Studi & Analisis Mengenai Felix Cipher Serta Modifikasinya Menggunakan Teknik – Teknik Transposisi

Andreas Parry Lietara ~ NIM 13506076
Jurusan Teknik Informatika ITB, Bandung, email : andreas.parry@gmail.com

Abstract *– Makalah ini akan membahas mengenai salah satu algoritma kriptografi klasik yang tergolong pencil and paper cipher, yaitu Felix Cipher. Felix Cipher termasuk salah satu algoritma kriptografi yang sederhana dan mudah dipelajari serta diterapkan oleh orang yang masih awam terhadap kriptografi. Dalam makalah ini akan dibahas mengenai konsep dasar penerapan algoritma Felix Cipher serta kelebihan dan kekurangannya. Selain itu pada makalah ini juga akan dibahas teknik – teknik yang dapat meningkatkan tingkat keamanan dari Felix Cipher. Selain itu, dalam pengembangan Felix Cipher yang dijelaskan makalah ini juga akan dipakai beberapa prinsip kerja metoda enkripsi modern (CBC dan CFB).*

Kata Kunci*: Felix Cipher, polyabus key, columnar transposition, myszkowski transposition, cipher block, Felix Cipher ++*

1. PENDAHULUAN

Informasi merupakan salah satu aspek penting dalam kehidupan di era modern ini. Segala pihak dari berbagai kalangan, baik itu dalam skala kecil (keluarga / individu), menengah (perusahaan / organisasi) dan besar (negara) sangat membutuhkan informasi. Namun adakalanya informasi itu menjadi sebuah rahasia yang tidak boleh diketahui oleh pihak lain sehingga diperlukan suatu cara untuk menyembunyikan informasi tersebut. Untuk memenuhi kebutuhan tersebutlah cabang ilmu kriptografi muncul.

Kriptografi merupakan cabang ilmu yang mempelajari cara penyembunyian pesan [1]. Di zaman modern ini, kriptografi telah memanfaatkan teknologi komputer untuk membantu dalam proses penyembunyian pesan, dengan bantuan komputer banyak sekali algoritma – algoritma kriptografi yang rumit dan menjamin keamanan pesan (contohnya berbagai algoritma *cipher block* seperti DES, GOST, RC5 dan AES). Namun bukan berarti algoritma – algoritma yang rumit itu yang selalu digunakan, sebab biasanya pemilihan algoritma (dari sisi rumit / tidak) dikaitkan dengan tingkat kepentingan dari pesan yang bersangkutan. Tentunya seorang laki – laki yang ingin mengenkripsikan surat cinta untuk kekasihnya tidak akan menggunakan algoritma kriptografi yang sama dengan yang digunakan oleh pihak kepolisian nasional.

Felix Cipher merupakan salah satu algoritma kiptografi sederhana yang tergolong dalam *pencil and paper cipher*. Walaupun sederhana dan mudah dipelajari, tampaknya *Felix Cipher* masih "kalah pamor" dibandingkan dengan algoritma *pencil and paper cipher* lainnya. Oleh karena itu, pada makalah ini penulis hendak memperkenalkan algoritma *Felix Cipher* dan melakukan modifikasi terhadap algoritma tersebut untuk meningkatkan keamanannya.

2. LANDASAN TEORI

2.1. Felix Cipher

Felix Cipher adalah algoritma enkripsi yang tergolong dalam *pencil and paper cipher*. Tidak seperti algoritma enkripsi modern, algoritma enkripsi yang termasuk golongan ini tidak sampai memerlukan bantuan komputer dalam aplikasinya. Bahkan, dalam penerapannya kita bisa hanya menggunakan kertas dan pensil saja, tentu saja komputer masih bisa digunakan untuk lebih mempermudah proses enkripsinya.

Algoritma Felix Cipher termasuk algoritma enkripsi *fractionate*, yaitu algoritma enkripsi yang memecah – mecah plainteks menjadi elemen – elemen (dalam kasus ini berupa dua bilangan yang melambangkan baris dan kolom letak karakter tersebut dalam *polyabus key*). Pada dasarnya Felix Cipher merupakan variasi dari algoritma enkripsi lainnya yaitu Bifid Cipher. Bifid Cipher dikembangkan pada tahun 1901 oleh Felix Marie Delastelle. Berikut adalah langkah – langkah enkripsi Felix Cipher [4] [5]:

1. Membuat sebuah matriks kunci (*polyabus key*) berukuran 6 x 6 yang kemudian diisi dengan bilangan alfanumerik (alfabet a-z dan angka 0 - 9). Pada langkah inilah Felix Cipher berbeda dengan Bifid Cipher (pada Bifid Cipher yang digunakan adalah matriks kunci 5 x 5).
2. Menentukan panjang periode enkripsi. Plainteks tidak dienkripsi sekaligus, tetapi dienkripsi dalam kelompok – kelompok kecil, periode yang dimaksud adalah jumlah huruf yang akan dienkripsi dalam 1 kelompok.
3. Melakukan substitusi karakter plainteks (dalam tiap kelompok) menjadi bilangan berdasarkan koordinat pada *polyabus key* (baris - kolom).
4. Melakukan transposisi horizontal terhadap bilangan – bilangan yang didapat dari langkah 3.
5. Substitusi bilangan – bilangan menjadi karakter cipherteks berdasarkan koordinat pada *polyabus key*.

2.2. Penggunaan Felix Cipher

Untuk memperlihatkan secara jelas cara kerja dari Felix Cipher, berikut ini akan diberikan contoh penggunaannya. Misalkan, kita ingin mengenkripsikan kata – kata "MAKALAH". Maka langkah – langkah yang kita lakukan :

1. Menyiapkan *polyabus key*. *Polyabus key* dapat disiapkan secara acak atau menggunakan kunci. Jika dengan kunci, maka kuncinya harus alfanumerik dan tidak boleh ada karakter yang berulang. Kunci yang telah disiapkan dituliskan terlebih dahulu dalam matriks dari indeks kiri atas (1,1), setelah itu diikuti dengan urutan alfabet yang belum dimasukkan dan angka. Pada contoh kali ini akan digunakan *polyabus key* yang acak.

Tabel 1. *Polyabus Key*

	1	**2**	**3**	**4**	**5**	**6**
1	a	s	d	f	2	h
2	j	k	l	1	g	3
3	q	w	e	4	R	t
4	5	y	u	8	I	o
5	7	p	z	x	9	c
6	v	b	6	n	M	0

2. Periode yang akan digunakan pada contoh ini adalah 7. Sehingga hanya ada 1 kelompok plainteks yang akan dienkripsi yaitu kata "MAKALAH"
3. Melakukan substitusi terhadap tiap karakter plainteks.

Tabel 2. Substitusi Plainteks ke Bilangan

	M	**A**	**K**	**A**	**L**	**A**	**H**
brs	6	1	2	1	2	1	1
klm	5	1	2	1	3	1	6

4. Melakukan transposisi horizontal, berikut adalah ilustrasinya :

```
    M A K A L A H       M A K A L A H
brs 6 1 2 1 2 1 1   klm 5 1 2 1 3 1 6
hsl 61 21 21 15 12 13 16
```

Gambar 1. Transposisi Horizontal

5. Mensubstitusikan kembali bilangan – bilangan dengan karakter cipherteks berdasarkan matriks kunci :

Tabel 3. Substitusi ke Cipherteks

bilangan	**61**	**21**	**21**	**15**	**12**	**13**	**16**
cipher	v	j	j	2	s	d	h

6. Diperoleh cipher teks : "V J J 2 S D H"

Untuk melakukan dekripsi cipherteks, kita memerlukan matriks kunci yang digunakan untuk melakukan enkripsi. Proses dekripsi dilakukan dengan membalikkan proses enkripsi.

2.3. Berbagai Metoda Transposisi

Pada makalah ini akan diberikan beberapa penggunaan dari Felix Cipher yang dikombinasikan dengan berbagai metoda transposisi untuk meningkatkan keamanannya. Transposisi adalah teknik enkripsi dengan mengubah letak huruf – huruf plainteks. Pada upabab ini akan dibahas beberapa metoda transposisi yang akan digunakan.

1. *Columnar transposition* [2]

   Pada *columnar transposition*, kriptografer menggunakan sebuah kata kunci untuk melakukan transposisi, berikut adalah contoh pemakaiannya. Misal, kata kunci yang digunakan adalah "SIMBOL" dan plainteks yang digunakan adalah "MAKALAH KRIPTOGRAFI". Pertama – tama kita memberikan urutan kepada tiap huruf pada kata kunci sesuai dengan kemunculannya pada alfabet, jika ada huruf yang sama maka urutan ditentukan dari yang paling kiri.

Tabel 4. Pengurutan Kata Kunci

S	**I**	**M**	**B**	**O**	**L**
6	2	4	1	5	3

   Setelah itu, tuliskan plainteks di bawah kata kunci pada n kolom dengan n adalah jumlah huruf pada kata kunci.

Tabel 5. Proses *Columnar Transposition*

S	**I**	**M**	**B**	**O**	**L**
M	A	K	A	L	A
H	K	R	I	P	T
O	G	R	A	F	I

   Untuk memperoleh cipherteks, kita membaca plainteks mulai dari kolom pertama (sesuai pengurutan kata kunci) secara vertikal dilanjutkan dengan kolom – kolom selanjutnya. Sehingga pada contoh di atas didapatkan cipherteks hasil enkripsi "AIAAKGATIKRRLPFMHO".

   Metoda *columnar transposition* memiliki sebuah kelemahan, di mana seorang kriptanalis bisa saja menebak – nebak panjang kunci dan mencoba menuliskan cipherteks pada kolom – kolom matriks kunci sehingga ditemukan sebuah plainteks yang bermakna. Untuk itu sebuah variasi dari *columnar transposition*, yang diperkenalkan di buku karangan General Luigi Sacco, dapat digunakan untuk memberikan tingkat keamanan yang lebih terjamin (selain itu biasanya digunakan metoda *double transposition* di mana metoda *columnar transposition* dilakukan dua kali). Berikut

adalah contoh penggunaannya :

Tabel 6. Variasi *Columnar Transposition*

S	I	M	B	O	L
M	A	K	A		
L	A				
H	K	R	I	P	T
O	G	R	A	F	
I					

Pada variasi *columnar transposition* ini, setiap baris ke n diisi sampai kolom dengan urutan ke n. Setelah itu, cipherteks diperoleh dengan cara yang sama dengan *columnar transposition* biasa. Pada contoh ini, cipherteksnya adalah "AIAAAKGTKRRPFMLHOI". Untuk plainteks yang panjangnya lebih dari 1 + 2 + 3 + … + n dengan n adalah jumlah karakter kunci, maka penulisan plainteks berulang kembali ke kolom urutan pertama.

2. *Myszkowski transposition* [3]
   Metoda ini juga merupakan salah satu variasi dari *columnar transposition*. Perbedaannya, pada metoda ini diperlukan kunci yang mengandung huruf yang berulang. Setiap kolom dengan urutan yang sama akan dibaca secara horizontal sebelum secara vertikal. Berikut adalah contoh aplikasinya untuk kata kunci "PASCAL" dan plainteks "MAKALAH KRIPTOGRAFI" :

Tabel 7. Contoh Myszkowski transposition

4	1	5	2	1	3
P	**A**	**S**	**C**	**A**	**L**
M	A	K	A	L	A
H	K	R	I	P	T
O	G	R	A	F	I

Dengan *myszkowski transposition* diperoleh cipherteks
"AAALKPGFCAIALATIPMHOSKRR".

3. HASIL DAN PEMBAHASAN

3.1. Kelebihan dan Kekurangan Felix Cipher

Felix Cipher memiliki beberapa kelebihan, yakni kemudahannya untuk dipelajari, baik itu bagi kriptografer pemula maupun orang awam sekalipun. Selain itu, enkripsi dengan Felix Cipher juga tidak bisa dipecahkan dengan analisis frekuensi biasa, mengingat pada Felix Cipher transposisi terjadi pada bilangan – bilangan yang menjadi penanda karakter, sehingga jumlah suatu karakter pada plainteks tidak mungkin sama dengan jumlah karakter hasil enkripsinya pada cipherteks, sehingga Felix Cipher masih termasuk sulit dipecahkan oleh orang awam yang bukan ahli. Namun, Felix Cipher oleh para ahli telah dapat dipecahkan dengan menggunakan perhitungan – perhitungan statistik (metoda kriptanalisisnya tidak dibahas pada makalah ini), sehingga besar kemungkinannya informasi yang bersangkutan dapat bocor, sehingga metoda enkripsi ini tidak dapat diterapkan untuk informasi – informasi yang sangat penting. Selain itu metoda ini hanya bisa mengenkripsikan pesan – pesan alfanumerik.

3.2. Pengembangan Felix Cipher

Pada makalah ini, penulis hendak menyampaikan salah satu ide penulis untuk meningkatkan keamanan dari Felix Cipher. Adapun metoda yang diusulkan penulis memanfaatkan metoda – metoda transposisi yang telah dijelaskan pada bab sebelumnya dan prinsip enkripsi dari kriptografi modern, seperti pada metoda *cipher block* (CBC dan CFB). Prinsip yang diambil dari algoritma enkripsi *cipher block* (CBC dan CFB) adalah prinsip enkripsi berantai.

Seperti yang kita ketahui, pada algoritma enkripsi CBC dan CFB, plainteks dibagi menjadi beberapa blok dan proses enkripsi dilakukan per blok. Hasil enkripsi dari blok yang lebih dulu dienkripsi akan mempengaruhi hasil enkripsi blok berikutnya. Pada Felix Cipher proses enkripsi juga dibagi menjadi beberapa kali (sebanyak panjang plainteks dibagi panjang periode), oleh karena kemiripan ini maka pada Felix Cipher juga dapat diterapkan prinsip enkripsi berantai. Untuk mempermudah penyebutan, untuk selanjutnya algoritma enkripsi yang baru ini akan penulis sebut sebagai algoritma Felix Cipher ++.

3.3. Ide Dasar Pengembangan

Pada algoritma Felix Cipher murni, cipherteks hasil enkripsinya masih mengandung informasi mengenai matriks kuncinya (*polyabus key*). Misalkan saja sebuah plainteks $P_1P_2P_3P_4P_5$ dienkripsi menjadi cipherteks $C_1C_2C_3C_4C_5$, maka dapat diperoleh informasi seperti tampak pada tabel berikut

Tabel 8. Pola Informasi Pada Cipherteks Felix Cipher

$P_1b = C_1b$	$P_1k = C_3k$
$P_2b = C_1k$	$P_2k = C_4b$
$P_3b = C_2b$	$P_3k = C_4k$
$P_4b = C_2k$	$P_4k = C_5b$
$P_5b = C_3b$	$P_5k= C_5k$

Keterangan :

- P_1b maksudnya elemen baris dari karakter P_1.
- P_1k maksudnya elemen kolom dari karakter P_1.

Informasi – informasi ini yang biasanya dieksploitasi oleh para kriptanalis untuk memecahkan Felix Cipher. Untuk itu penulis mempunyai ide untuk mengacak urutan cipherteks hasil enkripsi Felix Cipher dengan menggunakan metoda – metoda transposisi. Dengan demikian cipherteks akhir yang akan diperoleh tidak dapat memberikan informasi kepada para kriptanalis jika tidak berada dalam susunan yang benar.

Selain itu, bentuk proses enkripsi yang mirip dengan

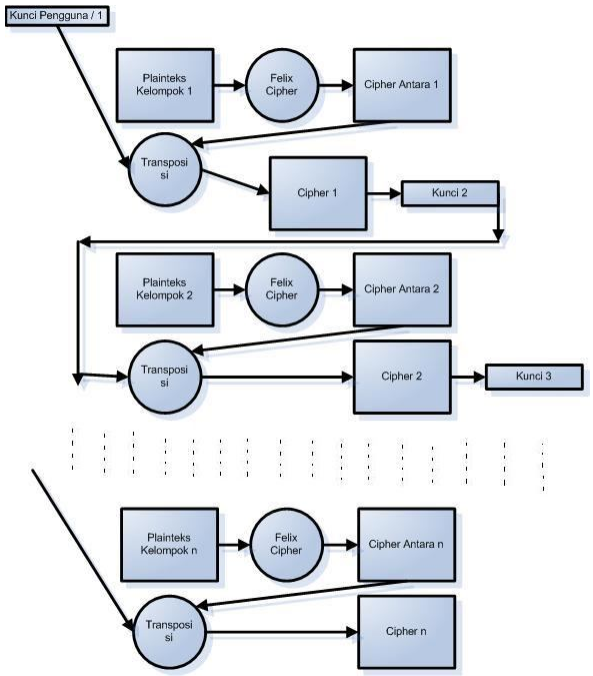
algoritma *cipher block* memberikan ide kepada penulis untuk memperumit proses transposisi yang dilakukan dengan enkripsi berantai. Berantai yang dimaksud di sini adalah perubahan kunci yang digunakan dalam melakukan proses transposisi. Untuk transposisi awal (paling pertama) digunakan kunci masukan dari pengguna, sementara kunci untuk transposisi selanjutnya dibangkitkan dari hasil enkripsi kelompok yang dienkripsi sebelumnya (sehingga untuk proses dekripsi kunci dapat dibangkitkan dari cipherteks).

3.4. Algoritma Felix Cipher ++

Berikut adalah langkah – langkah algoritma Felix Cipher baru yang dikembangkan oleh penulis :

1. Menyiapkan sebuah *polyabus key* yang akan digunakan untuk melakukan proses Felix Cipher.
2. Menentukan periode Felix Cipher yang akan digunakan.
3. Menyiapkan kunci yang akan digunakan untuk transposisi pertama. Panjang kunci bergantung pada panjang periode (sebab panjang periode merupakan panjang plainteks yang akan ditransposisi), panjang kunci lebih baik tidak sampai setengah dari panjang periode.
4. Membagi – bagi plainteks menjadi kelompok – kelompok berdasarkan panjang periode. Jika panjang kelompok terakhir tidak sama dengan periode, dapat dilakukan *padding* (penambahan karakter).
5. Untuk setiap kelompok :
    a. Enkripsi plainteks dengan *polyabus key*
    b. Gunakan kunci yang diperoleh dari enkripsi sebelumnya (untuk kelompok pertama dari masukan user) untuk melakukan transposisi. Hasil transposisi adalah cipherteks untuk kelompok tersebut.
    c. Gunakan hasil enkripsi kelompok ini untuk membangkitkan kunci transposisi kelompok berikutnya (kecuali untuk kelompok terakhir).

Berikut adalah diagram cara kerja algoritma Felix Cipher ++ :



Gambar 2. Diagram Kerja Felix Cipher ++

3.5. Penggunaan Felix Cipher ++

Berikut ini akan diberikan contoh penggunaan algoritma ini. Misalkan saja, kita akan mengenkripsikan pesan “BELAJAR KRIPTOGRAFI MENYENANGKAN”. Periode yang akan digunakan adalah 9, panjang kunci untuk transposisi adalah 4, kunci masukan user adalah “STEI” dan *polyabus key* yang digunakan adalah :

Tabel 9. *Polyabus Key* Pada Contoh Kasus

	1	**2**	**3**	**4**	**5**	**6**
1	f	p	w	e	2	o
2	t	k	1	u	x	3
3	m	a	4	z	n	d
4	0	y	j	s	7	8
5	g	v	5	6	b	h
6	l	c	q	i	r	9

Langkah selanjutnya adalah membagi plainteks menjadi kelompok – kelompok, pada contoh ini plainteks dibagi menjadi 4 kelompok, dimana :

1. Kelompok 1 : “BELAJARKR”.
2. Kelompok 2 : “IPTOGRAFI”
3. Kelompok 3 : “MENYENANG”
4. Kelompok 4 : “KANXXXXXX” (*padding* dilakukan untuk kelompok terakhir yang panjangnya belum sama dengan periode).

Selanjutnya kita akan melakukan enkripsi tiap kelompok, dimulai dari kelompok 1

.

Tabel 10. Substitusi Kelompok 1

	B	**E**	**L**	**A**	**J**	**A**	**R**	**K**	**R**
baris	5	1	6	3	4	3	6	2	6
kolom	5	4	1	2	3	2	5	2	5

Tabel 11. Transposisi Bilangan Kelompok 1

Cipher	**51**	**63**	**43**	**62**	**65**	**41**	**23**	**25**	**25**
	g	q	j	c	r	0	1	x	x

Sehingga didapat cipher sementara “GQJCR01XX”. Selanjutnya dilakukan transposisi terhadap cipher sementara yang diperoleh dengan menggunakan kunci “STEI”. Adapun metoda transposisi yang akan digunakan pada kasus ini adalah variasi *columnar transposition* yang telah dijelaskan di bab sebelumnya (pemilihan metoda transposisi dapat disesuaikan)

Tabel 12. Transposisi Cipher Kelompok 1

3	4	1	2
S	**T**	**E**	**I**
G	Q	J	
C	R	0	1
X			
X			

.Diperoleh cipherteks untuk kelompok 1 adalah “J01GCXXQR”. Dari hasil enkripsi ini kita bangkitkan kunci untuk fungsi transposisi kelompok berikutnya, adapun cara membangkitkannya adalah dengan mengambil 2 karakter awal dan dua karakter akhir (karakter ke – 1, 2, 8 dan 9), sehingga pada kasus ini diperoleh hasil kunci J0QR (Pemilihan cara pembangkitan kunci dapat bervariasi sesuai dengan panjang kunci yang dibutuhkan).

Selanjutnya dilakukan enkripsi kelompok 2.

Tabel 13. Substitusi Kelompok 2

	I	**P**	**T**	**O**	**G**	**R**	**A**	**F**	**I**
baris	6	1	2	1	5	6	3	1	6
kolom	4	2	1	6	1	5	2	1	4

Tabel 14. Transposisi Bilangan Kelompok 2

cipher	**61**	**21**	**56**	**31**	**64**	**21**	**61**	**52**	**14**
	L	T	H	M	I	T	L	V	E

Sehingga diperoleh cipher sementara “LTHMITLVE”. Setelah itu dilakukan transposisi dengan kunci “J0QR”.

Tabel 15. Transposisi Cipher Kelompok 2

1	4	2	3
J	**0**	**Q**	**R**
L			
T	H	M	
I	T	L	V
E			

Diperoleh hasil enkripsi kelompok 2 adalah “LTIEMLVHT” (perhatikan bahwa dalam penetapan urutan kolom numerik dianggap lebih akhir daripada alfabet).
Dari hasil enkripsi ini kita bangkitkan kunci untuk fungsi transposisi kelompok plainteks berikutnya, diperoleh kunci “LTHT” (2 karakter awal dan 2 karakter akhir cipherteks kelompok sekarang).

Pada kelompok ke 3 juga dilakukan proses yang sama.

Tabel 16. Substitusi Kelompok 3

	M	**E**	**N**	**Y**	**E**	**N**	**A**	**N**	**G**
baris	3	1	3	4	1	3	3	3	5
kolom	1	4	5	2	4	5	2	5	1

Tabel 17. Transposisi Bilangan Kelompok 3

cipher	**31**	**34**	**13**	**33**	**51**	**45**	**24**	**52**	**51**
	M	Z	W	4	G	7	U	V	G

Cipher sementara yang diperoleh : MZW4G7UVG

Tabel 18. Transposisi Cipher Kelompok 3

2	3	1	4
L	**T**	**H**	**T**
M	Z	W	
4			
G	7		
U	V	G	

Cipherteks untuk kelompok 3 adalah “WGM4GUZ7V”. Sementara kunci yang dibangkitkan untuk kelompok 4 adalah “WG7V”.

Proses enkripsi kelompok 4 plainteks :

Tabel 19. Substitusi Kelompok 4

	K	**A**	**N**	**X**	**X**	**X**	**X**	**X**	**X**
baris	2	3	3	2	2	2	2	2	2
kolom	2	2	5	5	5	5	5	5	5

Tabel 20. Transposisi Bilangan Kelompok 4

cipher	**23**	**32**	**22**	**22**	**22**	**25**	**55**	**55**	**55**
	1	A	K	K	K	X	B	B	B

Cipher sementara yang diperoleh “1AKKKXBBB”.

Tabel 21. Transposisi Cipher Kelompok 4

3	1	4	2
W	**G**	**7**	**V**
1	A		
K	K	K	X
B			
B	B		

Hasil enkripsi kelompok 4 : “AKBX1KBBK” (tidak diperlukan lagi pembangkitan kunci transposisi).

Sehingga plainteks “BELAJAR KRIPTOGRAFI MENYENANGKAN” dienkripsikan menjadi cipherteks “J01GCXXQR LTIEMLVHT WGM4GUZ7V AKBX1KBBK”.

3.6. Proses Dekripsi Felix Cipher ++

Sama seperti pada algoritma Felix Cipher biasa, proses dekripsi dilakukan dengan membalik proses enkripsi, berikut adalah langkah – langkah dekripsi Felix Cipher ++ :

1. Mulai dari kelompok paling akhir (ambil n buah karakter terakhir dengan n adalah periode enkripsi), sebutlah kelompok a.
2. Tentukan kunci matriks transposisi dari kelompok sebelumnya (kelompok a - 1) dengan mengambil 2 karakter awal dan akhir.
3. Dengan kunci yang didapat dari langkah 2, ubah urutan dari cipherteks kelompok tersebut.
4. Dari cipherteks hasil langkah 3, gunakan *polyabus key* untuk melakukan dekripsi seperti pada Felix Cipher biasa.
5. Ulangi langkah 1 sampai 4 untuk kelompok a-1

3.7. Keunggulan Algoritma Felix Cipher ++

Algoritma Felix Cipher ++ berhasil menghilangkan informasi yang terkandung dalam cipherteks Felix Cipher biasa dengan melakukan transposisi terhadap cipherteks hasil enkripsi Felix Cipher biasa. Sebenarnya Felix Cipher sendiri sudah merupakan algoritma enkripsi yang cukup kuat karena termasuk algoritma enkripsi *fractionate*, dengan ditambah metoda transposisi dengan kunci yang berantai, algoritma Felix Cipher ++ menjadi sangat sulit dipecahkan, apalagi jika kriptanalis yang hendak memecahkannya tidak mengetahui algoritma enkripsi yang digunakan.

4. KESIMPULAN

Berdasarkan pembahasan di atas dapat diambil kesimpulan :

1. Algoritma Felix Cipher merupakan algoritma enkripsi yang sederhana dan cukup kuat untuk digunakan dalam keperluan – keperluan pribadi
2. Algoritma Felix Cipher masih memiliki kelemahan – kelemahan yang dapat dieksploitasi oleh para ahli, sehingga algoritma ini tidak baik digunakan untuk pengiriman pesan yang memerlukan tingkat keamanan yang tinggi.
3. Algoritma Felix Cipher dapat dikembangkan dengan melakukan transposisi cipherteksnya untuk menghilangkan informasi – informasi mengenai *polyabus key* yang digunakan dalam proses enkripsi.
4. Proses enkripsi Felix Cipher yang melakukan enkripsi plainteks secara terpisah (berkelompok) memungkinkan penggunaan prinsip enkripsi kriptografi modern (*cipher block*).
5. Felix Cipher ++ merupakan algoritma enkripsi yang dikembangkan dari algoritma Felix Cipher dengan menggunakan metoda transposisi dan prinsip enkripsi *cipher block* (di mana hasil enkripsi satu kelompok mempengaruhi hasil enkripsi)
6. Algoritma Felix Cipher ++ mampu meningkatkan keamanan dari metoda Felix Cipher.

DAFTAR PUSTAKA

[1] R. Munir, "*Diktat Kuliah IF5054 Kriptografi*". Program Studi Teknik Informatika, Institut Teknologi Bandung, 2006.

[2] John Savard's Homepage. http://www.quadibloc.com/crypto/pp0102.htm
Waktu akses : 12 Maret 2009 pukul 16.00

[3]http://www.absoluteastronomy.com/topics/Transposition_cipher
Waktu akses : 1 April 2009 pukul 20.00

[4] http://www.zenosys.com/notes/felix.html
Waktu akses : 12 Maret 2009 pukul 21.00

[5] Classical Cryptography Course by Lanaki, lecture 17.
http://www.und.edu/org/crypto/crypto/lanaki.crypt.class/lessons/
Waktu akses : 30 Maret 2009 pukul 12.00

[6] M. Antonio, R. Rogerio. "*Automated Ciphertext-Only Cryptanalysis of the Bifid Cipher*".
http://www.fc.up.pt/cmup/v2/include/filedb.php?id=120&table=publicacoes&field=file
Waktu akses : 1 Maret 2009 pukul 13.00