Pengembangan Aplikasi Simulasi Pemecahan Rail Fence Cipher, Columnar Transposition dan Scytale

Yudi Retanto 13508085
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
If18085@students.if.itb.ac.id

Algoritma kriptografi transposisi adalah algoritma kriptografi klasik yang sangat sederhanan penggunaannya. Tiga algoritma yang digunakan adalah Rail Fence Cipher,Columnar Transposition dan Scytale. Ketiga algoritma tersebut adalah algoritma sederhana yang bekerja dengan mengatur posisi karakter-karakter pada plainteks untuk menghasilkan cipherteks. Sebagai algoritma klasik, cipherteks yang dihasilkan akan sangat mudah di pecahkan oleh orang yang tidak memiliki kunci untuk mendapatkan plainteks. Namun teteap dibutuhkan waktu untuk melakukan pemecahan terhadapa cipherteks jika dilakukan tanpa program bantu. Dengan menggunakan program sederhana diharapkan dpat meningkatkan performa dalam arti menurunkan waktu yang dibutuhkan untuk memecahkan suatu cipherteks hasil enkripsi algoritma transposisi.

***Index* Rail Fence Cipher, Columnar Transposition, Scytale, Pemecahan, Program bantu.**

1. PENDAHULUAN

Kriptografi berasal dari bahasa yunani yang terdiri dari kata *kryptos* yang berarti "hidden, secret" dan *graphin* yang berarti "writing, study". Jadi kriptografi adalah sebuah ilu yang mempelajari tentang bagaimana menyembunyikan informasi. Kriptografi modern menggabungkan berbagai disiplin ilmu seperti matematika, sains computer, dan electrical engineering.

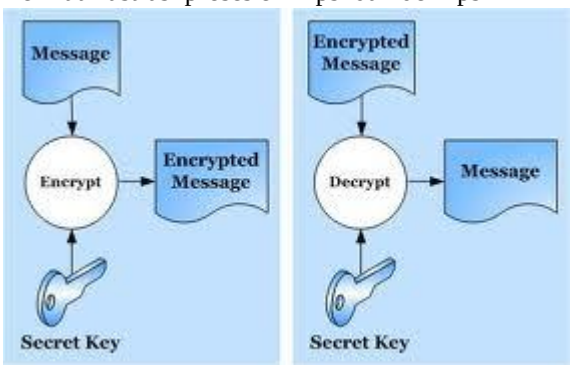
Pesan adalah data atau informasi yang dapat dibaca dan dimengerti maknanya atau dapat juga disebut plainteks. Rupa pesan dapat berupa teks, gambar, music mp3, video, tabel, daftar belanja, dan lain-lain. Pesan ini dapat dikrim melalui via pos, kurir, saluran telekom dll atau disimpan dalam storage speerti *disk*, kaset, dan CD.

Pesan yang telah disandikan sehingga tidak bermakna lagi dapat disebut cipherteks. Tujuan dari cipherteks adlaah agar pesan tidak dapat dibaca pihak lain yang tidak diinginkan. Nama lain dari cipherteks adalah kriptogram.

Enkripsi (encryption) adalah proses menyandikan plainteks menjadi teks atau juga dapat disebut *enciphering*. Proses ini dapat menggunakan algoritma enkripsi yang bermacam-macam sehingga dihasilkan cipherteks dengan kualitas bermacam-macam.

Dekripsi (decryption) adalah proses mengembalikan cipherteks menjadi plainteks yang dapat dibaca atau diambil mkana informasinya. Nama lainnya adalah proses *dechipering*.

Berikut ilustrasi proses enkripsi dan dekripsi



Secara umum system kriptografi (*cryptosystem)* terdiri dari :

- Algoritma kriptografi
- Plainteks
- Cipherteks
- Kunci

Kriptografi pada jaman modern dapat disamakan dengan proses enkripsi, yaitu proses mengkonversi informasi dari state yang dapat dibaca hingga menjadi informasi yang tidak bermakna apa-apa. Pengirim informasi dapat melakukan proses dekripsi sehingga data yang tidak bermakna tersebut dapat dikonversi kembali menjadi informasi yang bermakna.

Kriptografi tidak menjamin data yang di enkripsi akan sepenuhnya aman dari orang-orang yang tidak berhak. Kriptanalisis berasal dari bahasa yunani yang berasal dari gabungan kata *kryptos* dan *analyein* yang berarti "to losen" jadi kriptanalisis adlaah ilmu yang mempelajari metode-metode untuk mendapatkan informasi yang dikandung dari sebuah data yang dienkripsi. Biasanya proses ini dilakukan dengan melakukan *codebreaking* atau *cracking the code*. Kriptanalisis bekerja dengan mencari tahu bagaimana sebuah system enkripsi bekerja ataupun mencari kunci rahasia yang digunakan untuk proses enkripsi.

Sebelum jaman modern, kriptografi semata-mata

berfokus pada kerahasiaan pesan, yaitu menkonversi pesan dari susunan yang dapat dimakna menjadi pesan yang susunannya tidak dapat dimakna dan dilakukan proses sebaliknya ketika sampai di penerima.

Algoritma kriptografi dapat dikelompokkan menjadi dua kelompok yaitu algoritma kriptografi classic dan algoritma kriptografi modern.

Algoritma kriptografi classic terdiri dari beberapa jenis. Pertama adalah substitution yaitu mengganti suatu huruf pada plainteks menjadi huruf lain yang bersesuaian. Salah satu aplikasi yang terkenal adalah Caesar cipher.

Kedua adalah Polyalphabetic substitution yaitu mengganti suatu huruf sesuai dengan kunci yang digunakan sehingga dihasilkan cipherteks yang berubah-ubah sesuai dengan key yang diberikan. Salah satu contoh adalah Vigenere Cipher.

Ketiga adalah Polygraphic yaitu dilakukan substitusi yang seragam terhadap blok atau huruf-huruf yang berpasangan. Algoritma yang menggunakan prinsip ini adalah Playfair Cipher.

Keempat adalah Transposition Cipher yaitu merubah posisi huruf-huruf pada plainteks untuk mendapatkan cipherteks. Algoritma-algoritma yang menggunakan prinsip ini adalah seperti Rail Fence Cipher, Route Cipher, Columnar Transposition, Double Transposition, Disrupted transposition. Scytale termasuk kriptografi classic yang menggunakan proses dekripsi dengan menyusun huruf-huruf pada cipherteks dalam sebuah batang pohon.

Algoritma kriptografi modern terbagi menjadi dua yaitu simetric-key algorithm dan asymmetric-key algorithm. Secara garis besar simetric-key algorithm melakukan proses enkripsi dan menggunakan proses dekripsi dengan kunci yang sama untuk suatu pesan. Jadi jika kita melakukan proses enkripsi terhadap suatu pesan dengan menggunakan suatu kunci maka untuk melakukan proses dekripsi agar mendapatkan plainteks harus menggunakan kunci yang sama. Sedangkan pada asymmetric-key algorithm kunci untuk melakukan proses enkripsi dan dekripsi berbeda yaotu disebut public key dan private key. Algoritma-algoritma yang menggunakan kriptografi modern adalah speerti DES, Rijndael dll.

Pada makalah ini penulis akan berfokus pada algoritma kriptografi classic yaitu transpositional cipher. Algoritma yang dipilih penulis adalah Rail Fence Cipher, Columnar Transposition dan Scytale. Ketiga algoritma tersebut akan dibuat sebuah aplikasi sederhana untuk melakukan kriptanalisis terhadap cipherteks untuk mendapatkan plainteks. Karena transpositional cipher bergantung dari peletakan huruf-huruf yang berkesuaian maka aplikasi yang dikembangkan penulis akan membantu pengguna untuk memecahkan cipherteks yang diberikan.

Rail Fence Cipher, Columnar Transposition dan Scytale adalah contoh bentuk kriptografi sederhana. Algoritma yang digunakan sangat sederhana yaitu dengan merubah posisi huruf-huruf pada plainteks sehingga menjadi cipherteks. Ketiga jenis kriptografi tersebut menggunakan metode yang berbeda-beda untuk merubah posisi huruf pada plainteks sehingga untuk melakukan proses decrypt perlu dilakukan langkah-langkah yang sesuai. Meskipun sederhana, akan tetap menyulitkan kita ketika harus dilakukan secara manual atau dengan menuliskan diatas kertas. Oleh sebab itu perlu dibuat aplikasi sederhana yang dapat membantu proses dekripsi terhadap cipherteks hasil algoritma tersebut. Selanjutnya akan dilihat bagaimana aplikasi yang telah dibuat akan membantu pengguna untuk memecahkan ciperteks yang telah dibuat dengan algoritma-algoritma diatas. Hasil yang diharapkan adalah pengguna akan lebih cepat memecahkan cipherteks menggunakan aplikasi ini dibandingkan dengan cara manual.

Ketika pengguna mencoba memecahkan suatu cipherteks tanpa bantuan aplikasi komputer, dia akan melakukan beberapa pekerjaan yang berulang dan akan membuang-buang waktu meskipun untuk algoritma kriptografi yang sangat sederhana seperti algoritma diatas. Dengan membuang pekerjaan yang berulang, maka proses pemecahan cipherteks akan lebih cepat.

Aplikasi simulasi yang dibuat akan memudahkan pengguna untuk melakukan proses dekripsi sekaligus memecahkan plainteks dari cipherteks yang diberikan. Namun aplikasi tidak dapat melakukan pemecahan ciperteks secara mandiri, aplikasi akan menerima input dari pengguna. Aplikasi hanya akan membantu, nilai-nilai yang dibutuhkan untuk memecahkan cipherteks sepenuhnya ditentukan oleh pengguna.

2. Scytale

Dalam kriptografi, cytale adalah alat untuk melakukan sebuah transposition cipher, terdiri dari sebuah silinder dengan sebuah kertas strip yang dililitkan pada silinder tersebut dan mulai dituliskan pesan yang ingin dienkripsi. Yunani kuno dan Spartans dikatakan telah menggunakan prinsip cipher ini untuk melakukan komunikasi dalam misi militer.

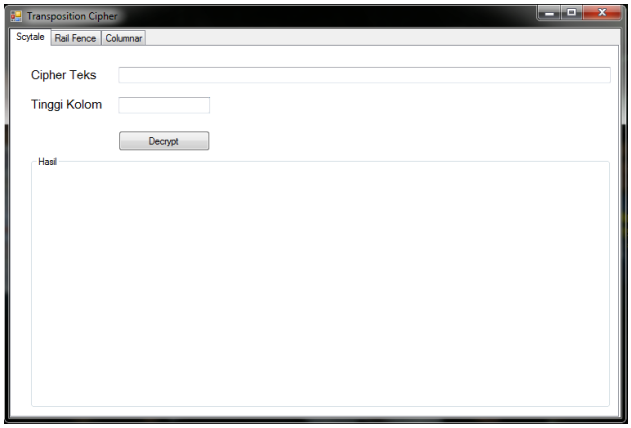
A Scytale

Penerima pesan menggunakan batang atau silinder

dengan diameter yang sama untuk melilitkan kertas cipherteks untuk membaca pesan yang dikandung plainteks.

Metode ini memiliki keuntungan yaitu cepat dan aman dari kesalahan dalam proses enkripsi maupun dekripsi meskipun sangat rentan untuk dipecahkan oleh pihak lawan.

Karena sifatnya yang rentan ataupun mudah untuk dipecahkan, pengguna mengembangkan sebuah aplikasi sederhana yang akan membantu mensimulasikan pemecahan cipherteks hasil dari Scytale. Berikut screenshot tampilan antarmuka aplikasi:



Antarmuka 1

Program ini menerima input cipherteks dan hipotesis diameter batang yang digunakan dalam satuan huruf. Cipherteks dimasukkan pengguna dalam bentuk string. Cipherteks ini akan disusun huruf demi huruf untuk membentuk sebuah susunan huruf yang dapat dibaca oleh pengguna untuk ditelusuri makna yang dikandungnya.

Penyusunan huruf disesuaikan dengan nilai tinggi kolom yang dimasukkan oleh pengguna. Jadi dengan mengilustrasikan sebuah batang yang digunakan untuk mendekripsi cipherteks menjadi dua dimensi yang berasal dari permukaan batang untuk melilitkan kertas cipherteks maka kita dapat melihat pesan plainteks yang dikandung dalam cipherteks. Format dua dimensi ini adalah sebuah segi empat dengan tinggi adalah jumlah huruf per kolom dan lebar adalah huruf-huruf dari cipherteks menyesuaikan tinggi kolom dan ukuran cipherteks.

Misal pengguna memasukkan cipherteks berupa “abcdefghijklmnopqrstuvwxyz”dengan panjang 26 dan tinggi kolom 6 maka aplikasi akan menyusun huruf-huruf pada cipherteks dalam sebuah segi empat dengan tinggi 6 huruf dan lebar yang dapat dihitung dengan rumus berikut :

```
Panjang = Ceil(Total Huruf  ÷ Tinggi Kolom)
```

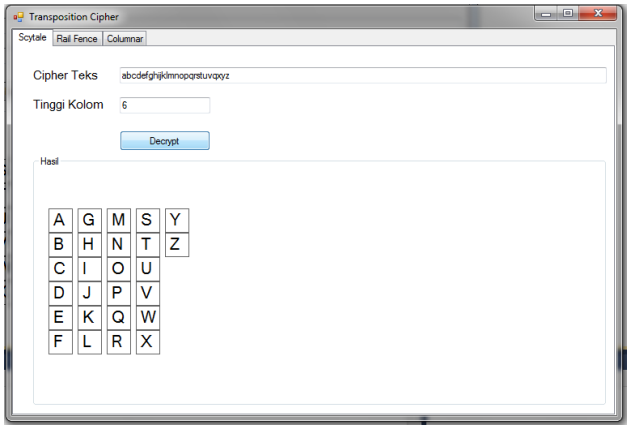
Fungsi ceil diatas adalah untuk menggenapkan hasil decimal, yang didapat dari pembagian antara total huruf dengan tinggi kolom, keatas. Sebagai contoh total huruf yang dimasukkan adalah 26 dan tinggi kolom adalah 6. Hasil pembagian antara 26 dan 6 adalah 4.3333 dengan fungsi Ceil terhadap 4.3333 kita mendapatkan nilai 5 untuk panjang segi empat susunan huruf.

Berikut ini hasil segiempat yang dihasilkan dari cipherteks yang diberikan diatas :

a	g	m	s	y
b	h	n	t	z
c	i	o	u	
d	j	p	v	
e	k	q	w	
f	l	r	x	

Hasil 1

Jika masalah diatas disimulasikan di dalam program maka hasilnya adalah :



Antarmuka 2

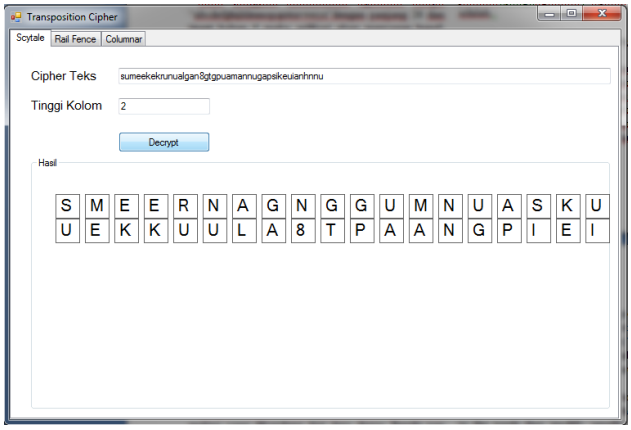
Setelah program dapat mensimulasikan pemecahan cipherteks hasil enkripsi menggunakan Scytale, perlu ditelusuri lebih lanjut efek dari penggunaan program ini dalam membantu pengguna memecahkan cipherteks.

Pengguna mencoba sendiri program yang telah dibuat dengan mencoba memecahkan cipherteks yang diberikan. Cipherteks diberikan oleh teman yang sengaja membuatnya untuk mencegah penulis mengetahui plainteks yang digunakan. Cipherteks yang diberikan adalah :

```
Sumeekekrunualgan8gtgpuamannugapsikeuianhnnu
```

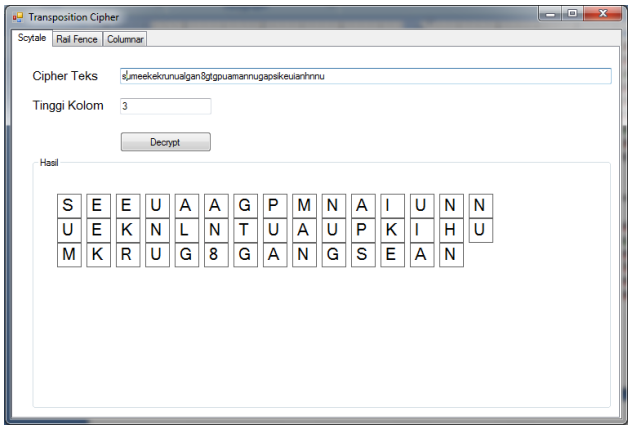
User mencoba memecahkan cipherteks diatas dengan progam simulasi ini. Langkah pertama yang dilakukan penulis adalah dengang memasukkan cipherteks diatas ke *field* cipherteks pada program simulasi. Selanjutnya penulis mulai mencoba memecahkan cipherteks dengan mulai mencoba berbagia kemungkinan nilai tinggi kolom

yang digunakan. Pertama penulis coba memasukkan nilai dua sebagai tinggi kolom. Dan program menghasilkan keluaran berikut ini :



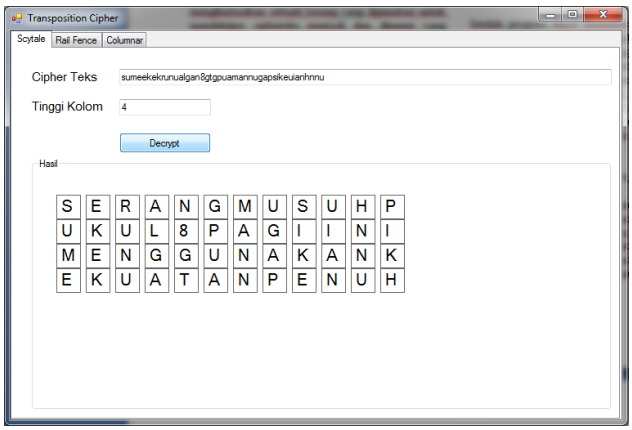
Antarmuka 3

Dengan melihat diatas penulis tidak bisa melihat makna yang dikandung dari data diatas. Penulis pun berkesimpulan bahwa tinggi kolom yang dimasukkan salah, oleh sebab itu penulis mencoba tinggi kolom yang lain. Dengan menggunakan metode exhaustive search, maka penulis mencoba nilai tiga untuk percobaan berikutnya, dan inilah hasilnya :



Antarmuka 4

Dengan melihat diatas penulis tidak bisa melihat makna yang dikandung dari data diatas. Penulis pun berkesimpulan bahwa tinggi kolom yang dimasukkan salah, oleh sebab itu penulis mencoba tinggi kolom yang lain. Kali ini penulis mencoba nilai empat untuk tinggi kolom dan hasilnya :



Antarmuka 5

Dengan melihat hasil diatas penulis mencoba kembali untuk mendapatkan makna dari hasil dan penulis berhasil mendapatkan informasi yang terkandung didalamnya yaitu:

Serang musuh pukul 8 pagi ini menggunakan kekuatan penuh

Dengan begitu penulis berkesimpulan bahwa silinder yang digunakan untuk membuat cipherteks diatas berdiameter empat huruf, sehingga untuk mendekripsinya menggunakan program simulasi yang telah dibuat adalah dengan memasukkan nilai empat pada tinggi kolom.

Penulis melakukan tiga kali percobaan memasukkan nilai tinggi kolom yaitu nilai dua, tiga, dan empat. Ketiga percobaan termasuk melihat apakah makna dari cipherteks sudah dapat diambil informasinya. Oleh sebab itu penulis membutuhkan waktu dibawah dua menit untuk memecahkan pesan tersebut, jauh lebih cepat dibandingkan cara manual atupun tanpa bantuan program apapun.

3. Rail Fence Cipher

Rail Fence Cipher atau nama lainnya zigzag cipher, adalah salah satu jenis transposition cipher. Dalam algoritma ini, plaintext dituliskan kebawah secara diagonal dalam “rel” yang berurutan, kemudian bergerak keatas ketika sudah mencapai dasar “rel”.paling bawah ketika kita kembali mencapai batas atas maka pesan dituliskan kembalai kebawah terus menerus sampai semua pesan selesai ditulis.

Sebagai contoh jika kita menggunakan 3 “rel” dan pesan yang dienkripsi sebgai berikut

WE ARE DISCOVERED. FLEE AT ONCE

Maka cipherteks yang dituliskan adalah sebgai berikut:

```
W . . . E . . . C . . . R . . . L . . . T . . . E
. E . R . D . S . O . E . E . F . E . A . O . C .
. . A . . . I . . . V . . . D . . . E . . . N . .
```

Dengan membaca secara mendatar atau horizontal maka kita akan mendapatkan cipherteksnya yaitu:

WECRL TEERD SOEEF EAOCA IVDEN

Pada kenyataannya Rail Fence Cipher sangat tidak aman untuk melakukan proses enkripsi terhadap suatu data. Cukup mengetahui jumlah rel yang digunakan untuk melakukan proses enkripsi maka kita akan dapat melakukan proses dekripsi terhadap cipherteks untuk mendapatkan plainteks.

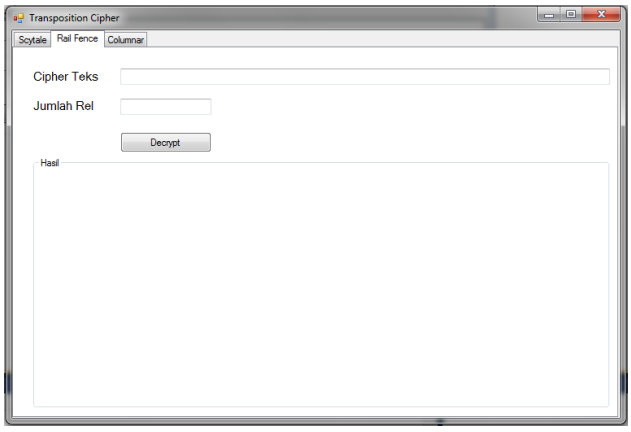
Untuk mensimulasikan bagaimana melakukan proses kriptanalisis terhadap cipherteks yang dihasilkan oleh algortma Rail Fence Cipher ini maka digunakan program simulasi yang telah dibuat untuk membantu proses kriptanalisis.

Penulis meminta kepada teman untuk dibuatkan sebuah cipherteks yang dibuat dari algoritma Rail Fence Cipher. Hal ini dilakukan agar penulis dapat benar-benar mensimulasikan proses kriptanalisis yang diinginkan. Berikut ini cipherteks yang diberikan:

BNNYEASEGUARKEPGGNASHMAAGGDIUNA

Proses kriptanalisis dilakukan dengna mencoba berbagai kemungkinan kunci yang dignakan untuk melakukan proses enkripsi, kunci dalam algoritma ini adlaah jumlah rel yang digunakan untuk melakukan proses enkripsi.

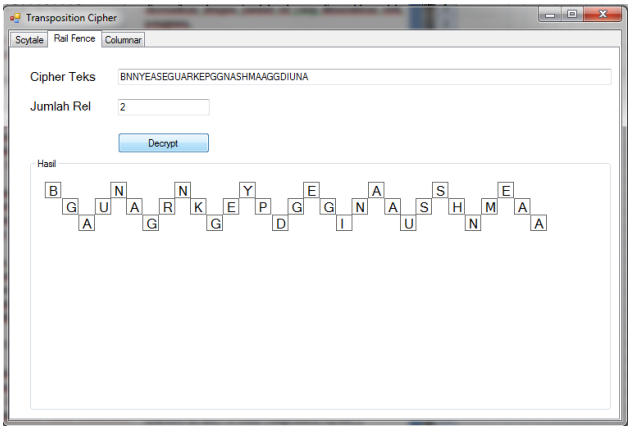
Untuk memecahkan cipherteks diatas penulis menggunakan program simulasi yang telah dibuat, berikut tampina antaramuka dasarnya:



Antarmuka 6

Field Cipher teks adalah tempat untuk memasukkan cipherteks yang ingin dicoba untuk dipecahkan. Cipherteks yang dimasukkan berupa string alfanumerik yang nantinya akan dipecah-pecah per huruf-huruf untuk nantinya dibentuk icon-icon dari label yang akan dimasukkan pada bagian hasil. Penyusunan huruf-huruf disesuaikan dengan jumlah rel yang dimasukkan oleh pengguna.

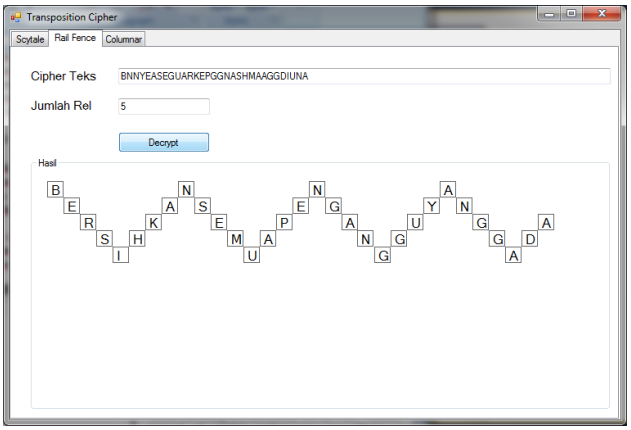
Penulis mulai mencoba memecahkan cipherteks yang telah diberikan dengan mencoba-coba nilai jumlah rel. dengan sedikit menggunakan heuristic dan asas coba-coba maka penulis tidak mencoba nilai satu dan dua sebagai nilai awal. Penulis mulai mencoba nilai tiga untuk mulai melakukan proses kriptanalisis berikut hasilnya:



Antarmuka 7

Penulis tidak dapat mengambil makana apapun dari hasil diatas, maka penulis beranggapan bahwa hasil diatas adalah salah karena jumlah rel yang dimasukkan tidak benar.

Berikutnya penulis mencoba lagi dengan jumlah rel yang lain, yaitu lima, penulis sengaja melompati nilai empat demi asas coba-coba yang lebih baik. Berikut ini hasil yang dikeluarkan oleh program simulasi:



Antarmuka 8

Dari hasildiatas penulis dapat melihat informasi yang dikandung, yaitu:

BERSIHKAN SEMUA PENGGANGGU YANG ADA

Dari dua percobaan, penulis berhasi mendapatkan informasi yang terkandung didalam cipherteks, hal ini sangat membantu pengguna untuk melakukan proses kriptanalasis terhadap suatu cipherteks.

4. Columnar Transposition

Dalam Colunar transposition, pesan ditulis daam baris-baris dengan panajng yang fix dan kemudian dibaca kolom per kolom dan kolom dipilih dalam suatu fungsi tertentu. Jumlah kolom dan permutasi urutan dari kolom biasanya ditentukan oleh kata kunci. Sebagai Contoh dengan menggunakan kunci:

ZEBRAS

Kata tersebut memiliki panjang 6 yang berarti jumlah kolom pada untuk membentuk cipherteks adalah 6 dan permutasi ditentukan dengna urutan alphabetic yang dimiliki kata kunci tersebut, dalam kasus ini berarti "6 3 2 4 1 5".

Dalam Regular Columnar Transposition Cipher, jika terdapat kolom kosong maka akan disisi dengna nilai null. Pada Irregular Columnar Transposition kolom kosaong tetap dibiarkan kosong.

Pada akhirnya pesan dibaca dalam kolom-kolm sesuai urutan kata kunci, sbeagai contoh kita menggunakan kata kunci diatas yaitu "ZEBRAS" dan pesan yang ingin dienkripsi adalah:

WE ARE DISCOVERED. FLEE AT ONCE

Dalam Regular Columnar transposition pesan kita tuliskan dalam kolom-kolom sehingga menjadi:

```
6 3 2 4 1 5
W E A R E D
I S C O V E
R E D F L E
E A T O N C
E Q K J E U
```

Hasil 2

Hasil diatas setelah menambahkan null (QKJEU) di akhir. Kemudian cipherteks dibaca sesuai urutan kolom sehingga didapatkan:

EVLNE ACDTK ESEAQ ROFOJ DEECU WIREE

Berbeda lagi dengan Irregular Columnar Transposition yang akan menghasilkan kolom-kolom sabgai berikut:

```
6 3 2 4 1 5
W E A R E D
I S C O V E
R E D F L E
E A T O N C
E
```

Hasil 3

Sehingga cipherteks yang dihasilkan adalah:

EVLNA CDTES EAROF ODEEC WIREE

Untuk melakukan proses dekripsi, penerima pesan harus membuat kolom-kolom sesuai panajng key, dengan membagi-bagi cipherteks sesuai dengan jumlah huruf pada key. Kemudain kata-kata yang telah dibagi bagi ini disusun sesuai urutan kolom yang didapat dari alphabet kata kunci.

Sayangnya penulis belum berhasil membuat program simulasi yang bias digunakan untuk melakukan simulasi pemecahan cipherteks yang dihasilkan oleh algoritma Columnar Transposition baik yang Regular ataupun Irregular.

Penulis menghabiskan waktu cukup banyak untuk membuat algoritma Rail Fence Cipher dan disertai banyaknya tugas kuliah lain yang harus dikerjakan pada waktu ang bersamaan. Kedepannya penulis akan mencoba melengkapi program simulasi yang dibuat dengan menyelesaikan program simulasi untuk Columnar Transposition.

5. Kesimpulan

Transposition adalah metode yang sangat sederhan utnuk melakukan proses enkripsi terhadap suatau data. Dengna merubah posisi huruf, kata atapun data yang dikandung maka akan dihasilkan cipherteks. Namun cipherteks yang dihasilkan sangat rentan terhadap ancaman-ancaman dari pihak yang tidak berkepentingan.

Scytale sebagai metode enkripsi pesan yang sangat kuno yaitu menggunakan diameter suatu silinder untuk melakukan proses enkripsi terhadap suatu pesan agar tidak dapat dibaca musuh. Cipherteks yang dihasilkan oleh metode ini sangat mudah dipecahkan jika kita memiliki batang atau silinder yang berdiameter sama. Atapun menggunakna program simulasi yang telah dibuat ini tidak akan membutuhkan waktu lama untuk bias mendapatkan pesan yang terkandung dalam cipherteks.

Rail Fence Cipher juga sangat rentan terhadap ancaman kriptanalisis. Cukup dengna mencoba-coba menggunakan jumlah rel yang pasti adalah sbeuah bilangan integer yang sederhana, maka kita akan

mendapatkan plainteks dari cipherteks yang dimiliki.

Columnar transposition juga rentan, namun lebih kuat disbandingkan dua lagoritma diatas. Algoritma ini mengandlakan kata kunci sebagai penentu untuk melakukan proses dekripsi. Selain diambil panjang kunci, algoritma ini juga mengambil urutan laphabetik untuk menyusun cipherteks, sehingga kriptanalisis perlu dua langkah yaitu mengira-ngira panajng kunci dan urutan alphabetic kunci.

REFERENCES

[1] Robert Stinson, Douglas. "Cryptography: theory and practice". Chapman & Hall/CRC. 2006

[2] http://en.wikipedia.org/wiki/Transposition_cipher. tanggal akses: 20 Maret 2011.

[3] http://en.wikipedia.org/wiki/Topics_in_cryptography. tanggal akses: 20 Maret 2011.

[4] http://en.wikipedia.org/wiki/Cryptography. tanggal akses: 20 Maret 2011.

[5] http://www.cryptogram.org/cdb/aca.info/aca.and.you/chapter_09.pdf #RAILFE. tanggal akses: 20 Maret 2011.

[6] http://www.math.cornell.edu/~mec/2003-2004/cryptography/transposition/transposition.html. tanggal akses: 20 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, 22 Maretl 2011

ttd

Yudi Retanto 13508085