Studi dan Analisis Keamanan serta Pemecahan Pesan pada Implementasi Enkripsi Berlapis Menggunakan Kombinasi Algoritma Kriptografi Klasik pada Dokumen Teks dengan Modifikasi Kunci

Fitriana Passa 13508036
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
if18036@students.if.itb.ac.id

***Abstrak* — Makalah ini membahas tentang studi dan analisis implementasi enkripsi berlapis dengan menggunakan kombinasi algoritma-algoritma kriptografi klasik yang telah di pelajari di kuliah. Algoritma kriptografi klasik menggunakan mode karakter dalam operasinya. Algoritma yang digunakan dalam makalah ini meliputi vigenere cipher, caesar cipher, substitusi cipher, dan enigma cipher. Masing-masing cipher menggunakan teknik dasar yang sama dalam proses enkripsi, tetapi masing-masing cipher memiliki kelemahan dan keunggulannya masing-masing.**

Pada makalah ini juga dibahas mengenai desain dan implementasi masing-masing algoritma yang digunakan dalam enkripsi berlapis dan serta desain kunci yang digunakan untuk masing-masing algoritma.

Selain itu, di makalah ini juga dibahas mengenai analisis keamanan dan pemecahan pesan cipher teks yang dihasilkan dari kombinasi keempat algoritma yang digunakan.

***Index* vigenere cipher, caesar cipher, cipher subtitusi, enigma cipher, kriptografi klasik, enkripsi berlapis.**

I. PENDAHULUAN

Pada kehidupan sehari-hari, orang sering mengirimkan pesan dengan mengenkripsi pesan tersebut dengan tujuan untuk mencegah orang-orang yang tidak berkepentingan membaca pesan yang bersangkutan. Algoritma kriptografi klasik yang mudah diterapkan pada enkripsi pesan menyebabkan algoritma tersebut masih sering digunakan pada enkripsi pesan sederhana yang dikirimkan dari satu orang ke orang lain. Kenyataannya, pada kebanyakan algoritma kriptografi klasik, pemecahan kode pesan mudah dilakukan dengan deteksi pesan menggunakan pola-pola dan teknik tertentu berdasarkan setiap algoritma yang ada.

Setiap algoritma kriptografi klasik mempunyai kelebihan dan kekurangan masing-masing pada implementasi enkripsi pesan sederhana. Kombinasi algoritma kriptografi klasik memungkinkan penggabungan kelebihan dari setiap algoritma dan mengurangi kemungkinan dekripsi pesan dilakukan oleh pihak ketiga karena pola enkripsi yang dilakukan secara bertingkat pada pesan yang dikirimkan. Dengan pemilihan urutan kombinasi algoritma kriptografi klasik yang tepat, diharapkan pesan yang ada lebih sulit untuk dipecahkan.

II. DASAR TEORI

Algoritma kriptografi klasik

Algoritma kriptografi klasik berbasis karakter dalam operasinya. Secara umum, algoritma kriptografi klasik dibagi menjadi 2 :

a. Cipher substitusi

Cipher substitusi beroperasi dengan mensubstitusikan setiap karakter pada plain teks dengan karakter lain berdasarkan rumus tertentu. Terdapat dua jenis substitusi:

1) Polyalphabetic Substitution Cipher

Cipher substitusi jenis ini enkripsi terhadap suatu karakter / huruf yang sama dapat menghasilkan karakter yang berbeda sehingga lebih sulit untuk menemukan pola substitus yang digunakan. Salah satu contoh *polyalphabetic substitution* cipher adalah vigenere cipher.

2) Monoalphabetic Substitution Cipher

Monoaplhabetic substitution cipher membuat suatu karakter yang sama akan dienkripsi menjadi karakter yang sama pula. Salah satu jenis cipher substitusi monoalfabetik adalah caesar cipher.

b. Cipher transposisi

Cipher transposisi beroperasi dengan mengubah susunan huruf pada plain teks sehingga urutannya berubah. Nama lain dari metode ini adalah permutasi, karena transpose setiap karakter di dalam teks sama dengan mempermutasikan karakter-karakter tersebut. Contoh sederhana dari cipher transposisi adalah mengubah suatu kalimat dengan menuliskan setiap kata dengan urutan terbalik.

1. Caesar cipher

Metode ini dinamakan caesar cipher karena metode ini digunakan oleh Julius Caesar dalam berkomunikasi dengan para petinggi militer di Yunani ketika itu. Operasi dasar yang dilakukan pada caesar cipher adalah dengan menggeser setiap karakter plain teks sebanyak N tempat

ke kanan. Julius Caesar menggunakan N=3 dalam pengiriman pesan yang dilakukannya. Pemecahan pesan dilakukan dengan cara terbalik yaitu menggeser setiap karakter cipher teks sebanyak N tempat ke arah sebaliknya.

Plain : ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher : DEFGHIJKLMNOPQRSTUVWXYZABC

Contoh:

Plainteks : AWASI ASTERIX DAN TEMANNYA OBELIX
Cipherteks : DZDVL DVWHULA GDQ WHPDQQBA REHOLA

Proses enkripsi / dekripsi dapat dituliskan secara matematis sebagai berikut:

Enkripsi : $c_i = E(p_i) = (p_i + N) \bmod 26$
Dekripsi : $p_i = D(c_i) = (c_i - N) \bmod 26$

N adalah jumlah pergeseran huruf yang dilakukan.

Metode caesar cipher mudah dipecahkan dengan exhaustive search karena jumlah kunci yang dipakai sangat sedikit (26 kunci untuk mode enkripsi huruf saja).

2. Vigenere Cipher

Vigenere cipher menggunakan bujursangkar vigenere untuk melakukan enkripsi. Setiap baris di dalam bujursangkar menyatakan huruf-huruf cipherteks yang diperoleh dengan caesar cipher. Secara sederhana, metode enkripsi pada vigenere cipher adalah dengan menjumlahkan karakter ke-i dengan kunci ke-i, sehingga pada dasarnya setiap enkripsi huruf adalah Caesar Cipher.

Apabila kunci yang digunakan tidak sepanjang pesan, maka pemakaian kunci diulang setiap M karakter pesan dimana M adalah panjang kunci asli. Proses enkripsi / dekripsi dapat dituliskan secara matematis sebagai berikut:

Enkripsi : $c_i = E(p_i) = (p_i + k_{(length(m) \bmod length(k))}) \bmod 26$
Dekripsi : $p_i = D(c_i) = (c_i - k_{(length(m) \bmod length(k))}) \bmod 26$

k_i menyatakan kunci ke i dengan i merupakan indeks kunci yang diperoleh dari sisa panjang pesan(m) dibagi dengan panjang kunci(k) (untuk mengatasi permasalahan plain teks lebih panjang dari kunci).

Vigenere cipher dapat mencegah frekuensi huruf-huruf di dalam cipher teks mempunyai pola tertentu yang sama seperti pada cipher abjad tunggal. Salah satu cara memecahkan kunci pada cipher teks vigenere cipher adalah dengan metode kasiski.

3. Substitusi Cipher

Metode substitusi cipher beroperasi dengan cara mensubsitusikan / mengganti kemunculan suatu huruf dengan huruf yang lain. Pemetaan huruf dapat dilakukan secara random atau telah ditentukan sebelumnya. Biasanya, pemetaan huruf telah ditetapkan sebelumnya oleh pengirim pesan baik manual maupun menggunakan generator pemetaan huruf.

Pada metode ini, huruf yang sama akan dienkripsi menjadi huruf lain yang sama. Karena itu, metode ini mudah dipecahkan dengan analisis frekuensi terhadap kemunculan huruf-huruf yang ada dan dibandingkan dengan data acuan frekuensi huruf pada buku-buku teks.

4. Enigma Cipher

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. Enigma menggunakan 3 atau 4 buah *rotor* untuk melakukan substitusi. Setiap kali sebuah huruf selesai disubstitusi, *rotor* pertama bergeser satu huruf ke atas. Posisi awal keempat *rotor* dapat di-*set* dan posisi awal ini menyatakan kunci dari Enigma.

Secara umum, cara kerja enigma ketika sebuah huruf diketikkan ke papan ketik adalah sebagai berikut (menggunakan 3 *rotor*):

1. Huruf yang diketikkan masuk ke rotor paling kanan. Pada rotor ini dicari padanan posisi pada rotor kedua. Setelah itu masuk ke rotor kedua.
2. Pada rotor kedua, huruf hasil padanan dari rotor pertama dicari padanan posisi pada rotor kedua. Setelah itu masuk ke rotor ketiga.
3. Pada rotor ketiga, dicari padanan untuk ke reflektor mesin untuk dicari pasangan huruf masukan.
4. Hasil dari reflektor dikembalikan ke rotor ke-3, 2, 1, dan akhirnya menghasilkan huruf enkripsi.

Karena E(E(a)) = a, a adalah suatu huruf yang diproses dan E adalah proses enkripsi, maka proses enkripsi dan dekripsi dilakukan dengan cara yang sama.

III. PERANCANGAN ALGORITMA

3.1 ENKRIPSI

Pada enkripsi berlapis yang dibuat, urutan algoritma yang digunakan untuk melakukan enkripsi berlapis adalah:

1. Vigenere cipher
2. Caesar cipher
3. substitusi
4. enigma cipher

Rancangan algoritma menggunakan mode enkripsi 26 karakter untuk untuk mempermudah membandingan dan mengecek hasil enkripsi.

1. Vigenere cipher

   Enkripsi vigenere dilakukan seperti pada tugas besar 1 yaitu menambahkan plain teks ke-i dengan kunci ke-i. Kunci yang digunakan pada vigenere cipher merupakan modifikasi dari kunci masukan user. Kunci yang ada dibalik / swap sehingga karakter pertama menjadi karakter terakhir, dst.

Perulangan kunci dilakukan apabila panjang karakter pesan melebihi panjang kunci.

2. Caesar cipher

Enkripsi dilakukan dengan menggeser suatu karakter dengan bilangan pergeseran yang diperoleh dari generator bilangan penggeser. Bilangan penggeser diperoleh dengan menjumlahkan seluruh karakter pada kunci user dan membaginya dengan 26. Masukan dari proses enkripsi adalah cipher teks dari vigenere cipher.

3. Substitusi cipher

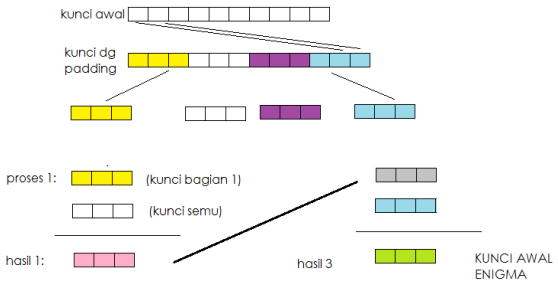
Masukan dari substitusi cipher adalah cipher teks hasil enkripsi dari caesar cipher. Pembangkitan substitusi dapat dilakukan dengan random dari seed kunci maupun ditetapkan oleh user. Karena huruf-huruf yang akan saya substitusi bukan merupakan plain teks asli tetapi cipher teks hasil operasi algoritma lain, saya menggunakan substitusi yang telah ditetapkan sejak awal sebagai berikut:

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

4. Enigma cipher

Perancangan enigma enkripsi dan dekripsi yang saya lakukan menggunakan 3 rotor dan posisi awal rotor merupakan penanda untuk melakukan enkripsi, maka dibutuhkan sebuah generator awal kunci enigma dari kunci asal. Generator ini bekerja dengan menggunakan bantuan enkripsi dari algoritma vigenere cipher. Misalkan kunci asal sepanjang 10 karakter, maka 10 karakter ini akan ditambahkan 2 karakter awal kunci sebagai padding sehingga kunci bentukan menjadi 12 karakter. 12 karakter dipecah menjadi 4 blok dan dilakukan vigenere cipher kunci 1 dengan kunci 2 sebagai kunci semunya, kemudian dilakukan kembali vigenere cipher kunci 2 dengan kunci 3 sebagai kunci semunya. Hasil dari proses tersebut adalah sebuah kunci sepanjang 3 karakter yang akan digunakan sebagai kunci enkripsi enigma.

Cara mendapatkan kunci asal adalah dengan mengenkripsi kunci masukan user dengan algoritma substitusi cipher dan caesar cipher.



3.2 DEKRIPSI

Secara umum, proses dekripsi dilakukan dengan membalik urutan proses enkripsi yang telah dilakukan pada plain teks. Langkah-langkah dekripsi :

a. Membangkitkan kunci awal enigma dari kunci masukan user yang telah dienkripsi dengan substitusi cipher dan caesar cipher seperti pada proses enkripsi bagian enigma.
b. Mengenkripsi kembali cipher teks yang ada dengan algoritma enigma menggunakan kunci yang telah diperoleh pada poin a.
c. Mensubstitusikan hasil yang diperoleh pada poin b dengan huruf-huruf yang ada pada tabel substitusi (jika menggunakan random, maka randomisasi dilakukan dahulu terhadap kunci untuk memperoleh seed).
d. Hasil yang diperoleh pada proses c didekripsi menggunakan caesar cipher dengan menghitung banyaknya pergeseran ke kiri sesuai kunci masukan.
e. Hasil yang diperoleh pada proses d didekripsi menggunakan algoritma vigenere cipher dengan sebelumnya membalik kunci masukan user yang telah dipadding. Plain teks yang dihasilkan pada bagian ini merupakan plain teks asli pada pesan.

IV. IMPLEMENTASI DAN PENGUJIAN ALGORITMA

Berdasarkan hasil rancangan algoritma enkripsi berlapis di atas, dilakukan implementasi menggunakan teknik manual dan memanfaatkan program yang sudah ada untuk sebagian algoritma guna mendapatkan cipher teks hasil enkripsi suatu pesan.

Implementasi pada bagian rotor enigma cipher menggunakan teknik substitusi untuk menentukan pasangan huruf pada tiap rotor yang ada. Pasangan huruf pada setiap rotor didapatkan dari jenis rotor yang pernah digunakan oleh enigma yang pernah ada:

Rotor ABCDEFGHIJKLMNOPQRSTUVWXYZ
I EKMFLGDQVZNTOWYHXUSPAIBRCJ
II AJDKSIRUXBLHWTMCQGZNPYFVOE
III BDFHJLCPRTXVZNYEIWGAKMUSQO
Reflektor ABCDEFGDIJKGMKMIEBFTCVVJAT

Reflektor	Left Rotor		Center Rotor		Right Rotor		In/Out
A	A	E	A	A	A	B	A
B	B	K	B	J	B	D	B
C	C	M	C	D	C	F	C
D	D	F	D	K	D	H	D
E	E	L	E	S	E	J	E
F	F	G	F	I	F	L	F
G	G	D	G	R	G	C	G
D	H	Q	H	U	H	P	H
I	I	V	I	X	I	R	I
J	J	Z	J	B	J	T	J
K	K	N	K	L	K	X	K
G	L	T	L	H	L	V	L
M	M	O	M	W	M	Z	M
K	N	W	N	T	N	N	N
M	O	Y	O	M	O	Y	O
I	P	H	P	C	P	E	P
E	Q	X	Q	Q	Q	I	Q
B	R	U	R	G	R	W	R
F	S	S	S	Z	S	G	S
T	T	P	T	N	T	A	T
C	U	A	U	P	U	K	U
V	V	I	V	Y	V	M	V
V	W	B	W	F	W	U	W
J	X	R	X	V	X	S	X
A	Y	C	Y	Q	Y	Q	Y
T	Z	J	Z	E	Z	O	Z

Pada implementasi algoritma, setiap kemunculan spasi dan huruf lainnya akan dihilangkan dan hanya karakter alfabet saja yang terdapat di dalam plainteks untuk mempersulit proses dekripsi yang dilakukan dengan menebak-nebak kata.

Di bawah ini terdapat ujicoba dan analisis hasil ujicoba untuk menguji implementasi algoritma enkripsi berlapis. Enkripsi vigenere cipher menggunakan kakas yang pernah dibuat untuk tugas kecil 1, caesar cipher dan substitusi cipher menggunakan enkripsi manual, dan enigma cipher enkripsi manual dari tabel yang telah ditetapkan sebelumnya di atas.

Plain Teks: NAMA SAYA FITRIANA PASSA
Kunci : KRIPTOGRAFI

a. vigenere
   kunci vigenere : IFARGOTPIRKIFARGOTPIR
   cipher hasil: VFMRYORPNZDZNAEGDTHAR

b. caesar cipher
   dari kunci masukan user:
   K + R + I + P + T + O + G + R + A + F + I = 130 mod 26 = 0 kali pergeseran
   cipher hasil: VFMRYORPNZDZNAEGDTHAR

c. substitusi
   cipher hasil: PXGJMHJSTNHNTZCDYQWZJ

d. enigma
   kunci enigma: KJG
   posisi awal rotor:

Reflektor	Left Rotor		Center Rotor		Right Rotor		In/Out
A	K	N	J	B	G	C	A
B	L	T	K	L	H	P	B
C	M	O	L	H	I	R	C
D	N	W	M	W	J	T	D
E	O	Y	N	T	K	X	E
F	P	H	O	M	L	V	F
G	Q	X	P	C	M	Z	G
D	R	U	Q	Q	N	N	H
I	S	S	R	G	O	Y	I
J	T	P	S	Z	P	E	J
K	U	A	T	N	Q	I	K
G	V	I	U	P	R	W	L
M	W	B	V	Y	S	G	M
K	X	R	W	F	T	A	N
M	Y	C	X	V	U	K	O
I	Z	J	Y	Q	V	M	P
E	A	E	Z	E	W	U	Q
B	B	K	A	A	X	S	R
F	C	M	B	J	Y	Q	S
T	D	F	C	D	Z	O	T
C	E	L	D	K	A	B	U
V	F	G	E	S	B	D	V
V	G	D	F	I	C	F	W
J	H	Q	G	R	D	H	X
A	I	V	H	U	E	J	Y
T	J	Z	I	X	F	L	Z

Posisi akhir dari mesin enigma setelah melakukan enkripsi terhadap pesan :

Reflektor	Left Rotor		Center Rotor		Right Rotor		In/Out
A	K	N	J	B	A	B	A
B	L	T	K	L	B	D	B
C	M	O	L	H	C	F	C
D	N	W	M	W	D	H	D
E	O	Y	N	T	E	J	E
F	P	H	O	M	F	L	F
G	Q	X	P	C	G	C	G
D	R	U	Q	Q	H	P	H
I	S	S	R	G	I	R	I
J	T	P	S	Z	J	T	J
K	U	A	T	N	K	X	K
G	V	I	U	P	L	V	L
M	W	B	V	Y	M	Z	M
K	X	R	W	F	N	N	N
M	Y	C	X	V	O	Y	O
I	Z	J	Y	Q	P	E	P
E	A	E	Z	E	Q	I	Q
B	B	K	A	A	R	W	R
F	C	M	B	J	S	G	S
T	D	F	C	D	T	A	T
C	E	L	D	K	U	K	U
V	F	G	E	S	V	M	V
V	G	D	F	I	W	U	W
J	H	Q	G	R	X	S	X
A	I	V	H	U	Y	Q	Y
T	J	Z	I	X	Z	O	Z

Karena jumlah pesan tidak mencapai 26 karakter, rotor tengah dan rotor kiri tidak berubah (rotor kanan belum mencapai 1 putaran penuh).

plain : PXGJMHJSTNHNTZCDYQWZJ
cipher: LARTXJZCJWYFCJHBLEHLZ

Analisis hasil ujicoba:

Pada ujicoba di atas terlihat bahwa pada kombinasi algoritma vigenere cipher dan caesar cipher tidak memberikan efek apapun terhadap tingkat keamanan pesan karena pada dasarnya kombinasi kedua algoritma tersebut menghasilkan 1 cipher baru yang plain teksnya dapat dicari dengan pemecahan vigenere cipher biasa. Analisis sederhana masih bisa dilakukan untuk pesan-pesan yang panjang karena pada dasarnya setiap kedua algoritma di atas bertumpu pada kunci user. Kunci user

dapat diibaratkan sebagai gabungan dari kunci vigenere yang mengalami pergeseran sebanyak N kali sesuai hasil temuan pada caesar cipher. Pergeseran pada algoritma caesar cipher tidak hanya dapat dilakukan pada cipher teks dari vigenere cipher saja tetapi dapat dianggap dilakukan pada kunci yang dipakai oleh vigenere cipher. Dengan demikian, misal diasumsikan seseorang mencoba memecahkan kunci dari cipher teks gabungan vigenere cipher dan caesar cipher, hasil yang didapatkan adalah sebuah kunci baru yang sebenarnya adalah kunci yang dipakai vigenere cipher yang telah digeser sebanyak N kali. Akan tetapi, ketika cipher teks hasil enkripsi vigenere cipher dan caesar cipher dienkripsi dengan cipher substitusi, hasil yang didapatkan akan sulit didekripsi dengan analisis frekuensi biasa karena huruf yang dienkripsikan juga merupakan cipher teks yang bukan merujuk ke huruf-huruf yang biasa muncul pada analisis frekuensi biasa.

Pada enkripsi plain teks enigma (cipher teks pada cipher substitusi) menjadi cipher teks enigma, terlihat bahwa terdapat huruf yang sama pada plain teks enigma dienkripsi menjadi huruf yang berbeda meskipun pada dasarnya operasi enigma adalah operasi substitusi seperti pada substitusi cipher. Dengan demikian, kombinasi dari algoritma-algoritma kriptografi klasik dapat menciptakan sebuah algoritma kriptografi yang masih sulit dipecahkan dengan cara biasa.

Dari hasil enkripsi di atas, terlihat bahwa enkripsi berlapis lebih aman digunakan untuk melakukan pengiriman pesan sederhana daripada menggunakan salah satu algoritma kriptografi klasik yang ada.

VI. ANALISIS KEAMANAN DAN PEMECAHAN PESAN

1. Kompleksitas algoritma

Kompleksitas algoritma berlapis dihitung dari perkalian kompleksitas setiap algoritma yang dipakai:

a. Pada mesin enigma dengan 3 buah rotor, terdapat 26 x 26 x 26 state awal rotor yang mungkin. Jika posisi keempat rotor dapat diubah-ubah, maka terdapat ${}_3P_3$ x 26^3 state yang mungkin. Hasil yang didapatkan sangat besar sehingga di kala itu Jerman berpendapat bahwa pesan tersebut tidak mungkin di dekripsi oleh pihak ketiga. Selain itu, jika substitusi huruf di setiap rotor tidak diketahui, maka dibutuhkan kombinasi tambahan sebesar 26! untuk setaip rotor untuk menentukan pasangan huruf dalam rotor.
b. Pada algoritma caesar cipher, terdapat 26 pergeseran yang mungkin untuk pesan yang dienkripsi karena implementasi dilakukan pada mode 26 karakter (algoritma yang ada tidak menangani enkripsi selain karakter).
c. Pada algoritma vigenere cipher, kompleksitas dihitung dari 26^k , k adalah panjang kunci. Jika panjang kunci sulit ditentukan, maka kompleksitasnya menjadi 26^p, p adalah panjang pesan karena kunci pada vigenere diulang sebanyak panjang pesan.
d. Pada substitusi cipher, kompleksitas algoritma yang ada sebanyak 26!.

Kombinasi algoritma yang dipakai pada enkripsi berlapis menyebabkan kompleksitas yang dihasilkan menjadi paling kecil sebanyak perkalian kompleksitas algoritma yang ada. Apabila kriptanalis tidak mengetahui sama sekali susunan algoritma yang digunakan, maka kompleksitasnya menjadi sangat besar dengan mencoba berbagai permutasi susunan dari algoritma yang digunakan. Hasil yang sangat besar ini menyiratkan bahwa algoritma enkripsi berlapis cukup aman digunakan dan dibutuhkan waktu bertahun-tahun untuk mendekripsi sebuah pesan.

Selain itu, karena kunci yang digunakan untuk melakukan enkripsi telah dimodifikasi dari kunci asli, kemungkinan untuk mendekripsi pesan oleh pihak ketiga dengan menebak kunci yang ada menjadi sangat sulit untuk dilakukan. Pada dasarnya kunci yang dipakai oleh seluruh algoritma adalah sama, dan hanya dilakukan modifikasi kecil untuk setiap bagian algoritma yang ada. Apabila kunci dijamin tidak tersebar ke pihak ketiga dan susunan algoritma yang dipakai juga tidak diketahui orang lain, maka algoritma ini cukup aman digunakan untuk pengiriman pesan.

2. Kelemahan algoritma enkripsi berlapis

Pada implementasi enkripsi berlapis ini, kekuatan utama terletak pada enkripsi yang dilakukan oleh substitusi cipher dan enigma yang dapat mengaburkan frekuensi huruf yang muncul seperti pada algoritma vigenere cipher dan caesar cipher.

Akan tetapi, enigma mempunyai beberapa kelemahan diantaranya penyandian yang dilakukan bersifat resiprok (enkripsi suatu huruf X yang menghasilkan huruf Y berarti bahwa enkripsi pada huruf Y akan menghasilkan huruf X), fakta bahwa sebuah huruf tidak mungkin dipetakan ke dirinya sendiri, kunci pesan yang harus dikirim 2 kali, dan kesalahan dalam proses assignment *initial value* yang mengandung kata yang mudah ditebak. Akan tetapi dalam enkripsi berlapis yang dibahas dalam makalah ini, kemungkinan menebak kunci enigma tidak mungkin dilakukan selama kunci asli masih tersimpan kerahasiaanya karena kunci enigma digenerate dari kunci asli.

3. Teknik pemecahan pesan sederhana atau serangan yang mungkin dilakukan untuk memecahkan algoritma enkripsi berlapis

Teknik pemecahan pesan yang biasa dilakukan untuk mendekripsi algoritma kriptografi klasik adalah:

a. analisis frekuensi
   teknik analisis frekuensi tidak dapat dilakukan pada enkripsi berlapis sebab algoritma-algoritma yang digunakan untuk melakukan enkripsi sebagian adalah algoritma yang membuat enkripsi setiap huruf plain teks belum tentu dienkripsi menjadi huruf cipher yang sama.
b. metode kasiski
   metode ini digunakan untuk menentukan panjang kunci pada cipher teks. Metode ini biasanya digunakan untuk kalimat berbahasa inggris dan data frekuensi kata dalam bahasa Indonesia belum

tersedia dengan baik sehingga metode ini tidak dapat dipakai untuk melakukan deteksi panjang kunci. Kemunculan huruf / gabungan huruf yang menjadi dasar deteksi dari metode kasiski dapat dikacaukan dengan teknik enkripsi vigenere cipher maupun enigma (suatu huruf plain teks yang sama belum tentu dienkripsi menjadi huruf cipher yang sama).

c. Exhaustive search. Karena kompleksitas dari enkripsi berlapis sangat besar, exhaustive search biasa tidak sanggup untuk memecahkan algoritma enkripsi berlapis dalam jangka waktu yang singkat.

d. Known plaintext attack
Meskipun sebagian teks asal sudah diketahui, pemecahan pesan menggunakan metode ini tetap sulit dilakukan karena tahap-tahap enkripsi antar algoritma masih tersembunyikan dan hasil enkripsi sebagian plain teks menjadi cipher teks, meskipun menghasilkan hasil yang benar, masih sangat sulit untuk membuat dekripsi keseluruhan pesan berhasil dilakukan.

e. Algoritma enkripsi diketahui
Ketika seseorang mendapatkan cipher teks dan mendapatkan algoritma apa saja yang digunakan untuk mengenkripsi plain teks menjadi cipher teks yang bersangkutan, orang tersebut harus membuat kombinasi sejumlah besarnya kompleksitas pada enigma cipher untuk menemukan kunci yang sesuai sebagai kunci enigma. Hal ini masih sangat sulit dilakukan untuk pemecahan cipher teks dengan metode sederhana tanpa bantuan alat apapun.

Karena penggunaan teknik – teknik sederhana kurang efektif untuk memecahkan cipher teks pada hasil enkripsi algoritma enkripsi belapis, algoritma enkripsi berlapis masih cukup aman digunakan untuk pengiriman pesan sederhana.

VII. KESIMPULAN

Enkripsi berlapis menggunakan algoritma kriptografi klasik merupakan salah satu cara sederhana untuk membuat pesan yang dienkripsi menggunakan mode karakter menjadi lebih aman dibandingkan hanya menggunakan 1 macam algoritma jika dilihat dari kompleksitas kombinasi dari semua algoritma yang ada. Modifikasi kunci yang dilakukan pada setiap algoritma membuat pemecahan pesan dengan teknik pencarian kunci lebih sulit untuk dilakukan karena kunci yang dihasilkan tidak membentuk suatu kata sehingga harus dilakukan kombinasi kemungkinan kunci yang lebih banyak.

Meskipun enkripsi berlapis aman digunakan untuk pengiriman pesan sederhana dan sulit dipecahkan dengan teknik pemecahan cipher teks biasa, tetapi enkripsi berlapis masih sangat mungkin dipecahkan menggunakan kakas yang sudah ada dan analisis yang lebih dalam pada cipher teks yang ditemukan.

REFERENSI

[1] Munir, Rinaldi. Algoritma Kriptografi Klasik (bagian 1-5). *Slide Kuliah IF3058 Kriptografi*.

[2] -----. The Enigma cipher machine. http://www.codesandciphers.org.uk/enigma/. Tanggal akses : 22 Maret 2011 pukul 11:28 WIB.

[3] -----. Enigma Cipher. http://www.cs.trincoll.edu/~crypto/historical/enigma.html. Tanggal akses : 22 Maret 2011 pukul 11:28 WIB.
-----. Re: Enigma Rotor Algorithm. http://coding.derkeiler.com/Archive/General/comp.programming/2007-01/msg00211.html Tanggal akses : 22 Maret 2011 pukul 11:33 WIB.

[4] -----. Enigma Cipher Machine. http://www.cryptomuseum.com/crypto/enigma/ Tanggal akses: 23 Maret 2011 pukul 10:40 WIB.

[5] -----. German Enigma Cipher. http://cryptocellar.web.cern.ch/cryptocellar/Shaylor/bombe.html Tanggal akses : 23 Maret 2010 pukul 10:40WIB.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 21 Maret 2011

Fitriana Passa
NIM 13508036