Studi, Analisis, dan Pengembangan Algoritma Enkripsi Trifid Cipher

M. Albadr Lutan Nasution - 13508011[1]

Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]albadr.ln@itb.ac.id

***Abstrak*—Algoritma kriptografi klasik trifid cipher merupakan algoritma kriptografi klasik yang tergolong sulit dipecahkan. Dilahirkan tahun 1901, diawal masa perang dunia, serta dimensi prosesnya, algoritma ini memiliki karakteristik di antara algoritma kriptografi klasik dan modern.**

Karakteristik yang dimiliki trifid cipher mengundang studi kembali terhadapnya sehingga dapat diterapkan prinsip algoritma kriptografi modern yang memecah huruf menjadi kode yang lebih kecil atau bit dalam pengembangan trifid cipher. Dilakukan pula perbandingan algoritma hasil pengembangan dengan beberapa algoritma lain.

***Kata Kunci*—Difid Cipher, Trifid Cipher, *Polybius Square*, Kriptografi Klasik, Kriptografi Modern**

I. SEKILAS KRIPTOGRAFI

Kriptografi adalah ilmu yang berkembang. Meskipun secara formal, kriptografi baru secara luas diajarkan pada sekolah publik pada awal abad 20 karena sifatnya yang tabu dan kerahasiaannya yang terjaga. Dahulu, pengajaran kriptografi adalah tabu dan hanya berada dalam ranah militer karena algoritma kriptografi dianggap tidak boleh bocor kepada musuh. Sebelum pada akhirnya, Prinsip Kerckhoffs menyatakan bahwa sebuah sistem haruslah tetap aman meskipun segala sesuatu tentangnya, kecuali sandi kunci, diketahui publik.

Kriptografi dapat dipandang sebagai ilmu dan juga seni untuk menjaga kerahasiaan berita. A. Menezes, P. van Oorschot, dan S. Vanstone berpendapat bahwa "Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data."

Kini kriptografi sebagai ilmu semakin berkembang pesat. Dengan datangnya era komputer kriptografi bertransformasi dari kriptografi klasik menjadi kriptografi modern. Algoritma bisa dibuat sangat kuat serta memenuhi Prinsip Kerckhoffs. Perkembangan komputer juga membuat pemecahan kriptografi semakin mudah sehingga kompetisi algoritma modern sangatlah tinggi.

Sebagai ilmu yang berkembang pesat, pemahaman terhadap dasar dari ilmu kriptografi tidak boleh diabaikan. Algoritma kriptografi klasik dan kriptografi modern yang sudah tertinggal tidak semestinya tinggal di tempat sampah. Kita dapat memelajari ulang algoritma tersebut demi memahami bagaimana sebenarnya perkembangan kriptografi sendiri dan bagaimana kriptografi dapat dikembangkan lebih jauh lagi.

II. BIFID DAN TRIFID CIPHER

Algoritma bifid dan trifid cipher adalah algoritma yang tergolong pada algoitma kriptografi klasik. Ditemukan oleh Felix Delastele, Algoritma ini menggunakan persegi polibius dan pemecahan karakter untuk memperoleh efek difusi pada cipherteksnya. Dilahirkan tahun 1901, algoritma ini bisa dipahami sebagai jembatan antara algoritma klasik dan algoritma modern.

Pada algoritma kriptografi bifid cipher, digunakan persegi polibius ukuran 5x5 atau 6x6. Ukuran ini digunakan atas pertimbangan jumlah huruf dalam abjad alfabet sejumlah 26 buah atau 36 buah termasuk angka.

Setiap huruf pada persegi ini dikenali dengan koordinat posisi huruf diletakkan. Misalkan persegi polibius berikut yang diperoleh dari kata kunci "Persegi Polybius Contoh" seperti tampak pada **Gambar 1**, huruf 'A' memiliki koordinat (4,1).

	1	2	3	4	5
1	P	E	R	S	G
2	I	O	L	Y	B
3	U	C	N	T	H
4	A	D	F	K	M
5	Q	V	W	X	Z

Gambar 1 *Persegi polibius*

Penyandian dilakukan dengan melakukan konversi huruf-huruf dari plainteks ke koordinat pada persegi polibius. Koordinat *x* dan *y* ditulis secara vertikal atas-bawah sesuai posisi huruf pada kalimat.

```
SABOTASE KAMP LINI UTARA
14223411 4441 2232 33414
41524142 4151 3131 14131
```

Gambar 2 *Contoh konversi plainteks ke koordinat*

Angka-angka koordinat yang telah dituliskan tadi kemudian dibaca dalam baris dan digabung menjadi satu baris. Angka koordinat ini kemudian dikelompokkan dua dan dikonversi lagi menjadi huruf dengan persegi polibius

yang sama. **Gambar 2** dan **Gambar 3** dapat mengilustrasikan penggunaan bifid cipher ini.

```
142234114441223233414415241424151313114131
S O N P K A O C N A K G Y S Y G R R P A U
```

Gambar 3 *Konversi plainteks pada Gambar 2 menjadi cipherteks*

Dengan demikian setiap karakter pada cipherteks bergantung pada dua karakter plainteks sehingga bifid cipher termasuk pada algoritma cipher substitusi digrafik.

Untuk melakukan dekripsi, cukup dilakukan pembalikan prosedur. Pada pesan yang panjang dapat dilakukan pemecahan teks menjadi beberapa blok. Setiap blok kemudian dienkripsi secara terpisah.

Berdasarkan bifid cipher, Felix kemudian mengembangkan algoritma trifid cipher yang termasuk Trigraf. Algoritma ini hanya mengubah persegi polibius yang digunakan pada bifid cipher dari dua dimensi menjadi tiga dimensi. Untuk karakter alfabet sejumlah 26 buah, biasanya digunakan kubus berukuran 3x3x3 sehingga persegi dapat memuat keseluruhan abjad. Sisa ruang satu buah biasanya dipakai untuk karakter titik.

Selanjutnya, prosedur enkripsi pesan mirip dengan prosedur yang digunakan pada bifid cipher. Setiap karakter pada plainteks dikonversi menjadi angka koordinat pada kubus polibius dan ditulis vertikal. Angka –angka koordinat dari masing-masing karakter ini dibaca perbaris dan dikonversi lagi dengan kubus polibius yang sama sehingga menghasilkan cipherteks.

Layer 1				Layer 2				Layer 3			
	1	2	3		1	2	3		1	2	3
1	P	E	R	1	B	U	C	1	J	K	M
2	S	G	I	2	N	T	H	2	Q	V	W
3	O	L	Y	3	A	D	F	3	X	Z	.

Gambar 4 *Contoh kubus polibius pada trifid cipher*

Gambar 4 merupakan contoh dari kobus polibius dengan kata sandi "Persegi Polybius Contoh". Secara teori, setiap huruf dikonversikan ke koordinat pada kubus seperti pada Gambar 4. Hanya saja, lebih praktis untuk memetakan setiap huruf menjadi tabel berisi daftar kode triplet setiap huruf seperti pada Gambar 5.

```
P 111     I 132     D 213     K 321
S 112     Y 133     C 231     V 322
O 113     B 211     H 232     Z 323
E 121     N 212     F 233     M 331
G 122     A 213     J 311     W 332
L 123     U 221     Q 312     . 333
R 131     T 222     X 313
```

Gambar 5 *Tabel triplet dari Gambar 4*

Berdasarkan kubus polibius pada Gambar 4 atau tabel referensi pada Gambar 5, pesan dapat dienkripsikan dengan cara yang sama seperti algoritma bifid cipher.

```
SABOTASE KAMP LINI UTARA
12212211 3231 1121 22212
11112112 2131 2313 22131
23132321 1311 3222 12313

122 122 113 231 112 122 212 111 121 122 131 231
 G   G   O   B   S   G   N   P   E   G   R   C
322 131 231 323 211 311 322 212 313
 V   R   C   Z   B   J   V   N   X
```

Gambar 6 *Contoh enkripsi dengan trifid cipher*

Melakukan dekripsi pun sama seperti bifid cipher. Kita hanya perlu melakukan prosedur secara terbalik, yakni berdasarkan kubus polibius setiap karakter cipherteks diubah menjadi angka koordinat dan ditulis secara membaris. Barisan angka kemudian dipecah menjadi tiga sehingga tersusun tiga baris. Setiap kolom yang terdiri dari tiga angka koordinat ini bisa dibalikkan menjadi karakter plainteks dengan kubus polibius yang sama.

III. STRATEGI PENGEMBANGAN : TRIFID DAN N-FID CIPHER

Pada pengembangan algoritma trifid cipher dari bifid cipher, dapat dilihat faktor pengembang yang utama adalah penambahan dimensi kotak polibius dari persegi menjadi kubus. Pada trifid cipher, ukuran 3x3x3 dipilih dengan pertimbangan jumlah karakter pada abjad alfabet adalah 26. Dengan $2^3 < 26 < 3^3$, logislah bahwa kita memerlukan kubus dengan orde minimal 3 agar dapat memasukkan seluruh huruf pada abjad alfabet.

Dengan mengubah kubus pada trifid cipher menjadi berukuran orde 4, kita akan memperoleh 64 buah simbol yang dapat dijadikan acuan. Dengan jumlah karakter pada abjad alfabet hanya 26 buah, jumlah ini mungkin terlalu banyak. Akan tetapi dengan membedakan antara huruf kecil dan huruf kapital serta memasukkan angka ke dalam kamus huruf, kita akan memperoleh 62 karakter yang dapat memenuhi kubus orde 4 tadi.

Pengembangan dengan mengubah orde kubus yang digunakan bisa melebihi orde 4. Hal ini bergantung pada karakter-karakter yang ingin dimasukkan pada ruang enkripsi. Kita bisa saja menggunakan satu set karakter ASCII sejumlah 128 karakter, set karakter ISO Latin 1 sejumlah 256 karakter, atau Unicode dengan ribuan karakter untuk memenuhi orde kubus yang tinggi.

Penggunaan set karakter berjumlah besar memang terlalu berlebihan untuk dan bukan karakteristik dari algoritma kriptografi klasik. Algoritma klasik biasanya hanya memakai 26 karakter pada set abjad alfabet dalam ruang enkripsinya. Hal ini menjadi salah satu alasan trifid cipher dapat dipandang sebagai algoritma kriptografi semi modern yang berada pada batas kriptografi klasik dan kriptografi modern.

Pengembangan dimensi kotak polibius dari dua dimensi ke tiga dimensi juga mengubah karakteristik cipher dari substitusi bigraf menjadi substitusi trigraf dan

menambah efek difusi dari enkripsi. Dengan melihat pengembangan dimensi ini, kita dapat pula mengembangkan trifid cipher menjadi n-fid cipher dengan menggunakan dimensi kotak polibius yang lebih tinggi. Dengan demukian, n-fid cipher yang dibangun memiliki karaktersistik substitusi poligraf.

Dengan menggunakan kotak polibius berdimensi 4, agar dapat memenuhi 26 karakter pada abjad alfabet dibutuhkan minimal kotak dimensi empat orde tiga. Akan tetapi, jumlah ruang yang dimiliki kotak kini $3^4 = 81$ yang terlalu banyak dibandungkan dengan 26 karakter yang kita miliki. Padahal, dengan menggunakan kotak dimensi empat orde dua, jumlah ruang yang dimiliki kotak kini hanya $2^4 = 16$, tidak mencukupi 26 karakter. Tentu saja hal ini dapat diatasi dengan memperbanyak jumlah karakter yang dapat dilakukan enkripsi.

Pada kotak polibius dimensi 5, kita hanya memerlukan orde dua untuk mendapatkan $2^5 = 32$ buah karakter. Jumlah ini mencukupi jumlah yang dimiliki oleh set abjad alfabet yang menjadi ruang enkripsi algoritma klasik. Akan tetapi, kini setiap huruf dalam mode enkripsi 5-fid ini dapat direpresentasikan menjadi lima bit sehingga konversi yang dilakukan menjadi seperti *encoding* biner. Hal inilah alasan lain yang membuat trifid cipher dapat berubah dari algoritma kriptografi klasik menjadi seperti algoritma kriptografi modern, karena karakteristik dari kriptografi modern adalah manipulasi bit.

Dengan mengetahui bahwa algoritma kriptografi trifid cipher yang dibesarkan dimensinya dapat membawa pengkodean karakter menjadi *binary encoding*, kita dapat membuat dimensi kotak polibius menjadi delapan dimensi. Dengan demikian, keseluruhan pengkodean dalam karakter ASCII sejumlah 128 karakter atau ISO Latin 1 sejumlah 256 karakter dapat dijangkau secara utuh oleh algoritma enkripsi ini.

Algoritma trifid cipher yang asli biasa diterapkan dengan enkripsi sejumlah tertentu karakter dari plainteks yang disebut dengan periode. Setiap periode dienkripsi secara terpisah. Dengan penerapan prinsip bit seperti yang telah dijelaskan dan penggunaan periode atau blok yang telah biasa diterapkan pada trifid cipher, dalam pengembangan algoritma ini dapat pula diterapkan mode-mode yang terdapat pada enkripsi cipher blok. Penerapan periode atau blok pada trifid klasik hampir sama dengan penerapan mode ECB pada enkripsi cipher blok. Dengan penggunaan bit, mode CBC, CFB, dan OFB menjadi mungkin untuk diterapkan.

Pemakaian kunci pada trifid cipher dan pengembang-annya ini hanya digunakan untuk membangun kotak polibius. Jumlah karakter kunci yang dimasukkan seharusnya tidak menjadi masalah, karena dengan masukan N karakter yang kurang dari jumlah ruang pada kotak polibius, N karakter yang tidak berulang akan diisikan ke kotak polibius. Selanjutnya sisa karakter akan diisikan ke sisa ruang yang ada hingga seluruh ruang pada kotak terisi.

Untuk menambah kerumitan, dapat pula dilakukan generasi sejumlah kunci dari kunci utama atau kunci blok yang dimasukkan oleh user. Masing-masing kunci yang digenerasi ini menjadi masukan untuk membentuk kotak polibius. Plainteks akan diekripsi dengan n-fid cipher beberapa kali sejumlah kunci yang digenerasi. Hanya saja, algoritma penggenerasi kunci ini diluar bahasan trifid cipher dan bergantung pada disainer penggenerasi kunci itu sendiri.

IV. IMPLEMENTASI

Dari beberapa strategi pengembangan trifid cipher yang telah dikemukakan dilakukan dua buah implementasi algoritma sebagai berikut.

A. Pentafid dengan Baudot-Murray Code

Implementasi pertama didasarkan atas strategi penaikan dimensi kotak polibius trifid cipher menjadi dimensi lima. Dengan menggunakan kotak polibius dimensi lima, ruang karakter untuk enkripsi menjadi 2^5 yaitu 32 buah karakter. Dengan jumlah karakter alphabet 26 buah, jumlah ini mencukupi.

Akan tetapi, terkadang pada pesan kita tidak hanya menggunakan huruf tetapi juga karakter lain seperti spasi, enter, dan tanda baca. Sisa ruangan dari 32 ruang pada kotak polibius dapat digunakan untuk karakter ini. Dapat pula digunakan dua kotak polibius ukuran 2^5 yang memiliki karakter kontrol yang memberikan perintah untuk berpindah antara satu kotak ke kotak lain.

Enkoding karakter dengan menggunakan lima bit pernah digunakan pada sistem telekomunikasi dahulu. Salah satu *encoding* yang terkenal adalah Baudot-Murray Code yang sering digunakan untuk komunikasi radio amatir dan telegraf. Enkoding ini memiliki struktur standar sebagai berikut.

Kode	Mode Karakter	Mode Simbol	Kode	Mode Karakter	Mode Simbol
000000	null	null	10000	E	3
00001	T	5	10001	Z	"
00010	Carriage	Carriage	10010	D	$
000011	O	9	10011	B	?
000100	space	space	10100	S	'
000101	H	#	10101	Y	6
000110	N	,	10110	F	!
000111	M	.	10111	X	/
001000	Line	Line	11000	A	-
001001	L	)	11001	W	2
001010	R	4	11010	J	'
001011	G	&	11011	Pindah_ke _Simbol	Pindah_ke _Simbol
001100	I	8	11100	U	7
001101	P	0	11101	Q	1
001110	C	:	11110	K	(
001111	V	;	11111	Pindah_ke_ Huruf	Pindah_ke_ Huruf

Gambar 7 Tabel Baudot-Murray Code

Pengambangan algoritma enkripsi dari trifid cipher dengan kotak berdimensi lima – sebut saja pentafid cipher – dapat pula menggunakan tabel di atas. Representasi kotak polibius adalah berupa dua buah senarai karakter yang berisi (secara *default*) huruf dan simbol dengan susunan seperti pada Gambar 7. Kotak polibius dibangun dari kunci yang dimasukkan pengguna, ditulis secara urut sesuai kemunculan karakter pada kunci sesuai dengan jenis karakter – huruf atau simbol, lalu diisikan huruf yang belum ada pada kunci secara berurut.

Enkripsi dapat direalisasikan dengan memodifikasi plainteks – yang terdiri dari huruf dan simbol – menjadi plainteks *extended* berupa senarai bilangan dengan bilangan masing-masing berupa posisi dari setiap huruf atau simbol pada kotak polibius dan disisipi sebuah karakter *pindah_ke_simbol* atau *pindah_ke_simbol* di saat terjadi perubahan dari mode huruf ke mode simbol (pada plain teks). Plainteks *enxtended* ini yang kemudian dienkripsi.

Karena pentafid cipher diturunkan dari trifid cipher, algoritma yang digunakan haruslah sama. Bilangan (*integer*) pada plainteks extended dikonversi menjadi bit (atau bilangan basis dua). Setiap bit dari bilangan ini kemudian ditulis secara vertikal sesuai posisi bilangan pada senarai (*array*). Setelah didapat lima baris rentetan bit sepanjang panjang senarai pada plainteks *extended*, kelima baris disatukan. Cipherteks didapat dari pengambilan setiap lima bit pada baris penyatuan tadi.

Dengan demikian, diperoleh senarai bilangan yang merupakan hasil enkripsi. Senarai bilangan ini kemudian diubah representasinya menjadi huruf atau simbol sesuai kotak polibius yang ada. Jika ada bilangan yang kebetulan karakternya adalah karakter *pindah_ke_simbol* atau *pindah_ke_simbol*, dilakukan pemindahan mode. Mode awal yang digunakan adalah mode huruf. Dengan demikian kita memperoleh senarai cipherteks yang mungkin berisi kombinasi huruf (sesuai daftar pada set *encoding* Baudot-Murray mode huruf) dan simbol (sesuai daftar pada set *encoding* Baudot-Murray mode simbol).

Karena setiap karakter representasi bit, operasi bit XOR dapat dilakukan sehingga dapat dibentuk blok cipher dengan implementasi algoritma pentafid cipher ini. Setiap blok dikonversi secara terpisah satu sama lain seperti ECB atau dengan mode block cipher lain seperti CBC, CFB, dan OFB.

Dengan demikian urutan enkripsi pada mode ini adalah

1. Mengubah plain teks menjadi plain teks extended yang sudah ditambahi karakter kontrol pemindah mode. Plain teks *extended* berupa senarai bilangan representasi posisi pada kotak polibius.
2. Membagi seluruh plain teks extended menjadi blok-blok sebesar lebar blok, misalkan delapan bilangan per blok.
3. Mengenkripsi setiap blok menurut mode yang digunakan dengan prosedur trifid cipher.
4. Ubah cipher teks *extended* yakni yang masih berupa senarai bilangan yang juga memiliki posisi ke karakter kontrol pemindah mode menjadi cipher teks biasa untuk ditampilkan ke pengguna.

Urutan dekripsi hanyalah kebalikan dari urutan diatas. Dengan penggunaan dua kotak polibius ini, dapat dilihat bahwa hal yang pertama dilakukan saat baik enkripsi maupun dekripsi adalah menambahi posisi karakter kontrol pemindah mode pada kotak polibius bersamaan dengan mengubah karakter manjadi bilangan penunjuk posisi ke kotak polibius.

Plainteks :

KRIPTOGRAFI, WAH HEBAT

Cipherteks:

EOW5”-(`:2!7!3?”’5.*null5/r6-crnull* 5 3 *null*

Gambar 8 Contoh Plainteks dan Cipherteks tanpa kunci

Plainteks :

KRIPTOGRAFI, WAH HEBAT

Kunci:

KEY

Cipherteks:

EKCSQNFKWGAF`EPJNEMM*cr*OXE*nullL**nullP**nullnull*

Gambar 9 Contoh Plainteks dan Cipherteks dengan kunci

Pada Gambar 8 dan Gambar 9, yang dicetak miring adalah karakter yang jika ditulis namanya tidak akan tampak. Terlihat pada gambar bahwa cipherteks lebih panjang dari plainteks. Hal ini disebabkan karena terdapat penambahan posisi karakter kontrol pemindah mode yang ikut dienkripsi dan *padding* karena plainteks plus karakter kontrol tadi tidak mencukupi besar blok.

B. Oktofid dengan ISO Latin-1

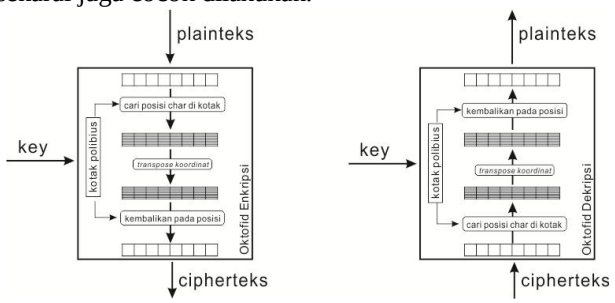
Implementasi kedua didasarkan atas strategi penaikan dimensi kotak polibius trifid cipher menjadi dimensi delapan dengan orde dua. Dengan jumlah ruang yang ada pada kotak polibius sejumlah $2^8 = 256$ karakter, set karakter yang digunakan dalam implementasi ini adalah set karakter pada ISO Latin-1. Dengan demikian, jika user tidak memasukkan kunci ke kotak polibius, atau memasukkan nol buah karakter, atau memasukkan karakter null, *encoding* pada kotak polibius menjadi sama persis dengan *encoding* pada ISO Latin-1.

Enkripsi akan dilakukan seolah-olah cipher blok dengan pemilihan periode atau besar blok sebesar 64 bit. Dengan blok cipher ini, dapat diterapkan mode blok cipher yang umum yakni ECB, CBC, CFB-8bit, dan OFB-8bit.

Setiap enkripsi satu blok hanya dilakukan satu kali enkripsi menggunakan oktofid cipher sehingga kunci blok yang dimasukkan user hanya akan berguna untuk membentuk satu kotak polibius. Berbeda dengan cipher blok biasa, panjang kunci tidak harus sama dengan panjang blok karena kunci akan digunakan untuk membentuk kotak polibius.

Pada praktiknya, kotak polibius dimensi delapan ini adalah senarai bilangan sebesar 256 karakter. Yang disimpan dalam kotak polibius adalah nilai bilangan dari

0 sampai 255, bukan karakter karena meskipun set karakter yang digunakan adalah set karakter ISO Latin-1, *encoding* atau urutan pengkodean yang digunakan tidak mesti sama, bergantung pada kunci yang dimasukkan oleh user. Jika user memasukkan hanya karakter null atau nol buah karakter, indeks bilangan dan isi bilangan pada senarai akan sama. Hal inilah yang menyebabkan *encoding* pada kotak polibius menjadi sama persis dengan *encoding* pada ISO Latin-1. Dengan maksimum nilai bilangan yang dipakai adalah 256, pemakaian byte untuk senarai juga cocok dilakukan.



Gambar 10 *Skema Blok Enkripsi dan Dekripsi Oktofid Cipher*

Setiap blok plainteks atau input yang masuk ke dalam fungsi enkripsi blok E akan dikonversi menjadi bilangan sesuai posisinya pada *encoding* ISO Latin-1. Bilangan ini kemudian dicari letaknya dalam senarai bilangan yang merepresentasikan kotak polibius dimensi delapan. Posisi ditemukannya bilangan ini akan sama dengan koordinat bit 8 dimensi pada kotak polibius. Nilai posisi kemudian dikonversi menjadi delapan bit. Selanjutnya dengan prosedur seperti halnya trifid cipher, dilakukan transposisi bit yang terdiri dari 8 baris.

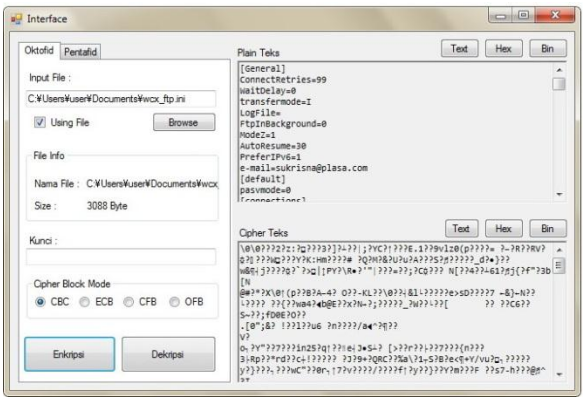
```
private byte[] oktoBox = new byte[256];

private byte subCharToPos (byte chara){
    int position=0;
    bool found = false;
    while (!found && position < 256)
    {  //cari chara di oktobox
       if (oktoBox[position] == chara)
          found = true;
       else
          position++;
    }
    return (byte) position;
}

private byte subPosToChar(byte position)
{ oktoBox[position];}

public byte[] encript(byte[] plain)
{
    byte[] cipher = new byte[8];
    //substitusi chara to pos
    for (int i = 0; i < 8; i++)
       cipher[i] = subCharToPos(plain[i]);
    //transpose koordinat
    cipher = eightbyteTranspose(cipher);
    //subst transposed koordinat to char
    for (int i = 0; i < 8; i++)
       cipher[i] = subPosToChar(cipher[i]);

    return cipher;
}
```

Gambar 11 *Code C# dari prosedur enkripsi oktofid cipher*

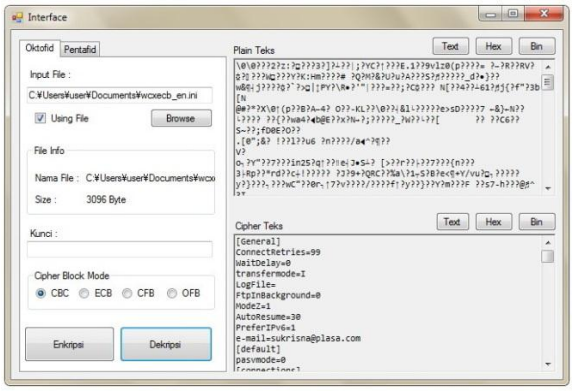
Dengan implementasi oktofid yang beroperasi dengan byte (delapan bit), implementasi ini dapat dengan mudah diterapkan untuk mengenkripsi berkas digital. Sehingga selayaknya algoritma kriptografi modern, algoritma ini dapat digunakan untuk mengamankan berkas.

Pada Gambar 12 hingga **Gambar 15**, dapat dilihat interface program implementasi oktofid dengan menggunakan bahasa C# pada Visual Studio.

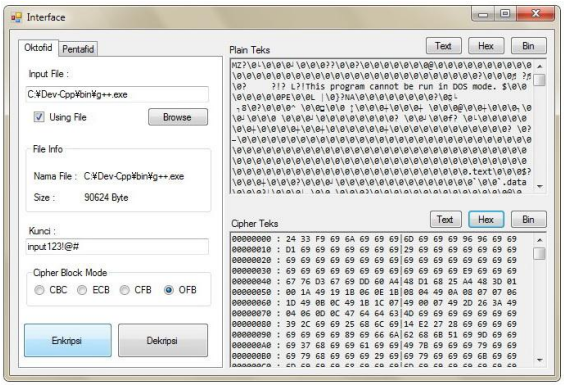
Pada Gambar 12 dan Gambar 13 didemonstrasikan enkripsi dan dekripsi dengan implementasi oktofid mode CBC dan tanpa menggunakan kunci, artinya urutan kotak polibius sama dengan encoding ISO Latin 1. Pada Gambar 14 dan **Gambar 15** didemostrasikan enkripsi dan dekripsi mode OFB dengan inisial vektor "**albadrln**" kata kunci "**input123!@#**".



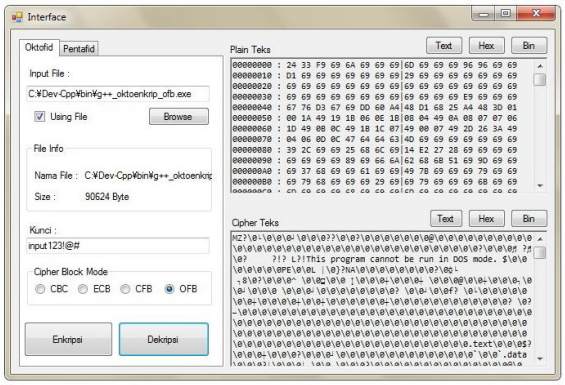
Gambar 12 *Program Kripto Oktofid, contoh enkripsi cipher blok sebuah berkas teks dengan mode CBC*



Gambar 13 *Program Kripto Oktofid, contoh enkripsi cipher blok sebuah cipherteks dari berkas teks dengan mode CBC*



Gambar 14 *Program Kripto Oktofid, contoh enkripsi cipher blok sebuah cipherteks dari berkas exe dengan mode OFB*



Gambar 15 *Program Kripto Oktofid, contoh dekripsi cipher blok sebuah cipherteks dari berkas exe dengan mode OFB*

Secara umum, enkripsi dengan implementasi oktofid dengan menggunakan mode CFB dan ECB sama dengan penggunaan algoritma lain sehingga gambar diatas cukup mewakili demo program dari pengembangan trifid cipher implementasi oktofid ini.

V. ANALISIS PENGEMBANGAN

A. Pentafid dengan Baudot-Murray Code

Algoritma yang dikembangkan dengan implementasi pentafid cipher memiliki beberapa kelebihan. Yang paling jelas adalah peningkatan keamanan karena karakteristik substitusi yang meningkat dari trigrafik menjadi pentagrafik.

Kelebihan lain adalah pada implementasi yang diajukan, dilakukan ekspansi ruang karakter yang digunakan sebagai ruang enkripsi dari 27 huruf menjadi 64 huruf dengan memanfaatkan dua kotak polibius dan karakter kontrol untuk pindah antar mode. Akan tetapi, pada pentafid cipher ekspansi dari 32 huruf menjadi 64 huruf ini tidak menambah keamanan. Hal ini karena algoritma yang digunakan adalah sama, dan enkripsi sebuah bilangan yang menandakan posisi sebuah karakter pada kotak polibius tidak bergantung pada mode representasinya. Ekspansi ini hanya memberikan perluasan representasi kepada pengguna dengan kata lain fitur bagi pengguna untuk representasi pesan yang lebih luas dengan dikenalinya simbol dan angka.

Pada implementasi pentafid cipher, telah digunakan komponen penyusun karakter berupa bit-bit. Dengan kara lain, enkripsi yang dilakukan adalah manipulasi bit seperti halnya algoritma kriptografi modern. Hanya saja, dengan jumlah ruang karakter yang digunakan untuk representasi hanya 32 karakter yang sebagian besar karakter alphabet biasa (atau 64 pada contoh implementasi dengan *encoding* Baudot Murray), algoritma pentafid cipher masih bisa dianggap sebagai algoritma krpitografi klasik. Dengan jumlah ruang karakter yang masih dapat dianggap sedikit ini, algoritma ini masih mungkin dilakukan dengan pensil dan kertas, meskipun cukup sulit. Kesulitan terjadi karena adanya karakter *carriage return*, *line feed*, dan *null* pada set karakter pada *encoding* Baudot-Murray, padahal karakter-karakter ini sulit dikenali manusia.

Dalam implementasi menggunakan dua kotak polibius dengan penambahan karakter kontrol pemindah untuk perpindahan seperti pada usulan juga terdapat beberapa hal yang menajadi masalah. Jika karakter kontrol dihapus pada cipher teks, artinya nantinya akan dihitung ulang saat dekripsi, jika saat enkripsi ternyata dihasilkan dua karakter pemindah ke mode yang sama berurutan hal ini akan membuat kesalahan dekripsi.

Kedua masalah terakhir dapat diatasi dengan membiarkan representasi cipherteks menjadi senarai bilangan yang merepresentasikan posisi kata kotak polibius yang digunakan, sehingga bilangan tidak perlu diterjemahkan ke representasi karakter di akhir enkripsi dan diterjemahkan ke bilangan di awal dekripsi. Akan tetapi, hal ini akan mereduksi keamanan enkripsi menjadi nol karena angka inilah yang seharusnya disembunyikan. Dibanding mengubah ke bentuk karakter, pengubahan karakter ke posisi bilangan pada *encoding* ASCII atau Latin-1-nya merupakan solusi yang lebih baik.

Dengan pengubahan karakter menjadi representasi bit, dapat pula dilakukan operasi bit pada algoritma ini. Hal ini berguna untuk membuat mode blok cipher seperti *Cipher Block Chaining* yang menggunakan operasi XOR antar bloknya. Hanya saja, karena representasi yang digunakan hanya lima bit, algoritma ini tidak praktikal untuk mengenkripsi sebuah berkas. Sebuah berkas digital direpresentasikan sebagai aliran byte yakni berupa representasi delapan bit. Sehingga untuk dapat mengenkripsi berkas, setiap byte pada file harus diubah menjadi senarai bit dahulu sebelum dikelompokkan lima-lima. Hal ini tentu merupakan usaha yang sangat besar karena sebuah berkas biasanya memiliki puluhan sampai ratusan ribu byte.

B. Oktofid dengan ISO Latin-1

Perbandingan antara algoritma trifid cipher dan implementasi oktofid cipher cukup nyata. Algoritma trifid cipher merupakan algoritma trigrafik praktikal pertama. Hal inilah yang menyebabkan algoritma ini digolongkan sebagai algoritma enkripsi tangan dan pensil tersulit yang pernah ada. Dengan meningkatkan algoritma trifid menjadi berdimensi delapan, tingkat difusi dan kesulitan yang dihasilkan menjadi berkali lipat. Belum lagi jumlah ruang enkripsi karakter yang juga bertambah banyak.

Implementasi yang digunakan dalam program di atas adalah blok cipher dengan panjang blok 8 bit. Karena dimensi kotak polibius pada implementasi oktofid adalah delapan juga, hal ini menyebabkan baris dan kolom pada langkah transpose bit-bit koordinat menjadi sama. Akibatnya transpose pada enkripsi dan dekripsi menjadi sama. Efeknya adalah skema enkripsi dan dekripsi yang ditunjukkan pada Gambar 10 menjadi identik sehingga fungsi enkripsi dan dekripsi blok menjadi sama. Hal ini sebenarnya bukan merupakan sebuah masalah karena sesuai prinsip Kerckhoffs algoritma ini akan diketahui publik juga. Hal ini justru memudahkan programmer

karena programmer tidak perlu membuat fungsi dekripsi yang berkebalikan dengan fungsi enkripsi. Tetapi jika tidak disukai, hal ini dapat diatasi dengan mengubah panjang blok menjadi bukan delapan.

Algoritma enkripsi yang dilakukan dengan menerapkan implementasi oktofid seperti dijelaskan diatas terbilang cukup menghabiskan performa. Alasannya adalah pada setiap pencarian koordinat dari sebuah karakter, dilakukan pencarian karakter secara sekuensial terhadap senarai berukuran 256 yang merepresentasikan kotak polibius oktobox. Peningkatan performa dapat dilakukan dengan membuat senarai kebalikan dari representasi kotak polibius oktobox tadi yang memetakan dari karakter ke posisi koordinat dalam kotak polibius. Dengan demikian, akses terhadap posisi tidak perlu dilakukan pencarian sekuensial tetapi bisa diakses secara langsung.

Penggunaan implementasi oktofid ini mungkin dapat menambah keamanan dibanding trifid cipher dan dapat memperluas aplikasi sehingga algoritmanya dapat digunakan untuk mengenkripsi berkas digital karena memperluas ruang enkripsinya menjadi 256 karakter. Akan tetapi, perluasan ruang enkripsi ini juga menjadi kelemahan dari implementasi ini. Hal ini disebabkan karena oktofid cipher mengandalkan **hanya** kotak polibius yang diperoleh dari masukan kunci. Padalah pada praktiknya, pengguna tidak pernah memasukkan kunci yang cukup panjang.

Lebih jauh lagi, untuk memaksimalkan penggunaan implementasi oktofid ini, kotak polibius yang dibangun mesti dibuat memiliki sekuens standar yang minimal. Artinya, masukan kunci dari pengguna haruslah sangat panjang, acak, dan unik. Padahal ruang enkripsi implementasi oktofid ini tidak hanya mengandung karakter alfanumerik tetapi juga karakter *extended* dan karakter tambahan lain. Hal ini menyebabkan kunci yang dimasukkan user tidak praktis. Belum lagi menyebutkan tidak adanya kibor yang memiliki fitur pengetikan ke-256 karakter pada set *encoding* ISO Latin 1.

Hal yang terakhir ini dapat diatasi dengan mendesain algoritma pembangkit kunci dari kunci berkarakter standar yang dimasukkan pengguna. Pembangkit kunci dapat didesain sedemikian rupa sehingga membangkitkan urutan karakter ISO Latin-1 untuk kotak polibius yang cukup acak. Pembangkit kunci juga dapat digunakan untuk memperkuat blok cipher dengan membangkitkan beberapa set kunci sehingga dalam enkripsi pada satu blok cipher bisa dilakukan perulangan enkripsi dengan *keyround* yang berbeda-beda selayaknya algoritma blok cipher modern saat ini.

VI. Perbandingan dengan Algoritma Lain

Dapat dilihat bahwa algoritma kriptografi klasik trifid cipher dapat dikembangkan menjadi sebuah algoritma yang masih menggunakan struktur yang sama tetapi memiliki karakteristik yang biasa dipakai pada algoritma kriptografi modern. Hal ini mungkin terjadi karena tidak ada batasan jumlah pada algoritma trifid cipher untuk memecah sebuah huruf menjadi komponen penyusun. Pada trifid cipher sendiri, sebuah huruf dipecah menjadi tiga komponen huruf berupa angka yang secara teori merepresentasikan koordinat huruf tersebut pada kubus polibius yang dibentuk sebagai kunci algoritma. Telah diusulkan bahwa besar kubus ini dapat diubah untuk memenuhi *encoding* karakter ASCII, Latin-1 atau *encoding* modern lain seperti Unicode yang sekarang dipakai di dunia komputer. Atau bahwkan ekspansi dimensi kotak polibius dapat memperbesar ruang karakter sebagai domain enkripsi ini. Telah disajikan pula bahwa ekspansi ke kotak polibius dimensi lima dan delapan adalah mungkin.

Jika dibandingkan dengan Playfair cipher jelas pengembangan trifid cipher yakni pada implementasi pentafid cipher dan oktofid cipher sangat berbeda. Playfai cipher merupakan algoritma kriptografi substitusi digrafik. Sedangkan implementasi pentafid cipher dan oktofid cipher dapat digolongkan sebagai algoritma kriptografi substitusi poligrafik, karena sebuah huruf bergantung pada banyak komponen lain, lima komponen bit pada pentafid dan delapan pada oktofid. Maka, algoritma pada pengembangan trifid ini tentu jauh lebih kuat dari algoritma kriptografi klasik seperti playfair cipher.

Jika dibandingkan dengan algoritma kriptografi modern saat ini, kedua implentasi bisa dibilang terlalu sederhana. Seperti pada implementasi pentafid dan oktofid, pada enkripsi setiap blok hanya digunakan kotak polibius sebagai acuan utama enkripsi. Pada algoritma kriptografi modern, misalkan AES, hal ini hanyalah merupakan satu dari langkah enkripsi yang dipakai.

Algoritma kriptografi bifid dan trifid serta pengembangan dan implentasinya yang disajikan pada makalah ini bisa dibilang merupakan algoritma substitusi (dan transposisi). Hal ini mungkin bisa disamakan dengan Substitusion Box pada algoritma kriptografi modern. Misalkan pada AES, SBox yang digunakan mirip seperti bifid cipher karena sebuah byte dipecah menjadi dua posisi pada Sbox.

Dengan kesederhanaan yang ada pada algoritma N-fid cipher ini, pengembangan tidak dapat digunakan begitu saja. Dibandingkan algoritma kriptografi modern lain hal ini tentu membuat N-fid cipher menjadi lemah. Jika ingin diaplikasikan, N-fid dapat dijadikan bagian atau langkah dari sebuah algoritma kriptografi modern lain.

VII. Paparan Hasil

Algoritma kriptografik klasik trifid cipher dapat dikembangkan menjadi algoritma kriptografi yang lebih kuat dengan memperbesar ukuran kubus polibius atau dimensi kotak polibius. Dengan memperbesar ukuran dimensi kotak polibius yang digunakan, pengembangan algoritma ini pun menjadi berkarakteristik seperti algoritma kriptografi modern. Hal ini menunjukkan bahwa sebuah algoritma kriptografi yang tergolong

algoritma klasik tidak bisa dilupakan begitu saja, karena masih ada peluang untuk mengembangkan algoritma tersebut.

Pengembangan algoritma trifid cipher ini juga dapat menggunakan mode-mode enkripsi pada blok cipher seperti algoritma kriptografi modern. Hal ini tentu merupakan hal yang hampir mustahil atau sulit dilakukan pada ranah kriptografi klasik. Otomatisasi komputer saat penghitungan (enkripsi dan dekripsi) memungkinkan hal ini.

Akan tetapi, pengembangan ini tidak begitu saja dapat menjadi praktikal. Pengembangan algoritma trifid cipher seperti yang telah ditunjukkan pada implementasi pentafid cipher dan oktofid cipher ini tidak terlalu praktikal. Penyebabnya adalah proses enkripsi yang digunakan pada kedua algoritma terlalu sederhana. Hal ini mungkin memudahkan serangan-serangan yang dipelajari pada kriptologi modern dan tentu saja *bruteforce* attack.

Penyebab lain adalah supaya lebih kuat, kedua implementasi mensyaratkan pengguna untuk memberi masukan kunci – yang akan digunakan untuk membangun kotak polibus – sepanjang mungkin dengan variasi huruf sebanyak mungkin. Belum lagi pada oktofid cipher ruang karakter yang digunakan pada enkripsi-dekripsi dan digunakan pada kotak polibius berjumlah 256 buah, seperti pada set *encoding* Latin-1. Pengguna tidak mungkin memasukkan puluhan karakter berbeda sebagai kuncinya, karena hal tersebut tidak manusiawi dan juga keterbatasan alat untuk memasukkan karakter-karakter tidak lazim (non-alfabet umum) tersebut.

Penyusunan kotak polibius masih sama dengan algoritma trifid atau bifid cipher. Artinya kunci dipecah per karakter dan karakter disusun ke kotak polibius dengan mengabaikan karakter yang telah dimasukkan ke kotak. Sisa karakter yang tidak ada dalam kunci ditulis secara berurut. Keserhanaan ini membuat penyerang dapat mengira-ngira kotak polibius yang digunakan. Belum lagi pada implementasi oktofid cipher pengguna tidak mungkin memasukkan kunci yang panjang sehingga sebagian besar karakter pada kotak polibius berada pada posisi *default*.

Pengembangan ini dapat dipakai sebagai bagian dari algoritma kriptografi modern yang lebih besar. Seperti pada AES, SBoxnya menggunakan difid cipher, pengembangan ini bisa saja dijadikan bagian dari SBox dari algoritma lain.

VIII. SIMPULAN

Algoritma kriptografi klasik dapat dipelajari kembali dan dikembangkan menjadi sesuatu yang baru. Trifid cipher contohnya dapat diekspansi menjadi algoritma kriptografi modern. Pengembangan dapat dipakai sebagai bagian dari algoritma kriptografi modern lain atau untuk pemakaian pribadi.

Ke-klasik-an sebuah algoritma kriptografi tidak menjadikannya tidak berharga untuk dipakai atau dipelajari ulang.

REFERENSI

http://en.wikipedia.org/wiki/Cryptography
http://www.quadibloc.com/crypto/pp1322.htm
http://en.wikipedia.org/wiki/Baudot_code

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, 23 Maret 2011

M. Albadr Lutan Nasution
13508011