Metode Enkripsi baru : *Triple Transposition Vigènere Cipher*

Maureen Linda Caroline (13508049)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
if18049@students.if.itb.ac.id

***Abstract*—Hingga saat ini ada beberapa metode enkripsi yang diklaim sangat sulit atau tidak dapat dipecahkan, yang salah satunya adalah *One-Time Pad*. Alasannya adalah karena penggunaan kunci yang sangat acak sehingga cipherteksnya menjadi sangat acak serta mendekripsikan cipherteks dengan beberapa kunci yang berbeda dapat menghasilkan plainteks yang bermakna, sehingga kriptanalis tidak tahu plainteks mana yang benar. Berkaca dari adanya metode enkripsi yang sulit atau tidak dapat dipecahkan semacam inilah, maka tercetuskan gagasan baru mengenai sebuah metode enkripsi baru dengan menggunakan algoritma kriptografi klasik yang diharapkan memiliki kelebihan tidak dapat dipecahkan. *Triple Transposition Vigènere Ccipher* yang menggunakan dua teknik penyandian yaitu transposisi dan substitusi.**

***Index Terms*—metode enkripsi baru, *One-Time Pad*, teknik penyandian klasik, *Triple Transposition Vigènere Cipher*.**

I. PENDAHULUAN

Sudah sejak lama informasi menjadi salah satu aspek penting dalam kehidupan. Mungkin teknik komunikasi berkembang, namun tidak ada satu alat komunikasi jarak jauh yang dapat mengirimkan suatu informasi penting atau dirahasiakan dengan aman. Karena itulah tercipta sebuah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Pada awalnya kriptografi hanya digunakan untuk menyandikan saja, tetapi seiring berjalannya waktu, kriptografipun menjadi salah satu aspek penting dalam pengamanan berbagai jenis informasi.

Sejak pertama kali munculnya kriptografi, metode enkripsi selalu mengalami perubahan. Metode ini berkembang dari waktu ke waktu mulai dari algoritma kriptografi kalsik hingga kriptografi modern, dari yang menggunakan kunci-simetris hingga kunci-asimetris. Semua perkembangan ini terjadi dengan satu tujuan, yaitu membuat kriptanalisis yang sesulit mungkin, dengan kata lain meninggkatkan keamanan.

Hingga saat ini, sudah banyak metode enkripsi yang diklaim sangat sulit atau tidak dapat dipecahkan. Salah satunya adalah *One-Time Pad.* Sekalipun diklaim sangat sulit atau tidak dapat dipecahkan, tetapi tetap saja ada kelemahannya. Salah satu kelemahan dari One-Time Pad adalah dibutuhkannya saluran komunikasi yang aman dan terpercaya untuk mengirimkan kuncinya kepada penerima pesan serta kebutuhan untuk membuat kunci baru setiap kali akan melakukan enkripsi.

Untuk membuat sebuah algoritma enkripsi yang tidak dapat dipecahkan, ada beberapa syarat. Syarat-syarat tersebut adalah kunci yang harus benar-benar acak dan panjang kunci harus sama dengan panjang plainteks sehingga plainteks yang sama tidak selalu menghasilkan cipherteks yang sama.

Karena itu muncullah sebuah gagasan untuk membuat suatu metode enkripsi baru yang merupakan pengembangan dari algoritma klasik. Seperti yang telah diketahui bahwa ada salah satu algoritma klasik yang cukup terkenal yaitu *Vigènere Cipher*.

II. LANDASAN TEORI

1. Algoritma Kriptografi Klasik

Pada kriptografi klasik, ada dua macam cara enkripsi yang dilakukan. Teknik enkripsi itu adalah *Cipher* Substitusi dan *Cipher* Transposisi.

1.1 *Cipher* Substitusi

Pada teknik ini, setiap huruf pada plainteks akan digantikan dengan huruf lain berdasarkan suatu cara atau rumus tertentu. Ada empat jenis cipher substitusi, yaitu cipher abjad-tunggal, cipher substitusi homofonik, cipher abjad-majemuk, dan cipher substitusi poligram.

Yang pertama adalah cipher abjad-tunggal, enkripsi dilakukan dengan mengganti satu huruf di plainteks dengan satu huruf yang bersesuaian. Contoh cipher ini adalah *Caesar Cipher*.

Yang kedua adalah cipher substitusi homofonik. Setiap huruf plainteks dipetakan kedalam salah satu huruf cipherteks yang mungkin. Tujuan pemetaan ini adalah untuk menyembunyikan hubungan statistik antara plainteks dengan cipherteks. Fungsi *ciphering* adalah dengan pemetaan *one-to-many*.

Yang ketiga adalah cipher abjad-majemuk. Bila pada cipher abjad-tunggal satu kunci digunakan untuk setiap huruf pada plainteks, maka pada cipher abjad-majemuk menggunakan kunci yang berbeda-beda untuk setiap

huruf pada plainteks. Contoh cipher ini adalah *Vigènere Cipher*.

Dan yang terakhir adalah cipher substitusi poligram. Enkripsi dilakukan dengan pengelompokan huruf-huruf dalam plainteks menjadi n huruf tiap bloknya dengan membuang spasi. Blok-blok yang terbentuk disubstitusi dengan blok-blok cipherteks. Jika blok huruf plainteks/cipherteks panjangnya 2 huruf, maka disebut bigram/digram. Jika 3 huruf maka disebut ternary-gram dan seterusnya. Tujuannya adalah untuk mendistribusikan kemunculan poligram menjadi *flat* sehingga menyulitkan analisis frekuensi. Contoh cipher ini adalah *Playfair Cipher*.

1.2 *Cipher* Transposisi

Cipher transposisi adalah mengubah susunan huruf pada plainteks sehingga urutannya berubah. Plainteks yang dirubah susunan hurufnya seperti ini merupakan cipherteksnya.

Nama lain untuk metode ini adalah permutasi, karena *transpose* setiap huruf didalam teks sama dengan mempermutasikan karakter-karakter tersebut. Contoh paling sederhana adalah dengan membalik kata-kata pada plainteks :

Plainteks : AYAH PERGI KE KANTOR
Cipherteks : HAYA IGREP EK ROTNAK

Contoh transposisi lainnya adalah menyusun plainteks menjadi n baris dengan bentuk zigzag. Contoh berikut dengan menggunakan 3 baris :

Plainteks : AYAH PERGI KE KANTOR
Mode zigzag 3 baris :

```
A       P       I       A       R
  Y   H   E   G   K   K   N   O
    A       R       E       T
```

Cipherteks : APIARYHEGKKNOARET

2. *Vigènere Cipher* dan Metode Kasiski

2.1 Vigènere Cipher

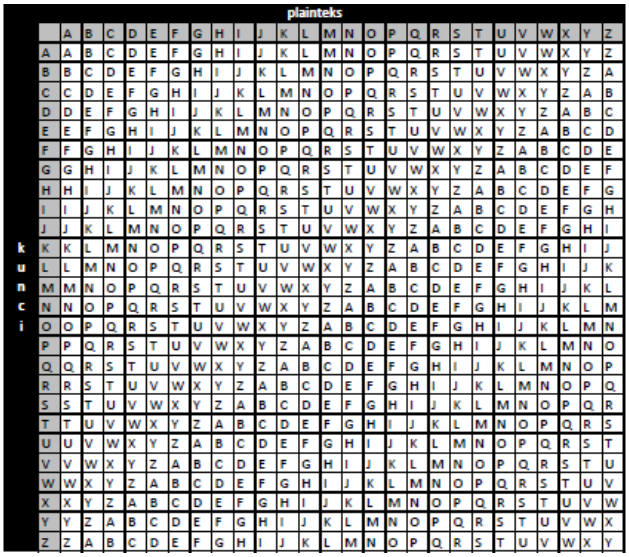
Vigènere Cipher adalah metode enkripsi abjad-majemuk manual. Algoritma ini dipublikasikan oleh diplomat sekaligus kriptologis Perancis, Blaise de Vigènere, pada abad XVI (tahun 1586). Tetapi sebenarnya Giovan Batista Belaso telah menggambarkannya pertama kali pada tahun 1553. Sekalipun algoritma ini dipublikasikan pada abad XVI, akan tetapi algoritma ini baru dikenal luas 200 tahun kemudian yang kemudian dinamakan *Vigènere Cipher*

Sayangnya algoritma ini berhasil dipecahkan oleh Babbage dan Kasiski pada pertengahan abad XIX. Metode tersebut kemudian diberi nama Metode Kasiski.

Vigènere Cipher digunakan oleh Tentara konfiderasi pada Perang Sipil Amerika. Perang Sipil terjadi setelah *Vigènere Cipher* berhasil dipecahkan.

Pada dasarnya, *Vigènere Cipher* menggunakan bujursangkar *Vigènere Cipher* untuk melakukan enkripsi. Setiap baris pada dibujursangkar menyatakan huruf-huruf cipherteks yang diperoleh dengan *Caesar Cipher*. Bedanya, pada *Vigènere Cipher*, setiap huruf pada plainteks dienkripsi menggunakan kunci yang berbeda. Huruf pertama pada plainteks dienkripsi dengan kunci yang berupa huruf pertama pada kata kunci dan begitu seterusnya. Jika panjang kunci lebih pendek daripada panjang plainteks, maka kunci diulang secara periodik. Oleh karena itu, jika panjang kncinya adalah satu huruf, maka enkripsi sama saja dengan *Caesar Cipher* biasa.

Berikut adalah bujursangkar *Vigènere*.



Gambar 1. Bujursangkar *Vigènere*

Cara menggunakan bujursangkar *Vigènere* adalah sebagai berikut: baris paling atas menyatakan huruf-huruf plainteks dan kolom paling kiri menyatakan huruf-huruf pada kunci. Pertama tarik garis vertikal dari huruf plainteks kebawah. Setelah itu tarik garis horizontal dari huruf kunci ke kanan. Cari titik perpotongannya. Perpotongan kedua garis tersebut menyatakan huruf cipherteks dari huruf plainteks yang bersangkutan. Sebenarnya karakter cipherteks didapat dengan rumus $c(p) = (p+k) \bmod 26$. Berikut adalah contoh plainteks dan cipherteks dengan menggunakan *Vigènere Cipher*:

Plainteks: THIS PLAINTEXT
Kunci: sony
Cipherteks: LVVQ HZNGFHRVL

Terlihat dari contoh diatas bahwa huruf yang sama tidak selalu dienkripsi menjadi huruf cipherteks yang sama pula. Hal ini merupakan karateristik dari cipher abjad-majemuk yaitu setiap huruf cipherteks dapat memiliki kemungkinan bnayak huruf plainteks. Dengan karakteristik ini, *Vigènere Cipher* dapat mencegah frekuensi huruf-huruf didalam cipherteks yang mempunyai pola tertentu sana seperti pada cipher abjad-tunggal.

Dekripsi pada *Vigènere Cipher* dapat dilakukan dengan cara sebaliknya, yaitu menarik garis horizontal ke kanan dari huruf kunci hingga ditemukan huruf cipherteks yang dituju, kemudian dari huruf cipherteks tersebut ditarik garis vertikal ke atas sampai ke huruf plainteks.

Secara umum dekripsi *Vigènere Cipher* dapat dirumuskan sebagai berikut:

Rumus : p = (c-k) mod 26

Dilihat dari kedua rumus tersebut, dapat dilihat bahwa karakteristik dari cipher abjad-majemuk adalah setiap huruf cipherteks dapat memiliki kemungkinan banyak huruf plainteks. Berbeda dengan cipher substitusi sederhana dimana setiap huruf cipherteks selalu menggantikan huruf plainteks tertentu.

Vigènere Cipher dapat mencegah frekuensi huruf-huruf dalam cipherteks yang mempunyai pola tertentu yang sama seperti pada cipher abjad-tunggal. Jika periode kunci diketahui dan tidak terlalu panjang, maka kunci dapat ditentukan dengan menulis program komputer untuk melakukan *exhaustive key search.* Tetapi akan sangat sulit jika mencari kuncinya dengan menggunakan *exhaustive key search* karena usaha ini membutuhkan percobaan sebanyak 26^p kali.

2.2 Metode Kasiski

Metode Kasiski pertama kali di temukan oleh Friedrich Kasiski pada tahun 1863 untuk memecahkan *Vigènere Cipher*. Metode Kasiski membantu untuk menemukan panjang kunci *Vigènere Cipher*.

Metode ini memanfaatkan keuntungan bahwa Bahasa Inggris tidak mhanya mengandung perulangan huruf, tetapi juga perulangan pasangan huruf atau *triple* huruf, seperti TH, THE, dsb. Perulangan kelompok huruf ini ada kemungkinan menghasilkan kriptogram yang berulang. Contoh 1:

Plainteks : CRYPTO IS SHORT FOR CRYPTOGRAPHY
Kunci : abcd
Cipherteks : **CSASTP** KV SIQUT GQU **CSASTP**UIAQJB

Pada contoh ini, CRYPTO dienkripsi menjadi kriptogram yang sama, yaitu CSATP. Tetapi kasus ini tidak selalu demikian misalnya pada contoh 2 berikut ini:

Plainteks : CRYPTO IS SHORT FOR CRYPTOGRAPHY
Kunci : abcdef
Cipherteks : **CSASXT** IT UKWST GQU **CWYQVR**KWAQJB

Pada contoh diatas CRYPTO tidak dienkripsi menjadi kriptogram yang sama. Hal ini disebabkan panjang string plainteks bukan merupakan kelipatan panjang kunci.

Secara intuitif, jika jarak antara dua buah string yang berulang didalam plainteks merupakan kelipatan dari panjang kunci, maka string yang sama tersebut akan muncul menjadi kriptogram yang sama pula didalam cipherteks.

Pada contoh 1,

- Kunci = abcd
- Panjang kunci = 4
- Jarak antara dua CRYPTO yang berulang = 16
- 16 adalah kelipatan 4

∴ CRYPTO dienkripsi menjadi kriptogram yang sama.

Sedangkan pada contoh 2,

- Kunci = abcdf
- Panjang kunci = 5
- Jarak antara dua CRYPTO yang berulang = 16
- 16 bukan adalah kelipatan 5

∴ CRYPTO tidak dapat dienkripsi menjadi kriptogram yang sama.

Berikut adalah langkah-langkah metode Kasiski:

1. Temukan semua kriptogram yang berulang didalam cipherteks (pesan yang panjang biasanya mengandung kriptogram yang berulang).
2. Hitung jarak antara kriptogram yang berulang.
3. Hitung semua faktor (pembagi) dari jarak tersebut (faktor pembagi menyatakan panjang kunci yang mungkin).
4. Tentukan irisan dari himpunan faktor pembagi tersebut. Nilai yang muncul didalam irisan menyatakan angka yang muncul pada semua faktor pembagi dari jarak-jarak tersebut. Nilai tersebut mungkin adalah oanjang kunci.

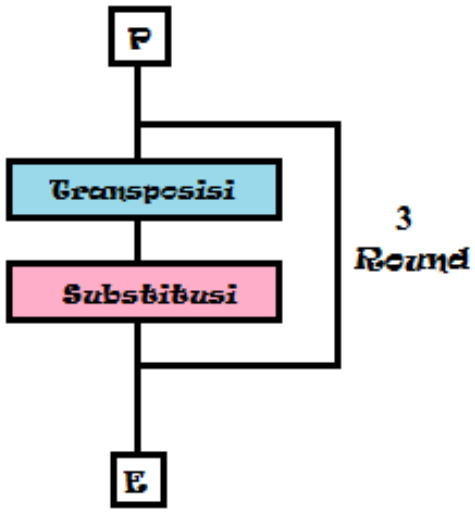
Metode ini dapat ditangkal dengan menggunakan panjang kunci yang sama dengan panjang plainteks. Namun, tentu sulit untuk mengingat kunci yang begitu panjang (jika plainteksnya panjang) atau perlu mekanisme lain untuk mengirim pesan kepada penerima pesan.

III. METODE ENKRIPSI BARU

Triple Transposition Vigènere Cipher

Triple Transposition Vigènere Cipher adalah metode enkripsi dengan cara mengulang teknik *Vigènere Cipher* yang setiap plainteksnya dilakukan transposisi terlebih dahulu sebanyak tiga kali dengan menggunakan kunci yang tiap kuncinya harus berbeda satu dengan yang lainnya.

Metode *Triple Transposition Vigènere Cipher* dapat digambarkan sebagai berikut:



Proses yang terjadi pada *Triple Transposition Vigènere Cipher* terbagi menjadi dua bagian. Metode transposisi dapat disimbolkan dengan T dan metode substitusi menggunakan vigenere yang disimbolkan dengan E serta kunci untuk melakukan vigenere K. Secara matematis metode *Triple Transposition Vigènere Cipher* ini dapat dituliskan sebagai:

Proses enkripsi: $C = S_3(T_3(S_2(T_2(S_1(T_1(P))))))$

Bila dijabarkan, cipherteks diperoleh dengan mentransposisikan plainteks, kemudian hasilnya disubstitusi menggunakan kunci pertama, lalu ditransposisikan kembali, lalu disubstitusi dengan menggunakan kunci yang berbeda dari kunci pertama, disebut saja kunci kedua, setelah itu dilakukan transposisi lagi yang kemudian diakhiri dengan proses substitusi menggunakan kunci ketiga. Substitusi disini menggunakan *Vigènere Cipher*

Ketiga algoritma transposisi sudah didefinisikan terlebih dahulu dengan suatu kunci atau suatu aturan tertentu setiap kali proses enkripsi metode transposisinya akan selalu tetap.

Untuk metode enkripsi ini, spasi tidak diperhitungkan sehingga lebih baik dihilangkan saja. Rumus untuk transposisi adalah membagi panjang cipherteks dengan suatu kunci tertentu yang ditentukan oleh pengguna yang kemudian teks dibaca secara vertikal dari kolom pertama.

Sebagai ilustrasinya perhatikan contoh dibawah ini:

Plainteks (P):

INI ADALAH PLAINTEKS KRIPTOGRAFI

Transposisi pertama (T_1) dengan kunci=3:

I	N	I
A	D	A
L	A	H
P	L	A
I	N	T
E	K	S
K	R	I
P	T	O
G	R	A
F	I	

Hasil T_1: IALPIEKPGFNDALNKRTRIIAHATSIOA

Substitusi pertama (S_1) dengan kunci= SEMBILAN:

AEXQQPKCYJZEIWNXJXDJQLHNLWUPI

Transposisi kedua (T_2) dengan kunci=5:

A	E	X	Q	Q
P	K	C	Y	J
Z	E	I	W	N
X	J	X	D	J
Q	L	H	N	L
W	U	P	I	

Hasil T_2 : APZXQWEKEJLUXCIXHPQYWDNIQJNJL

Substitusi kedua (S_2) dengan kunci=GAJAH:

GPIXXCETEQRUGCPDHYQFCDWIXPNSL

Transposisi ketiga (T_3) dengan kunci=11:

G	P	I	X	X	C	E	T	E	Q	R
U	G	C	P	D	H	Y	Q	F	C	D
W	I	X	P	N	S	L				

Hasil T_3 : GUWPGIICXXPPXDNCHSEYLTQEFQCRD

Substitusi ketiga (S_3) dengan kunci=SEBELAS:

YYXTRIAUBYTAXVFGIWPYDLUFJBCJV

Jadi hasil total enkripsinya adalah
YYXTRIAUBYTAXVFGIWPYDLUFJBCJV

Proses dekripsi dapat dilakukan dengan arah

sebaliknya. Bila dirumuskan maka akan terlihat sebagai berikut:

Proses dekripsi: $P = T_1'(S_1'(T_2'(S_2'(T_3'(S_3'(C))))))$

Maksud T' disini adalah transposisi kebalikkannya dan S' adalah substitusi kebalikannya.

IV. ANALISIS

Pada metoda *Triple Transposition Vigènere Cipher* ini, terlihat bahwa tergantungan hasil cipherteks terhadap kunci sangat tinggi. Salah satu huruf saja, maka akan berakibat kesalahan yang cipherteks. Setiap kunci harus didefinisikan dengan baik.

Dengan begitu dapat dikatakan bahwa *Triple Transposition Vigènere Cipher* berpotensi untuk mengimbangi kekuatan *One-Time Pad*. Bila ditinjau lebih jauh lagi, kunci dapat ditransposisikan terlebih dahulu baru disubstitusikan secara virtual. Namun sayangnya hal ini tidak dapat dilakukan karena posisi akhir pada cipherteks terubah. Bandingkan dengan contoh diatas:

$T_1'(K_1)$

S	M	I
E	B	L
M	I	A
B	L	N
I	A	S
L	N	E
A	S	M
N	E	B
S	M	I
E	B	

Hasil : SMIEBLMIABLNIASLNEASMNEBSMIEB

Plainteks: INI ADALAH PLAINTEKS KRIPTOGRAFI
Kunci : SMIEBLMIABLNIASLNEASMNEBSMIEB
Cipherteks : AZQEELXIHQWNQNLPXWKJUCXPY DIJJ

Pada contoh, cipherteks yang didapat dari hasil substitusi pertama adalah AEXQQPKCYJZEIWNXJXDJQLHNLWUPI dan hasil ini berbeda dengan hasil yang didapat ketika hanya kunci yang ditransposisikan. Hal ini disebabkan karena susunan huruf pada plainteks yang berubah. Tetapi jika ditinjau lebih jauh, huruf-huruf yang dihasilkan sama.

Kunci yang terbentuk terasa seperti kunci dengan panjang yang sama dengan panjang plainteks dan teracak. Karena itulah maka metoda baru ini dapat dikatakan setara dengan *One-Time Pad*.

Ada beberapa hal yang perlu diperhatikan saat menetapkan kunci, antara lain:

1. Kunci substitusi sebaiknya memiliki panjang yang berbeda satu dengan yang lainnya.
2. Kunci transposisi harus merupakan angka yang berbeda satu dengan yang lain agar hasil transposisinya berbeda-beda.

V. KESIMPULAN

Triple Transposition Vigènere Cipher memiliki beberapa keunggulan. Keungulan-keunggulan itu adalah sebagai berikut:

1. Proses enkripsi/dekripsi yang sederhana. Hanya diperlukan 3 kunci transposisi dan 3 kunci substitusi yang berbeda satu dengan yang lainnya untuk melakukan proses enkripsi/dekripsinya.

2. Proses enkripsi/dekripsinya relatif fleksibel dan mudah untuk dilakukan secara manual ataupun dengan bantuan program komputer. Untuk prosesnya, cukup digunakan metode transposisi dan sebuah bujursangkar *Vigènere* yang akan digunakan sebanyak tiga kali. Karena itu, mudah untuk diimplementasikan sebagai sebuah program komputer. Pengimplementasian tidak akan sulit berhubung sudah banyak perangkat lunak yang mengimplementasikan *Vigènere Cipher* di dunia maya dan hanya tinggal diunduh saja. Dan untuk pengguna, tidak diperlukan perangkat lunak bantuan lainnya.

3. Kekuatan enkripsinya sekuat *One-Time Pad*. Seperti yang telah dijelaskan pada bagian 4, yaitu analisis, bahwa kunci yang digunakan sesuai dengan syarat untuk *unbreakable cipher*. Bila pada teknik enkripsi *One-Time Pad* diklaim tidak dapat dipecahkan dengan menggunakan *exhaustive key search attack*, maka pada *Triple Transposition Vigènere Cipher* juga berpotensi memiliki kekuatan tersebut. Pengacakan posisi teks dan kunci membuat metoda ini terasa seperti memiliki sebuah kunci yang benar-benar teracak dengan panjang kunci yang sama dengan panjang kunci plainteks.

4. Salah satu kelemahan *One-Time Pad* adalah dibutuhkannya saluran komunikasi yang aman dan dapat dipercaya untuk memberi tahu kuncinya kepada penerima pesan. Saluran ini diperlukan karena panjang kuncinya yang tidak mungkin diingat. Selain itu juga karena kunci yang hanya digunakan satu kali untuk setiap penyandian sehingga pengiriman kunci harus dilakukan berkali-kali setiap kali melakukan enkripsi. Ini membuat peluang bocornya kunci semakin besar. Berbeda halnya dengan *Triple Transposition*

Vigènere Cipher. Kunci pada metode enkripsi baru ini tidak perlu terlalu panjang selama kunci ini memenuhi persyaratan seperti pada bagian 4. Secara virtual, kunci yang dihasikan terlihat benar-benar acak yang juga panjangnya sepanjang plainteksnya, sehingga kunci terlihat serupa seperti *One-Time pad*.

Disamping keunggulan-keunggulannya itu, ada juga kelemahan dari *Triple Transposition Vigènere Cipher* ini. Kelemahannya antara lain:

1. Untuk ukuran plainteks yang besar, sulit untuk mendapatkan tiga buah kunci yang cukup pendek dengan tetap memenuhi syarat kedua bahwa kunci yang digunakan merupakan kelipatan persekutuan terkecil dari panjang kunci. Karena kunci ini tidak cukup pendek untuk diingat maka ada kemungkinan diperlukan saluran komunikasi untuk mengirimkan kuncinya. Seperti yang telah dibahas bahwa saluran komunikasi tidak aman dan tidak dapat dipercaya.

2. Masih ada kemungkinan terjadinya pengulangan kriptogram baik itu pasangan huruf atau triplet huruf atau yang lebih banyak dari itu yang sama pada plainteks yang terpisah sejauh kelipatan dari panjang kunci baru K. Dengan demikian masih ada kemungkinan kunci dapat dipecahkan oleh kriptanalis mengunakan metode Kasiski walaupun kemungkinan tersebut lebih kecil dibandingkan alogritma *Vigènere Cipher* sederhana ataupun Cipher transposisi.

Melakukan modifikasi terhadap algoritma kriptografi klasik dapat juga menghasilkan algoritma yang kuat tetapi senderhana.

REFERENCES

Munir, Rinaldi, *Slide Algoritma Kriptografi bagian 1*, Program Studi Teknik Informatika. Tanggal akses: 15 Maret 2011.

Munir, Rinaldi, *Slide Algoritma Kriptografi bagian 2*, Program Studi Teknik Informatika. Tanggal akses: 15 Maret 2011

Munir, Rinaldi, *Slide Kriptanalisis*, Program Studi Teknik Informatika. Tanggal akses: 15 Maret 2011.

Munir, Rinaldi, *Slide One-Time Pad, Cipher yang Tidak Dapat Dipecahkan*, Program Studi Teknik Informatika. Tanggal akses: 15 Maret 2011. Tanggal akses: 23 Maret 2011.

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

ttd

Maureen Linda Caroline - 13508049