (2)

Kunci	A	B	C	D	E	F	G	H	I
Pergeseran k	0	1	2	3	4	5	6	7	8
Kunci	J	K	L	M	N	O	P	Q	R
Pergeseran k	9	10	11	12	13	14	15	16	17
Kunci	S	T	U	V	W	X	Y	Z	
Pergeseran k	18	19	20	21	22	23	24	25	

Tabel. 2.2 *Pergeseran Huruf Pada Kriptografi Caesar*

2.3 Vigenere Cipher

Ditemukan oleh diplomat (sekaligus seorang kriptologis) Perancis, Blaise de Vigènere pada abad 16.

Gambar. 2.3.1 *Blaise de Vigènere*

Pada kriptografi caesar pergeseran akan sama pada seluruh pesan, Jika kunci yang digunakan adalah huruf E, maka setiap huruf pada pesan akan bergeser 4 huruf. Begitu juga bila digunakan kunci-kunci lainnya, pada kriptografi Vigenere, plaintext akan dienkripsi dengan pergeseran huruf seperti pada kriptografi Caesar tetapi setiap huruf di dalam plaintext akan mengalami pergeseran yang berbeda.

Kunci pada kriptografi Vigenere adalah sebuah kata bukan sebuah huruf. Kata kunci ini akan dibuat berulang sepanjang plaintext, sehingga jumlah huruf pada kunci akan sama dengan jumlah huruf pada plaintext. Pergeseran setiap huruf pada plaintext akan ditentukan oleh huruf pada kunci yang mempunyai posisi yang sama dengan huruf pada plaintext. fungsi enkripsi dan dekripsi adalah

- ci = E(pi) = (pi + k) mod 26) (1)
- pi = D(ci) = (ci – k) mod 26) (2)

Cara lain untuk melakukan enkripsi dan dekripsi adalah dengan menggunakan Vigenere Square sebagai berikut :

	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. 2.3.2 *Vigenere Square*

2.4 Autokey Cipher

Kriptografi Autokey adalah pengembangan dari kriprografi Caesar dan Vigenere. Cara melakukan enkripsi sama dengan kedua kriptografi sebelumnya. Pada kriptografi Autokey juga digunakan sebuah kata sebagai kunci.

Kunci ini kemudian diikuti dengan plaintext sehingga membentuk huruf-huruf yang sama panjang dengan plaintext. Urutan huruf-huruf ini yang akan digunakan sebagai kunci pada saat enkripsi. Rumus yang berlaku untuk kriptografi Autokey sama dengan untuk Caesar dan Vigenere dan bisa menggunakan vigenere square.

2.5 Reverse Cipher

Ini adalah contoh kriptografi klasik yang menggunakan substitusi yaitu mengganti satu huruf dengan huruf lain. Ini contoh yang paling sederhana dari substitusi yaitu mengubah suatu kalimat dengan menuliskan setiap kata secara terbalik

2.6 Column Cipher

Pada kriptografi kolom (column cipher), plaintext disusun dalam kelompok huruf yang terdiri dari beberapa huruf. Kemudian huruf-huruf dalam kelompok ini dituliskan kembali kolom per kolom, dengan urutan kolom yang bisa berubah-ubah.

2.7 Zig-Zag Cipher

Pada kriptografi kolom zig-zag, plaintext disusun dalam kelompok huruf yang terdiri dari beberapa huruf. Kemudian huruf-huruf dalam urutan kolom yang dimasukkan secara pola zig-zag

2.8 Segitiga Cipher

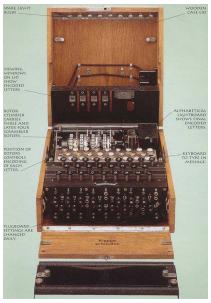
Pada kriptografi kolom Triangle, plaintext disusun dalam kelompok huruf yang terdiri dari beberapa huruf. Kemudian huruf-huruf dalam urutan kolom yang dimasukkan secara pola segitiga

2.9 Super Enkripsi

Kombinasi Antara Cipher Substitusi (Caesar Cipher) dan Cipher Tranposisi (Column Cipher) Sehingga Memperoleh Cipher yang lebih kuat (Super) dari pada Satu Cipher saja.

2.10 Enigma Machine

Enigma Machine adalah mesin yang digunakan Jerman selama Perang Dunia II untuk mengenkripsi/dekripsi pesan-pesan militer. Enigma menggunakan sistem *rotor* (mesin berbentuk roda yang berputar) untuk membentuk huruf cipherteks yang berubah-ubah. Setelah setiap huruf dienkripsi, *rotor* kembali berputar untuk membentuk huruf cipherteks baru untuk huruf plainteks berikutnya.

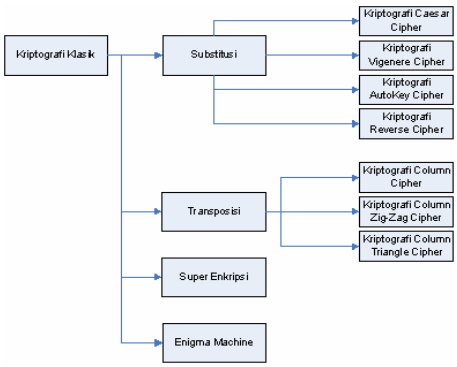


Gambar. 2.10 *Enigma Machine*

III. PERANCANGAN DAN PEMBUATAN APLIKASI

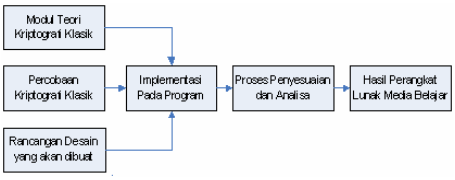
3.1 PERANCANGAN APLIKASI

Diagram Struktur perangkat lunak media pembelajaran kriptografi klasik:



Gambar 3.1. Bagan Struktur Media Pembelajaran Kriptografi Klasik

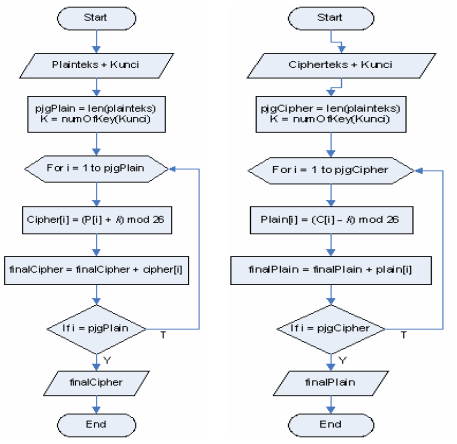
Tahapan–tahapan dalam proses perancangan media pembelajaran :



Gambar 3.2 Bagan Proses Pembuatan

Caesar Cipher

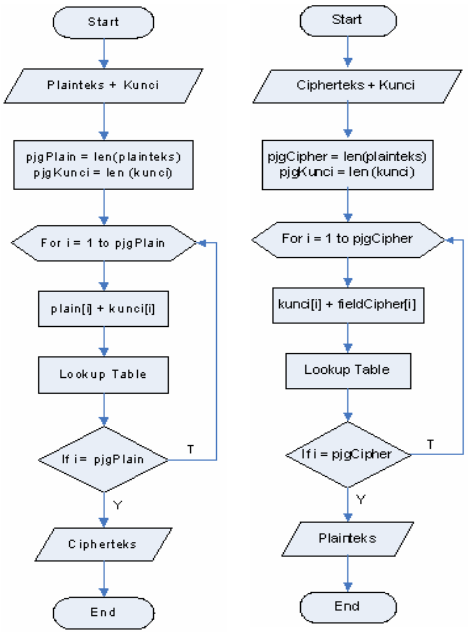
Berikut adalah Flowchart dari proses enkripsi dan dekripsi caesar cipher :



Gambar 3.3 Flowchart Enkripsi dan Dekripsi Caesar Cipher

Vigenere Cipher

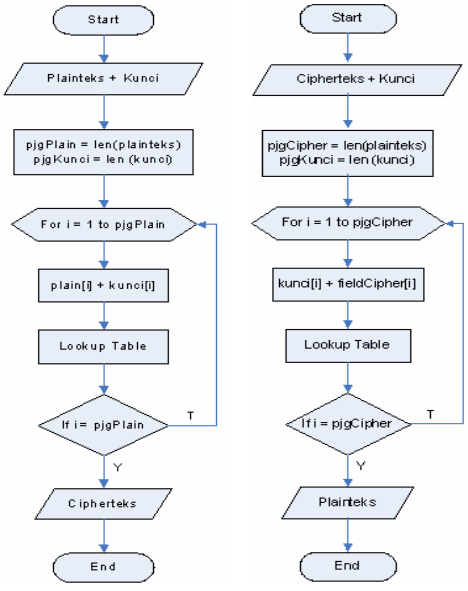
Berikut adalah Flowchart dari proses enkripsi dan dekripsi Vigenere cipher :



Gambar 3.4 Flowchart Enkripsi dan Dekripsi Vigenere Cipher

Autokey Cipher

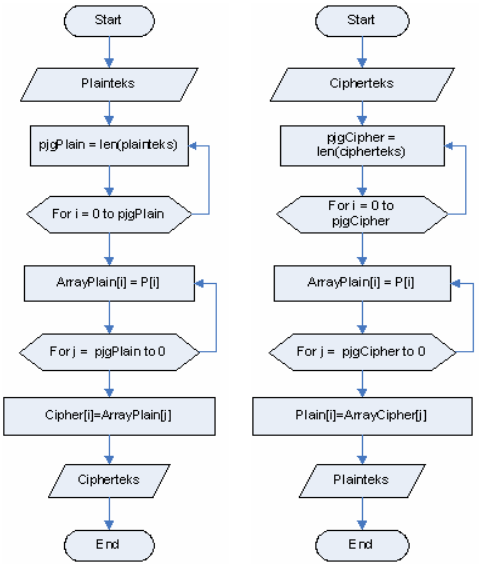
Berikut adalah Flowchart dari proses enkripsi dan dekripsi autokey cipher :



Gambar 3.5 Flowchart Enkripsi dan Dekripsi Autokey Cipher

Reverse Cipher

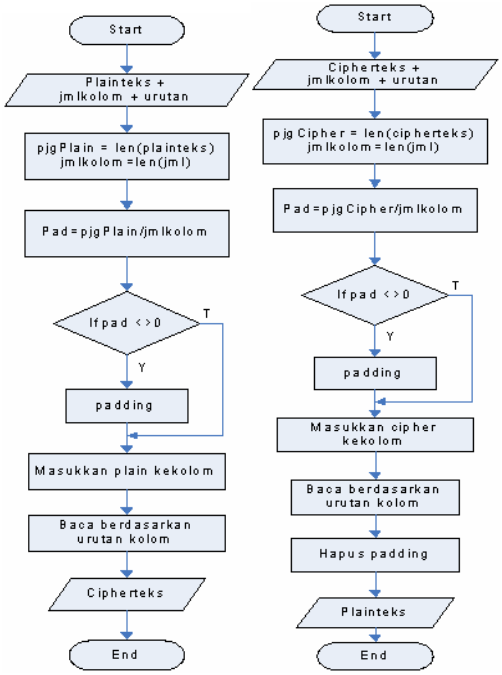
Berikut adalah Flowchart dari proses enkripsi dan dekripsi reverse cipher :



Gambar 3.6 Flowchart Enkripsi dan Dekripsi Reverse Cipher

Column Cipher

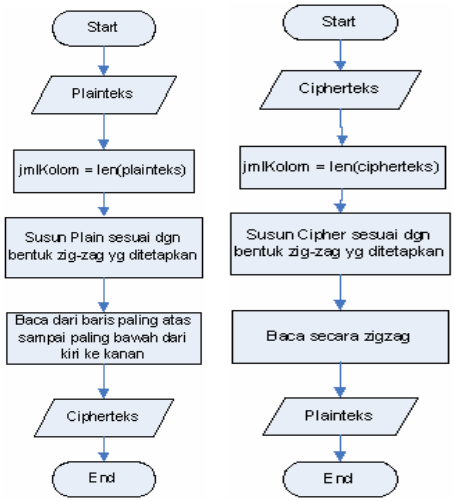
Berikut adalah Flowchart dari proses enkripsi dan dekripsi column cipher :



Gambar 3.7 Flowchart Enkripsi dan Dekripsi Reverse Cipher

Zig-Zag Cipher

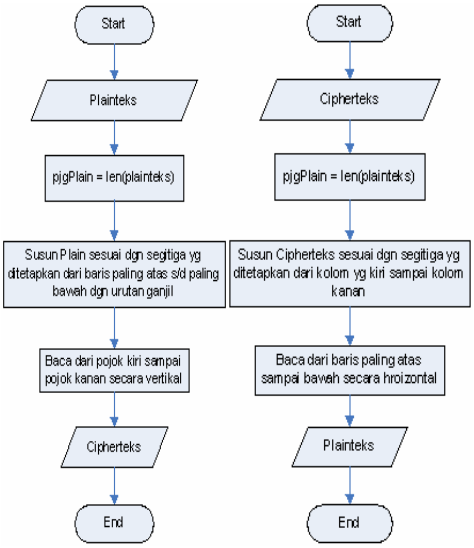
Berikut adalah Flowchart dari proses enkripsi dan dekripsi zig-zag cipher :



Gambar 3.8 Flowchart Enkripsi dan Dekripsi Zig-Zag Cipher

Segitiga Cipher

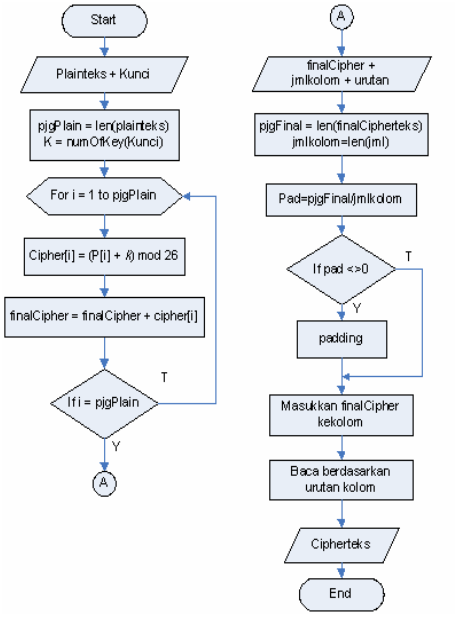
Berikut adalah Flowchart dari proses enkripsi dan dekripsi segitiga cipher :



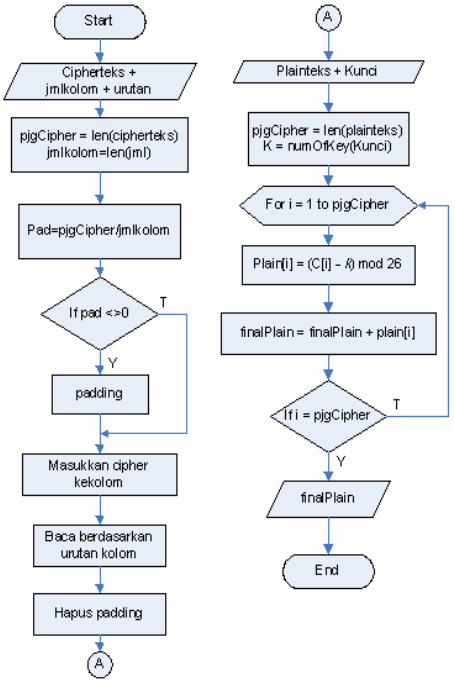
Gambar 3.9 Flowchart Enkripsi dan Dekripsi Segitiga Cipher

Super Enkripsi

Berikut adalah Flowchart dari proses enkripsi dan dekripsi super enkripsi :



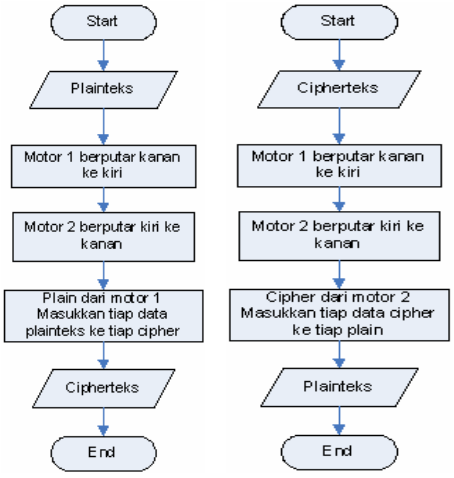
Gambar 3.10 Flowchart Enkripsi Super Enkripsi



Gambar 3.11 Flowchart Dekripsi Super Enkripsi

Enigma Machine

Berikut adalah Flowchart dari proses enkripsi dan dekripsi Enigma Machine :



Gambar 3.12 Flowchart Enkripsi dan Dekripsi Enigma Machine

Adapun form inti dalam aplikasi pembelajaran ini adalah form visualisasi beberapa metode kriptografi klasik seperti berikut :

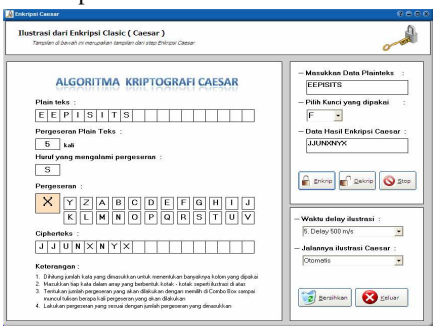
Form Utama

Di dalam aplikasi diperlukan menu agar semua fungsi dari aplikasi tersebut dapat diakses dengan cepat oleh pengguna

Gambar 4. Tampilan Form Utama

Form Caesar Cipher

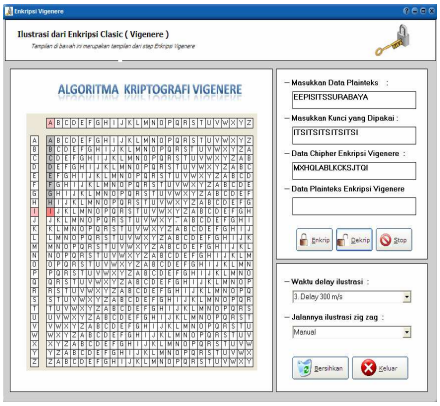
Berikut ini desain tampilan dari form caesar cipher :



Gambar 5. Tampilan Form Caesar Cipher

Form Vigenere Cipher

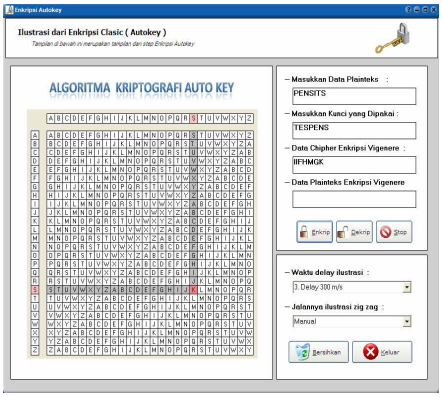
Berikut ini desain tampilan dari form vigenere cipher :



Gambar 6. Tampilan Form Vigenere Cipher

Form Autokey Cipher

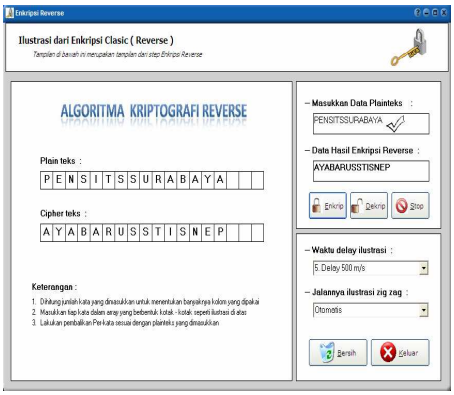
Berikut ini desain tampilan dari form autokey cipher :



Gambar 7. Tampilan Form Autokey Cipher

Form Reverse Cipher

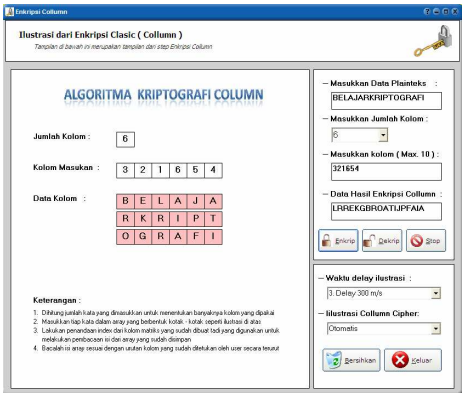
Berikut ini desain tampilan dari form reverse cipher :



Gambar 8. Tampilan Form Reverse Cipher

Form Column Cipher

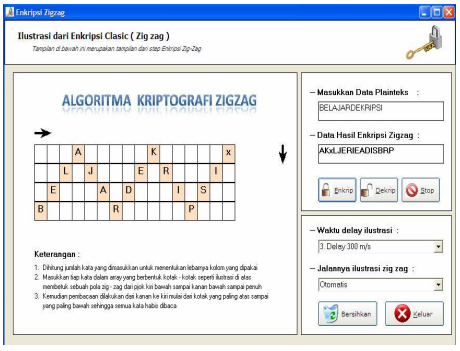
Berikut ini desain tampilan dari form column cipher :



Gambar 9. Tampilan Form Autokey Cipher

Form Zig-Zag Cipher

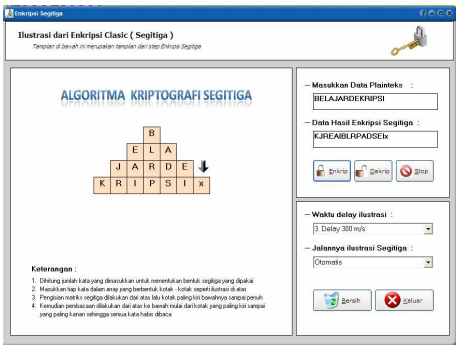
Berikut ini desain tampilan dari form zig-zag cipher :



Gambar 10. Tampilan Form Zig-Zag Cipher

Form Segitiga Cipher

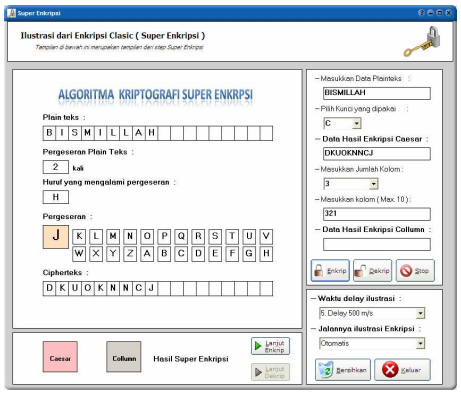
Berikut ini desain tampilan dari form segitiga cipher :



Gambar 11. Tampilan Form Segitiga Cipher

Form Super Enkripsi

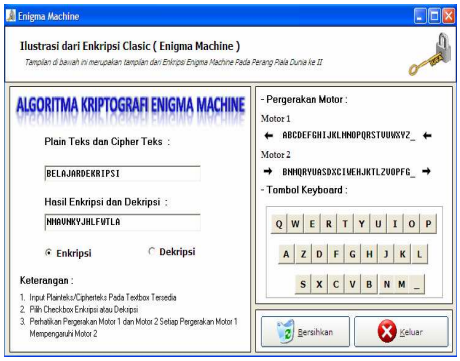
Berikut ini desain tampilan dari super enkripsi :



Gambar 12. Tampilan Form Super Enkripsi

Form Enigma Machine

Berikut ini desain tampilan dari form Enigma Machine :



Gambar 13. Tampilan Form Enigma Machine

IV. ANALISA

Pada proyek akhir ini untuk mengetahui berhasil atau tidaknya aplikasi yang telah dibuat ditentukan dari kemampuan aplikasi untuk melakukan proses visualisasi step by step penampilan dari keseluruhan proses kriptografi.

Adapun analisa yang didapatkan penulis setelah melakukan semua pengujian yaitu:

1. Aplikasi akan memulai proses enkripsi dan dekripsi dengan cara memasukkan plainteks, cipherteks dan memilih kunci sesuai dengan metode kriptografi klasik yang ingin diproses atau dipilih.
2. Setiap metode kriptogarfi klasik mempunyai cara yang berbeda-beda untuk proses enkripsinya dan dekripsinya.
3. Pada Metode Caesar Cipher output dari plainteks ke cipherteks atau sebaliknya dari cipherteks ke plainteks tergantung dari kunci yang digunakan berupa satu huruf yang menyatakan pergeserannya tetapi kunci berulang-ulang dengan huruf tersebut sampai dengan panjangnya plainteks atau cipherteks.
4. Pada Metode Vigenere Cipher output dari plainteks ke cipherteks atau sebaliknya dari cipherteks ke plainteks tergantung dari kunci yang digunakan berupa kata atau kalimat yang menyatakan pergeserannya tetapi jika kunci panjangnya tidak sama dengan plain teks maka kunci akan ditambah dengan kunci itu lagi secara berulang sesuai panjangnya plainteks yang digunakan.
5. Pada Metode Autokey Cipher output dari plainteks ke cipherteks atau sebaliknya dari cipherteks ke plainteks tergantung dari kunci yang digunakan berupa kata atau kalimat yang menyatakan pergeserannya tetapi jika kunci panjangnya tidak sama dengan plain teks maka kunci akan ditambah dengan plain teks sesuai panjangnya plainteks yang digunakan.
6. Pada Metode Reverse Cipher output dari plainteks ke cipherteks atau sebaliknya dari cipherteks ke plainteks

tergantung dari plainteks atau cipherteks yang digunakan sehingga setiap huruf atau kata dibaca secara terbalik.

7. Pada Metode Column Cipher output dari plainteks ke cipherteks atau sebaliknya dari cipherteks ke plainteks tergantung dari jumlah kolom dan urutan kolom yang digunakan, proses pembacaan plain teks dari baris yang pertama pertama ke baris berikutnya sampai baris terakhir sedangkan proses pembacaan cipher teks dari urutan yang paling kecil ke urutan paling besar dari atas ke bawah.
8. Pada Metode Zig-Zag Cipher output dari plainteks ke cipherteks atau sebaliknya dari cipherteks ke plainteks tergantung dari data plainteks/cipherteks karena menentukan jumlah kolom yang digunakan dan dimasukkan secara zig-zag, proses pembacaan plain teks dilakukan dari kolom pertama hingga kolom terakhir dengan ziz-zag dari bawah ke atas dengan urutan kolom terurut sehingga semua data terbaca. Sedangkan proses pembacaan cipher teks dilakukan dari kanan kekiri mulai baris yang paling atas sampai yang paling bawah sehingga semua data terbaca.
9. Pada Metode Segitiga Cipher output dari plainteks ke cipherteks atau sebaliknya dari cipherteks ke plainteks tergantung dari data plainteks/cipherteks karena menentukan bentuk segitiga yang digunakan, proses pembacaan plainteks teks dilakukan dari baris paling atas ke ke baris paling bawah secara horizontal kiri ke kanan sehingga semua data terbaca sedangkan proses pembacaan cipher teks dilakukan dari kiri ke kanan secara vertikal dari atas ke bawah sehingga semua data terbaca.
10. Pada Metode Super Enkripsi output dari plainteks ke cipherteks atau sebaliknya dari cipherteks ke plainteks tergantung dari kunci, jumlah kolom dan urutan kolom.
11. Pada Metode Enigma Machine output dari plainteks ke cipherteks atau sebaliknya tergantung dari pergerakan motor yang digunakan dan sudah di set.

V. PENUTUP

5.1 KESIMPULAN

Berdasarkan studi dan penelitian yang dilakukan pada bab - bab sebelumnya,maka dapat disimpulkan beberapa hal antara lain:

1. Perangkat lunak pembelajaran ini dapat menampilkan langkah-langkah penyelesaian algoritma untuk proses enkripsi dan dekripsi secara tahap demi tahap sehingga mempermudah pemahaman.
2. Perangkat lunak pembelajaran ini menyediakan fasilitas pengaturan kecepatan visualisasi proses.
3. Perangkat lunak pembelajaran ini menyediakan teori-teori dasar mengenai metode kriptografi klasik, caesar cipher, vigenere cipher, autokey cipher, reverse cipher, column cipher, zig-zag cipher, segitiga cipher, super enkripsi dan enigma machine.

5.1 SARAN

Beberapa saran yang dapat dipertimbangkan untuk pengembangan selanjutnya.

1. Perangkat lunak dapat dikembangkan agar dapat digabungkan dengan pembelajaran untuk metode kriptografi yang lain.
2. Perangkat lunak dapat ditambahkan fasilitas *multimedia* agar lebih menarik.

DAFTAR PUSTAKA

[1] Kurniawan, Yusuf, "*Kroptografi keamanan internet dan jaringan komnunikasi*", Informatika, 2004.

[2] Munir, Rinaldi. 2006. Diktat Kuliah IF5054 Kriptografi. Program Studi Teknik Informatika - Institut Teknologi Bandung.

[3] Stallings Wiliam, Cryptography and Network Security, Prentice Hall, 2000

[4] Uzzin, Isbat. 2008. Diktat Kuliah Security Jaringan Introduction Kriptografi. Jurusan Teknik Informatika – Politeknik Elektronika Negeri Surabaya- ITS.

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

[6] Ariyus, Dony. 2008. "Pengantar Ilmu Kriptografi", Penerbit Andi, Jakarta