Super-Playfair, Sebuah Algoritma Varian Playfair Cipher dan Super Enkripsi

Gahayu Handari Ekaputri [1)]

1) Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung
Jl.Ganesa 10 Bandung, Indonesia. Email: if14031@students.if.itb.ac.id

.

Abstract – *Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan. Algoritma kriptografi klasik merupakan algoritma penyandian yang sudah ada sebelum zaman digital, dan yang termasuk dalam sistem kriptografi simetri adalah algoritma yang memiliki kunci yang sama dalam melakukan enkripsi dan dekripsi. Algoritma klasik pada dasarnya hanya terdiri dari Cipher substitusi dan Cipher transposisi. Playfair Cipher dan Super Enkripsi merupakan contoh dari algoritma kriptogradi klasik.*

Makalah ini membahas tentang algoritma Super-Playfair. Algoritma Super-Playfair adalah sebuah varian dari algoritma Playfair Cipher dengan merubah aturan kubus yang 5x5 yang terkandung di dalamnya, untuk kemudian dilakukan Super Enkripsi. Super Enkripsi sendiri adalah melakukan enkripsi mula-mula dengan Cipher substitusi sederhana (Cipher abjad-tunggal), lalu hasilnya dienkripsi lagi dengan Cipher transposisi. Proses modifikasi terhadap Playfair Cipher diharapkan dapat memperkuat algoritma ini.

Kajian tentang algoritma Super-Playfair ini meliputi proses enkripsi, dan dekripsi yang dilakukan. Proses Kriptanalisis yang mungkin dilakukan untuk memecahkan algoritma ini. Pengujian dari algoritma Super-Playfair ini, yang dapat menyimpulkan hal-hal yang menjadi kekuatan dan kelemahan algoritma ini.

Kata Kunci*: enkripsi, dekripsi, Playfair Cipher, Super Enkripsi, Super-Playfair*

1. PENDAHULUAN

Dunia berkembang kian cepat seiring majunya teknologi informasi. Komunikasi kini menjadi tidak terbatas. Dengan banyaknya kemudahan untuk melakukan pengaksesan informasi, adakalanya diperlukan pengamanan akan akses informasi tersebut. Pengamanan ini berfungsi untuk melakukan pencegahan atas sampainya informasi ke tangan yang tidak berhak. Banyak sekali metode pengamanan yang dilakukan untuk menjaga komunikasi yang baik, seperti dengan pemberian sandi lewat, penyandian isi pesan dan metode lainnya untuk memperkuat keamanan.

Pengiriman data dan penyimpanan data melalui media elektronik memerlukan suatu proses yang dapat menjamin keamanan dan keutuhan dari data yang dikirimkan tersebut. Data tersebut harus tetap rahasia selama pengiriman dan harus tetap utuh pada saat penerimaan di tujuan. Untuk memenuhi hal tersebut, dilakukan proses penyandian terhadap data yang akan dikirimkan.

Proses penyandian yang dilakukan adalah dengan menggunakan kriptografi. Kriptografi merupakan seni untuk menyembunyikan pesan. Kriptografi melingkupi proses transformasi informasi menjadi suatu bentuk yang tidak dapat dipahami, sehingga orang-orang yang tidak berhak tidak mungkin mengerti. Transformasi ini harus berlangsung dengan dua arah, sehingga orangyang bermaksud membaca informasi tersebut dapat mengerti makna dari bentukan transformasi. [2]

Proses transformasi tersebut terdiri dari enkripsi dan dekripsi. Enkripsi dilakukan pada saat pengiriman dengan cara mengubah data asli menjadi data rahasia sedangkan dekripsi dilakukan pada saat penerimaan dengan cara mengubah data rahasia menjadi data asli. Jadi data yang dikirimkan selama proses pengiriman adalah data rahasia, sehingga data asli tidak dapat diketahui oleh pihak yang tidak berkepentingan. Data asli hanya dapat diketahui oleh penerima dengan menggunakan kunci rahasia.

Algoritma kriptografi klasik pada dasarnya terdiri dari cipher substitusi dan cipher transposisi, dimana kunci untuk enkripsi dan dekripsinya sama. Banyak sekali contoh algoritma kriptografi klasik seperti Caesar Cipher, Vigenere Cipher,, dan Playfair Chipher. Namun, algoritma-algoritma tersebut masih rentan terhadap serangan dan memiliki banyak kelemahan. Algoritma kriptografi klasik pada umumnya dapat dikalahkan dengan melakukan metode analisis frekuensi ataupun teknik terkaan. Dengan kelemahan inilah yang melahirkan lahirnya algoritma kriptografi modern.

Walaupun banyak kelemahan dari algoritma kriptografi klasik, namun kriptografi klasik dapat dijadikan sebagai sumber pemahaman konsep dasar kriptografi, dan dari kelemahan-kelamahan itulah didapat suatu algoritma baru yang lebih aman terhadap serangan-serangan yang ada.

2. LANDASAN TEORI KRIPTOGRAFI

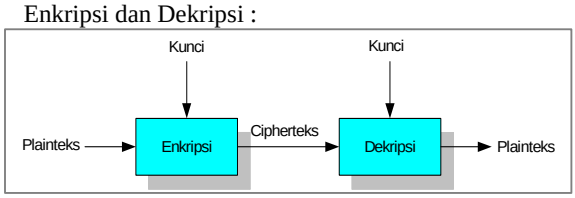
2.1. Kriptografi secara Umum

Kriptografi pada awalnya merupakan ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Kemudian seiring dengan berkembangnya kriptografi yaitu kriptografi tidak lagi sebatas mengenkripsikan pesan, tetapi juga memberikan aspek keamanan yang lain seperti serangan dari kriptanalisis. Karena itu pengertian kriptografi pun berubah menjadi ilmu sekaligus seni untuk menjaga keamanan pesan.

Kriptografi selain menyandikan pesan juga menyediakan beberapa aspek keamanan. Berikut aspek keamanan kriptografi :

1. Kerahasiaan (confidentiality), layanan yang digunakan untuk menjaga isi pesan dari siapapun yang tidak berhak untuk membacanya.
2. Integritas data (*data integrity*), layanan yang menjamin bahwa pesan masih asli/utuh atau belum pernah dimanipulasi selama pengiriman.
3. Otentikasi (*authentication*), layanan yang untuk mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication*) dan untuk mengidentifikasi kebenaran sumber pesan (*data origin authentication*).
4. Nirpenyangkalan (*non-repudiation*), layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

Proses menyandikan plainteks menjadi cipherteks disebut dengan Enkripsi. Sementara proses mengembalikan cipherteks menjadi plainteks semula disebut dedngan Dekripsi. Kunci adalah parameter yang digunakan untuk transformasi dekripsi dan enkripsi. Berikut adalah gambaran tentang hubungan Enkripsi dan Dekripsi :



Gambar1 Gambaran Enkripsi dan Dekripsi

Fungsi enkripsi E memetakan P ke C, $E(P) = C$
Fungsi dekripsi D memetakan C ke P, $D(C) = P$
Dengan demikian, fgngsi enkripsi dan dekripsi harus memenuhi sifat: $D(E(P)) = P$ [1]

2.2. Algoritma Kriptografi Klasik

Algoritma kriptografi klasik merupakan algoritma yang sudah digunakan sejak dulu kala, dan merupakan cikal bakal tumbuhnya algoritma kritografi modern. Kriptografi klasik merupakan algoritma yang berbasis karakter, dan termasuk ke dalam kriptografi kunci-simetri. Algoritma kunci simetri bermakna bahwa kunci yang digunakan untuk melakukan proses enkripsi sama dengan kunci untuk dekripsi.

Secara umum, algoritma kriptografi klasik melingkupi kedua jenis pengolahan cipher berikut:

1. *Cipher* Substitusi (*Substitution Ciphers*), menggantikan karakter di plainteks dengan karakter lain untuk cipher teks.
2. *Cipher* Transposisi (*Transposition Ciphers*), merubah urutan plainteks.

Algoritma kriptografi klasik tetap masih penting peranannya karena algoritma kriptografi klasik merupakan landasan dasar algoritma kriptografi modern, seperti operasi substitusi dan transposisi, hanya saja algoritma modern berada pada operasi bit per bit, bukan operasi karakter.

2.3. Algoritma Playfair Cipher

Playfair Cipher ditemukan oleh Sir Charles Wheatstone (1802-1875) pada tahun 1854, dan dipopulerkan oleh Baron Lyon Playfair (1819-1898), yang namanya diabadikan untuk algoritma ini. Meskipun algoritma Playfair ini sudah tidak aman untuk kegunaan dunia saat ini, Playfair cipher banyak digunakan dan cukup efektif pada jamannya. Playfair cipher pertama kali digunakan oleh tentara Inggris pada perang Boer dan masih digunakan pada Perang Dunia I. [3]

Playfair Cipher merupakan suatu algoritma kriptografi klasik yang termasuk ke dalam *polygram cipher*, dimana plainteks diubah menjadi bentuk poligram dan proses enkripsi dekripsi dilakukan untuk poligram tersebut. Kunci kriptografinya adalah 25 buah huruf yang disusun di dalam bujursangkat 5x5 dengan menghilangkan huruf J dari abjad.[2] Kemungkinan kuncinya adalah 25!. Susunan kunci di dalam bujursangkar diperluas dengan menambahkan kolom keenam dan baris keenam. Basis keenam merupakan baris pertama, sementara kolom keenam berisi kolom pertama. Pada umumnya, kunci yang digunakan adalah serangkaian kata yang mudah dimengerti.

Pesan yang akan dienkripsi diatur terlebih dahulu, dengan aturan sebagai berikut :

1. Ganti huruf dengan J (bila ada) dengan huruf I
2. Tulis pesan dalam pasangan huruf
3. Jangan sampai ada pasangan huruf yang sama. Jika ada, sisipkan Z di tengahnya
4. Jika jumlah huruf ganjil, tambahkan Z di akhir

Algoritma enkripsi sebagai berikut:

1. Jika ada dua huruf terdapat pada <u>baris kunci yang sama</u> maka tiap huruf diganti dengan huruf di kanannya (pada kunci yang sudah diperluas)
2. Jika dua huruf terdapat pada <u>kolom kunci yang sama</u> maka tiap huruf diganti dengan huruf di bawahnya (pada kunci yang sudah diperluas)
3. Jika dua huruf tidak pada <u>baris yang sama atau kolom yang sama</u>, maka huruf pertama diganti dengan huruf pada perpotongan baris huruf pertama dengan kolom huruf kedua.

4. Huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari 3 huruf yang digunakan sampai sejauh ini

Algoritma dekripsi kebalikan dari algoritma enkripsi,. Untuk setiap pasangan huruf pada cipher teks, tentukan titik sudut empat persegi panjang yang terbentuk dari pasangan huruf tersebut. Dua huruf titik sudut menyatakan pasangan huruf cipher teks, sedangkan dua huruf pada titik sudut yang lain menyatakan pasangan huruf plainteksnya. Urutan huruf pada pasangan plainteks tersebut mengikuti arah emapt persegi panjang yang dibentuk oleh pasangan huruf cipherteks.

Contoh :
Plainteks : MAHASISWA INFORMATIKA
Kunci : JUARA DUNIA
Kunci yang sudah diperluas dituliskan sebagai berikut:

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

Plainteks diubah dalam bentuk pasangan huruf :
MA HA SI SW AI NF OR MA TI KA
Lakukan proses enkripsi, dan didapat cipher teks sebagai berikut :
KO KI QG RX GA FP AT KO QO RC
Ketika dilakukan proses dekripsi, didapatkan hasil seperti plainteks semula :
MA HA SI SW AI NF OR MA TI KA

Hal-hal ini merupakan karakteristik dari Playfair Cipher :
1. Merupakan salah satu cipher subtitusi
2. Jumlah karakter pada cipher teks akan selalu genap
3. Perhitungan frekuensi kemunculan akan menghasilkan tidak lebih dari 25 karakter huruf, karena huruf J tidak akan pernah muncul
4. Jika terjadi perulangan panjang, akan muncul pada interval yang regular, dan dalam banyak kasus, akan berulang dalam jumlah karakter yang genap
5. Banyak kemungkinan transformasi untuk suatu bigram.

Terdapat beberapa keunikan dalam Playfair cipher ini:
1. Tidak ada karakter pada plainteks yang akan muncul di cipher teks dengan karakter yang sama
2. Karakter apapun dalam plainteks dapat direpresentasikan dalam cipher teks dengan 5 karakter lain
3. Karakter apapun dapat merepresentasikan 5 karakter lain
4. Karakter apapun tidak dapat merepresentasikan karakter yang dikombinasikan diagonal.
5. Ketika suatu karakter cipherteks sudah diinterpretasikan sebagai suatu subtitusi dari karakter plainteks, ada 20% kemungkinan bahwa karakter tersebut merepresentasikan karakter plainteks yang sama pada kemunculan lain. [5]

Untuk melakukan kriptanalisis dari Playfair ini diawali dengan melakukan perhitungan frekuensi kemunculan karakter dan bigram pada plainteks. Perhitungan frekuensi kemunculan karakter dilakukan karena huruf dengan frekuensi kemunculan yang tinggi pada cipher teks akan diikuti dengan dekat oleh karakter berfrekuensi tinggi yang direpresentasikan dan diletakkan pada baris atas di bujur sangkar. Dengan demikian, karakter dengan frekuensi kemunculan rendah diikuti dengan pasangan plainteksnya (UVWXYZ) dan akan dilokasikan pada baris akhir dari bujur sangkar. Secara singkat, huruf-huruf dengan frekuensi kemunculan tinggi umumnya berada pada baris atas dari bujur sangkar dan huruf dengan frekuensi kemunculan rendah akan muncul di baris bawah dari bujur sangkar.

Perhitungan kemunculan bigram berguna karena frekuensi kemunculan bigram pada cipher teks akan bersesuaian dengan frekuensi kemunculan di plainteks. Misal TH direpresentasikan menjadi HM, maka frekuensi HM akan tinggi di cipher teks. Perhitungan poligram juga dapat dilakukan untuk melakukan terkaan atas isi bujur sangkar.

Bigram yang berkebalikan dengan menggunakan Playfair Cipher ini akan menghasilkan pola huruf yang sama. Misalnya AB dan BA akan ditransformasikan menjadi ER dan RE. Pada bahasa Inggris, banyak sekali kata yang mengandung pasangan bigram yang berkebalikan, seperti DEpartED atau REceivER. Dengan melakukan identifikasi jarak antar bigram yang berkebalikan pada cipherteks dan menyesuaikan pola dengan kata pada plainteks yang sering muncul dan menggandung pola tersebut dapat dengan mudah untuk membangkitkan kemungkinan kata plainteks yang mungkin dibangun untuk menjadi kunci.

2.4. Super Enkripsi

Menggunakan metode *Cipher* substitusi dengan cipher transposisi. Algoritma ini bertujuan untuk memperoleh *Cipher* yang lebih kuat daripada hanya satu *Cipher* saja. Proses yang dilakukan dengan mula-mula enkripsi dengan *Cipher* substitusi sederhana, lalu hasilnya dienkripsi lagi dengan cipher transposisi [1]

Contoh:
Plainteks: MAHASISWA INFORMATIKA
Enkripsi dengan Caesar Cipher (pergeseran huruf 3) menjadi:
PDKDVLVZD LQIRUPDWLND

Kemudian enkripsi lagi dengan cipher transposisi (untuk nilai k=5):
PDKDV

LVZDL
QIRUP
DWLND

Cipherteks akhir adalah:

PLQDDVIWKZRLDDUNVLPD

3. ALGORITMA SUPER-PLAYFAIR

Super–Playfair merupakan varian dari *Playfair Chiper* yang dilanjutkan dengan melakukan super enkripsi. Tujuan algoritma ini adalah menambah kemungkinan isi bujur sangkar pada playfair cipher dan memperkuat cipher dengan melakukan 2 kali enkripsi.

3.1. Latar Belakang Algoritma Super-Playfair

Algoritma Playfair dapat dipecahkan dengan menggunakan teknik analisis frekuensi untuk kemunculan huruf dan analisis frekuensi untuk kemunculan bigram dan poligram. Hal ini dikarenakan isi dari bujur sangkar, yang merupakan kunci yang statis.

Karena itulah untuk memperumit proses kriptanalisis, maka diperlukan pembuatan kunci yang dinamis, yaitu kunci yang berubah untuk digunakan dalam melakukan proses enkripsi pada masing-masing pasangan huruf di plainteks.

Playfair cipher mengganti setiap kemunculan huruf J dengan huruf I. Huruf J tidak akan pernah muncul pada cipher teks. Untuk memperbanyak kemungkinan variasi huruf yang muncul pada cipherteks maka yang digantikan tidak hanya huruf J saja, tetapi huruf Q atau Y. Penentuan huruf yang digantikan tergantung kepada huruf mana yang lebih banyak muncul pada kunci. Huruf Q dan Y dipilih karena bersama dengan huruf J memiliki kemunculan yang rendah pada Bahasa Inggris.

Super enkripsi mampu menambah kerumitan dengan mengubah baris menjadi kolom, dan tidak hanya melakukan sekali enkripsi saja. Super enkripsi inilah yang merupakan cikal bakal dari algoritma kriptografi modern.

Karena alasan itulah, lahirlah algoritma Super-Playfair yang menggunakan kunci yang berubah untuk setiap proses enkripsi, serta pergantian atas huruf J bisa digantikan dengan huruf Q dan Y tergantung pada huruf mana antara J, Q dan Y yang muncul lebih banyak pada kunci.

3.2. Algoritma Super-Playfair

Algoritma kriptografi super-playfair merupakan algoritma yang dibuat guna memperbaiki algoritma kriptografi klasik khususnya algoritma playfair yang mudah diserang dengan teknik analisis frekuensi untuk bigram dan poligram.

Algoritma ini melakukan variansi terhadap Playfair Cipher, untuk kemudian melakukan super enkripsi dengan melakukan cipher transposisi sejumlah panjang kunci terhadap hasil cipher teks yang dihasilkan oleh varian playfair cipher tersebut.

Varian Playfair Cipher yang dilakukan adalah huruf yang dihilangkan bukanlah huruf J saja melainkan variasi antara huruf Q dan Y (yang merupakan huruf dengan frekuensi kemunculan terendah dalam bahasa Inggris) berdasarkan huruf mana (antara J,Q,Y) yang paling banyak muncul pada kunci. Huruf yang digantikan untuk J adalah I, sementara Q digantikan oleh R, dan Y dengan X. Pemilihan huruf pengganti berdasarkan pemilihan dua huruf terdekat dengan huruf tersebut yang memiliki frekuensi kemunculan karakter pada bahasa Inggris yang lebih kecil. Dengan demikian kombinasi isi bujur sangkar akan bertambah, mengingat tidak hanya huruf J saja yang dihilangkan tapi bisa juga huruf Q dan Y yang dihilangkan.

Pembentukan bujur sangkar kunci sama dengan pembentukan kunci pada Playfair Cipher, ditambah dengan aturan penghapusan huruf (huruf yang tidak ada di bujur sangkar) sesuai yang dijelaskan sebelumnya. Hanya saja pada proses enkripsi untuk bigram ke dua dilakukan perubahan isi bujur sangkar, dengan aturan sebagai berikut :

1. Baris dan kolom yang diperluas dihapuskan (baris dan kolom yang keenam)
2. Kolom kelima dipindah menjadi kolom pertama, sementara kolom pertama mejadi kolom kedua, kolom kedua menjadi kolom ketiga, dan seterusnya
3. Tambahkan baris dan kolom yang diperluas dengan baris pertama dan kolom pertama dari bujursangkar

Pesan yang akan dienkripsi diatur terlebih dahulu, dengan aturan sebagai berikut:

1. Ganti huruf dengan J (bila ada) dengan huruf I, atau huruf Q dengan huruf R atau Y dengan huruf X, sesuai dengan huruf mana dari J,Q, dan Y yang lebih banyak muncul pada kunci.
2. Tulis pesan dalam pasangan huruf
3. Jangan sampai ada pasangan huruf yang sama. Jika ada, sisipkan Z di tengahnya
4. Jika jumlah huruf ganjil, tambahkan Z di akhir

Algoritma enkripsi sebagai berikut:

1. Jika ada dua huruf terdapat pada baris kunci yang sama maka tiap huruf diganti dengan huruf di kanannya (pada kunci yang sudah diperluas)
2. Jika dua huruf terdapat pada kolom kunci yang sama maka tiap huruf diganti dengan huruf di bawahnya (pada kunci yang sudah diperluas)
3. Jika dua huruf tidak pada baris yang sama atau kolom yang sama, maka huruf pertama diganti dengan huruf pada perpotongan baris huruf pertama dengan kolom huruf kedua.

4. Huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari 3 huruf yang digunakan sampai sejauh ini

Lakukan kembali langkah-langkah di atas untuk bigram plainteks berikutnya dengan bujur sangkar kunci yang baru. Setelah semua bigram plainteks selesai dienkripsi, gunakan super enkripsi. Karena *Cipher* subtitusi sudah dilakukan dengan metode varian *playfair chiper*, maka kini lakukan *chiper* transposisi dengan k = panjang kunci. Dengan demikian super-playfair selesai mengenkripsi plainteks.

Untuk melakukan dekripsi, diawali dengan melakukan dekripsi dengan metode yang sama untuk cipher transposisi (membalik baris menjadi kolom sesuai dengan panjang kunci), dan dilanjutkan dengan dekripsi untuk playfair cipher. Aturan dekrispi sama dengan aturan playfair cipher. Hanya saja untuk bigram cipher yang kedua dilakukan pergeseran bujursangkar seperti pada langkah yang disebutkan sebelumnya.

3.3. Hasil dan Pengujian Algoritma Super-Playfair

Penulis telah membuat program untuk melakukan pengujian terhadap algoritma Super-Playfair ini. Namun, untuk memperjelas proses kerja dari algoritma Super-Playfair ini akan dilakukan simulasi dengan gambar dan kata-kata. Pengujian dilakukan dengan menggunakan contoh berikut ini :

PLAINTEKS : PERUSAHAAN AIR OKE

Diubah ke dalam bentuk bigram : PE RU SA HA ZA NA IR OK EZ

KUNCI :BANYU JAYA

Karena kunci yang dipilih lebih banyak mengandung huruf Y daripada J, maka huruf yang akan dihilangkan dari bujur sangkar adalah huruf J. Sehingga, hasil bujursangkar kunci :

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

Melakukan enkripsi untuk bigram pertama. Cipher teks yang didapat : QD

Melakukan perubahan bujursangkar kunci :

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

Melakukan enkripsi untuk bigram kedua. Cipher teks yang didapat: QD ZF

Melakukan perubahan bujursangkar kunci :

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

Melakukan enkripsi untuk bigram keteiga. Cipher teks yang didapat: QD ZF TB

Melakukan perubahan bujursangkar kunci :

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

Melakukan enkripsi untuk bigram keempat. Cipher teks yang didapat: QD ZF TB CO

Melakukan perubahan bujursangkar kunci :

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

Melakukan enkripsi untuk bigram kelima. Cipher teks yang didapat: QD ZF TB CO TU

Melakukan perubahan bujursangkar kunci :

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

Melakukan enkripsi untuk bigram keenam. Cipher teks yang didapat: QD ZF TB CO TU XN

Melakukan perubahan bujursangkar kunci :

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

Melakukan enkripsi untuk bigram ketujuh. Cipher teks yang didapat: QD ZF TB CO TU XN LP

Melakukan perubahan bujursangkar kunci :

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

Melakukan enkripsi untuk bigram kedelapan. Cipher teks yang didapat: QD ZF TB CO TU XN LP

Melakukan perubahan bujursangkar kunci :

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

Melakukan enkripsi untuk bigram kesembilan. Cipher teks yang didapat: QD ZF TB CO TU XN LP QH
Melakukan perubahan bujursangkar kunci :

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

Melakukan enkripsi untuk bigram kesepuluh. Cipher teks yang didapat:
QD ZF TB CO TU XN LP QH WF

Setelah selesai dilakukan enkripsi dengan memakai varian Playfair, berikutnya adalah melakukan super enkripsi. Melakukan cipher transposisi dengan k=9, sesuai dengan panjang kunci:
QDFZTBCOT
UXNLPQHWF
Hasil akhir enkripsi adalah :
QUDXFNZLTPBQCHOWTF
Ketika dilakukan proses dekripsi, maka plain teks yang dihasilkan adalah :
PE RU SA HA ZA NA IR OK EZ
Karena algoritma ini mampu untuk melakukan proses enkripsi dan dekripsi maka algoritma ini telah memenuhi prinsip dasar kriptografi.

3.4. Kriptanalisis Algoritma Super-Playfair

Langkah kriptanalisis yang mungkin dilakukan adalah diawali dengan menerka panjang kunci. Menerka panjang kunci merupakan suatu yang rumit, karena panjang kunci baru dapat diketahui setelah menerka isi bujur sangkar kunci. Maka untuk mendapatkan panjang kunci ini bisa dilakukan dengan metode brute force, dengan menerka semua kemungkinan panjang kunci. Setelah didapat panjang kunci, dilakukan dekripsi untuk cipher transposisi dengan panjang kunci terkaan.

Yang dilakukan berikutnya adalah dengan melakukan terkaan isi bujur sangkar. Isi bujur sangar dapat diketahui dengan teknik perhitungan frekuensi untuk bigram dan poligram di cipherteks untuk kemudian dibandingkan dengan frekuensi bigram dan poligram pada kata bahasa Inggris. Selain itu dengan melakukan teknik terkaan huruf bigram yang berkebalikan seperti pada teknik kriptanalisis pada Playfair Cipher, hanya saja ditambah kerumitannya karena isi bujur sangkar yang berubah.

3.5. Kekuatan Algoritma Super-Playfair

Algoritma Super-Playfair ini memberikan kemungkinan kunci lebih banyak daripada algoritma Playfair biasa. Karena pada setiap bigram yang diproses akan dibentuk bujur sangkar kunci yang baru, sehingga kunci cukup dinamis. Kemungkinan kunci yang dimiliki oleh Super Playfair ini menjadi 5 kali lebih banyak daripada kemungkinan kunci pada algoritma Playfair, menjadi 5x 25!

Selain itu Algoritma Super-Playfair ini juga lebih rumit dengan dilakukannnya cipher transposisi sesuai panjang kunci. Karena untuk menerka panjang kunci sendiri perlu diketahui isi dari bujur sangkar kunci awal, dan untuk menerka isi bujur sangkar kunci awal diperlukan proses yang cukup rumit.

2.1. Kelemahan Algoritma Super-Playfair

Dengan melakukan perubahan isi bujur sangkar kunci hanya dengan menggeser sesuai banyaknya kolom, maka sebetulnya kunci yang dihasilkan berulang setiap 5 kali. Dengan demikian ini akan menghasilkan celah untuk melakukan kriptanalisis.

4. KESIMPULAN

Terdapat beberapa kesimpulan yang diambil dari pembuatan makalah algoritma Super-Playfair ini, yaitu:

1. Kriptografi saat ini telah menjadi sangat penting dan berkembang. Dengan pembuatan makalah ini semakin membuat penulis memahami tentang konsep kriptografi
2. Algoritma kriptografi klasik umumnya hanya terdiri dari cipher transposisi dan cipher subtitusi. Dengan demikian banyak sekali kemungkinan untuk menciptakan varian baru dari algoritma klasik ini.
3. Algoritma Super-Playfair menggabungkan dua algoritma klasik, yaitu Playfair Cipher dan Super Enkripsi.
4. Dengan adanya algoritma Super-Playfair ini memperbanyak kemungkinan kunci untuk algoritma Playfair Cipher
5. Super-Playfair memberikan tingkat keamanan yang lebih baik dari pada sekedar Playfair Cipher dan Super Enkripsi sederhana, karena kunci yang digunakan lebih banyak dan beragam.
6. Kunci yang berulang setiap 5 kali memungkinkan adanya celah untuk melakukan kriptanalisis. Namun proses kriptanalisis sendiri memerlukan komputasi yang rumit.

DAFTAR REFERENSI

[1] Munir, Rinaldi. *Diktat Kuliah IF5054 Kriptografi*. Program Studi Teknik Informatika Sekolah Teknik Elektro dan Informatika , Institut Teknologi Bandung. 2006

[2] Bishop, David. *Introduction to Cryptography with Java Aplets*. Jones and Batrlet Publisher. 2002

[3] http://www.simonsingh.net/The_Black_Chamber/playfaircipher.htm, diakses tanggal 9 Oktober 2007

[4] http://www.crosswordman.com, diakses tanggal 22 September 2007

[5] http://www.wisdom.weizmann.ac.il/~albi/cryptanalysis/lect3.htm, diakses tanggal 9 Oktober 2007