Modifikasi *Columnar transposition* Menggunakan Sebuah Fungsi Transposisi

Odit Ekwardo – 135 04 079
Jurusan Teknik Informatika ITB, Bandung, email: if14079@students.if.itb.ac.id

Abstraksi – *Komunikasi merupakan faktor penting dalam kehidupan manusia. Kini manusia semakin dipermudah oleh teknologi untuk menyampaikan informasi. Media–media komunikasi yang diciptakan manusia tersebut memang memudahkan penyampaian informasi, tapi di sisi lain penyampaian pesan melalui media tertentu tidak menjamin keamanan terhadap kerahasiaan pesan. Oleh karena itu dikembangkan ilmu kriptografi untuk menjaga keamanan informasi saat penyampaian melalui media informasi. Salah satu teknik kriptografi yang populer adalah Columnar transposition. Namun, Columnar transposition masih memiliki kelemahan, karena jika kunci telah ditemukan, akan mudah memecahkannya. Modifikasi terhadap teknik ini dapat dilakukan untuk mempersulit pemecahan kode. Salah satu caranya adalah dengan modifikasi menggunakan fungsi rancangan sendiri. Fungsi yang dirancang menggunakan permainan posisi berdasarkan teknik Transposition Cipher tanpa menggunakan kunci.* Cipherteks *yang dihasilkan enkripsi menggunakan modifikasi ini lebih rumit sehingga lebih sulit dipecahkan dari Columnar transposition biasa. Gabungan 2 fungsi transposisi menggunakan kunci (Columnar transposition) dan tanpa menggunakan kunci (fungsi rancangan) membuat* cipherteks *yangh dihasilkan akan sulit dipecahkan walaupun kunci telah berhasil ditemukan oleh kriptanalis karena ada proses transposisi lain yang tanpa menggunakan kunci.*

Kata Kunci*: Columnar Tansposition, Transposition Cipher.*

1 PENDAHULUAN

Dalam hidup manuasia salah satu faktor penting yang mempengaruhi kemajuan manusia adalah komunikasi. Tanpa komunikasi manusia tidak akan bisa berhubungan, berinteraksi dan bertukar pikiran untuk membuat sesuatu untuk kemajuan manusia itu sendiri dan menyampaikannya pada orang lain. Dilatarbelakangi oleh kebutuhan manusia tersebut, teknologi komunikasi dewasa ini maju dengan pesat. Dengan kemajuan teknologi tersebut, manusia dapat melakukan pengiriman pesan dengan mudah dimana saja dan kapan saja dengan menggunakan berbagai media.

Media–media komunikasi yang diciptakan manusia tersebut memang memudahkan penyampaian informasi, tapi di sisi lain penyampaian pesan melalui media tertentu tidak menjamin keamanan terhadap kerahasiaan pesan. Banyak pihak yang tidak bertanggung jawab memanfaatkan ketidakamanan tersebut untuk mencuri atau menyadap pesan milik orang lain untuk disalahgunakan.

Masalah keamanan pengiriman pesan mulai dikembangkan oleh manusia untuk melindungi para pengguna media informasi. Diantaranya dengan memperkenalkan teknologi kriptografi. Telah banyak algoritma kriptografi, baik kriptografi modern maupun klasik yang sudah diterapkan untuk menjaga keamanan suatu pesan. Konsep penggunaan kriptografi pada pengiriman pesan adalah dengan meng-enkripsi pesan yang dikirim menjadi cipherteks, kemudian si penerima men-dekripsi menjadi pesan asli. Dengan begitu, jika ada pihak yang menyadap pesan saat pengiriman, pesan yang disadap masih berupa cipherteks yang tidak memiliki arti.

Salah satu algoritma kriptografi klasik yang cukup populer adalah transposition *cipher*. *Cipher* transposisi ini memiliki berbagai macam bentuk dan algoritma, diantara contoh dari *cipher* transposisi ini adalah Rail Fence *Cipher*, Route *Cipher* dan Columnar *Cipher*. Yang akan dibahas pada makalah ini adalah Columnar *Cipher* yang memakai kunci berupa kata.

Columnar Cipher merupakan salah satu teknik kriptografi yang populer dan sudah cukup lama digunakan orang-orang, sehingga para kriptanalis di dunia pun sudah banyak yang menemukan cara untuk memecahkan teknik ini. Oleh karena itu dibutuhkan modifikasi dari teknik *Columnar transposition* ini, salah satunya dengan menggunakan fungsi .

Fungsi akan dibuat serumit mungkin untuk menyulitkan para kriptanalis untuk memecahkannya. Modifikasi *Columnar transposition* dengan fungsi diharapkan mampu meningkatkan keamanan dalam pengiriman pesan.

2 DASAR TEORI

2.1 Transposition *Cipher*

Di dalam kriptografi klasik, *Transposition Cipher* mengubah posisi suatu karakter dari plainteks ke posisi yang lain. Perubahan tersebut menyebabkan susunan karakter yang menyusun teks berubah. Secara matematika suatu fungsi bijektif yang digunakan pada

posisi-posisi karakter itu digunakan untuk enkripsi dan satu fungsi *invers* digunakan untuk dekripsi..
(http://wikipedia.org/Transposition Chiper)

2.2 *Columnar transposition*

Columnar transposition merupakan salah satu metode kriptografi dimana pesan dituliskan berderet dari suatu panjang yang ditetapkan, lalu dibaca kembali kolom per kolom dengan urutan pembacaan berdasarkan suatu kata kunci. Panjang deret ditentukan oleh panjang kata kunci. Urutan pembacaan kolom berdasarkan urutan abjad kata kunci, misalnya ZEBRAS menjadi "6 3 2 4 1 5". [3]

Misalkan ada sebuah pesan NAMA SAYA ODIT akan dienkripsi menggunakan transposisi kolumnar dengan kata kunci HOI maka proses enkripsinya akan menjadi seperti ini:

HOI → 1 3 2

1	3	2
N	A	M
A	S	A
Y	A	O
D	I	T

Hasilnya chipertext adalah NAYD ASAT MAOT.

3 HASIL DAN PEMBAHASAN

3.1 Perancangan Fungsi Enkripsi

Penulis merancang sebuah fungsi enkripsi sederhana yang terdiri dari 2 tahap, yaitu:

1. Mengacak urutan huruf pada pesan
   Pengacakan urutan huruf pada pesan dilakukan dengan aturan ganjil-genap. Langkah-langkah implementasi aturan tersebut adalah sebagai berikut:
   a. Memisahkan huruf-huruf yang berada pada posisi ganjil dan genap.
   b. Melakukan tahap a terhadap huruf-huruf kelompok ganjil dan genap menjadi kelompok ganjilganjil, ganjilgenap, genapganjil, dan genapgenap.
   c. Menggabungkan kembali huruf-huruf yang telah terpisah menjadi empat kelompok tersebut dengn aturan ganjilganjil-ganjilgenap-genapganjil-genapgenap.
2. Meng-*inverse* urutan huruf setelah diacak
   Menuliskan posisi huruf dari dari yang paling akhir hingga ke paling awal.

3.2 Perancangan Fungsi Dekripsi

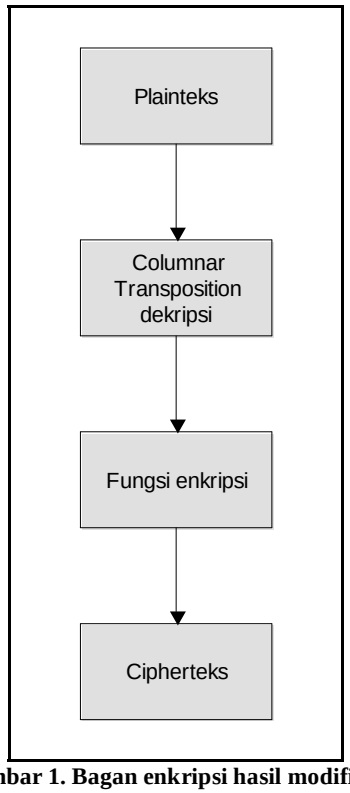
Penulis merancang sebuah fungsi dekripsi sederhana yang terdiri dari 2 tahap, yaitu:

1. Meng-inverse urutan huruf
   Menuliskan posisi huruf dari dari yang paling akhir hingga ke paling awal.
2. Mengacak urutan huruf setelah inverse
   Mengembalikan posisi huruf ke posisi semula sebelum diacak-acak menggunakan aturan ganjil-genap. Tahapan yang dilakukan adalah:
   a. Membagi pesan menjadi 2 bagian sama banyak. Jika jumlah huruf pada pesan adalah ganjil maka bagian pertama berjumlah lebih banyak 1 huruf dibandingkan dengan bagian kedua.
   b. Melakukan tahap a terhadap huruf-huruf kelompok pertama dan kedua. Hasil pembagian pada kelompok pertama menjadi bagian 1 dan bagian 2, sedangkan kelompok kedua menjadi bagian 3 dan 4.
   c. Menggabungkan keempat bagian yang telah terbentuk diatas pada posisi semula, dimana pada saat enkripsi bagian 1 adalah kelompok ganjilganjil, bagian 2 adalah kelompok ganjilgenap, bagian 3 adalah kelompok genapganjil, dan bagian 4 adalah genapganjil.

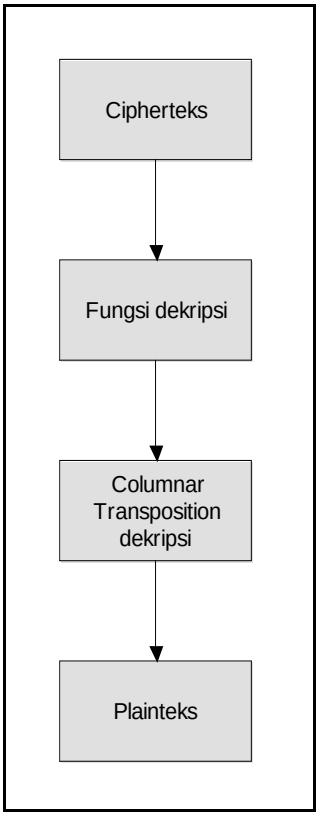
3.3 Hasil Modifikasi *Columnar transposition* menggunakan fungsi yang telah dirancang

Modifikasi yang dilakukan penulis dalam makalah ini adalah dengan memasukkan fungsi yang telah dirancang penulis pada langkah enkripsi dan dekripsi menggunakan *Columnar transposition*. Peletakkan penggunaan fungsi pada modifikasi ini adalah pada proses setelah *Columnar transposition* telah selesai dilakukan.

Untuk lebih jelasnya, proses enkripsi dan dekripsi pada *Columnar transposition* setelah dimodifikasi dapat dilihat pada bagan pada gambar berikut:



Gambar 1. Bagan enkripsi hasil modifikasi



Gambar 2. Bagan dekripsi hasil modifikasi

Penggunaan modifikasi *Columnar transposition* menggunakan fungsi dalam melakukan proses enkripsi dan dekripsi plainteks dapat dilihat pada contoh berikut:

Misalkan ada pesan "Bunuh dia nanti sore". Maka jika pesan tersebut di-enkripsi dengan kunci "KAMU", prosesnya sebagai berikut:

1. Melakukan *columnar transposition*
   KAMU → posisi abjadnya "2 1 3 4"

2	1	3	4
B	U	N	U
H	D	I	A
N	A	N	T
I	S	O	R
E			

   Hasil transposition →
   UDA SBH NIE NIN OUA TR

2. Menjalankan fungsi yang telah dirancang
   a. Memisahkan huruf-huruf yang berada pada posisi ganjil dan genap
      Ganjil → UABNEIOAR
      Genap →DSHINNUT

   b. Melakukan tahap a pada Ganjil dan Genap
      ganjilganjil → UBEOR
      ganjilgenap → ANIA
      genapganjil → DHNU
      genapgenap → SINT

   c. Menggabungkan kembali huruf-huruf yang telah terpisah menjadi empat kelompok tersebut dengn aturan ganjilganjil-ganjilgenap-genapganjil-genapgenap.
      Hasil dari tahap ini →
      UBE ORA NIA DHN USI NT
   d. Menuliskan posisi huruf dari dari yang paling akhir hingga ke paling awal.
      Hasil dari tahap ini →
      TNI SUN HAD INA ROE BU

Maka diperoleh cipherteks hasil enkripsi sebagai berikut: TNI SUN HAD INA ROE BU

Untuk mendapatkan plainteks, akan dilakukan proses dekripsi oleh penerima pesan. Prosesnya sebagai berikut:

1. Menjalankan fungsi dekripsi
   a. Menuliskan posisi huruf dari dari yang paling akhir hingga ke paling awal
      Hasilnya → UBE ORA NIA DHN USI NT
   b. Membagi pesan menjadi 2 bagian sama banyak. Jika jumlah huruf pada pesan adalah ganjil maka bagian pertama berjumlah lebih banyak 1 huruf dibandingkan dengan bagian kedua.

      Jumlah huruf ada 17. Jika dibagi 2 grup maka masing-masing grup terdiri dari 9 dan 8 huruf. Grup awal 9 huruf pertama, grup akhir 8 huruf terakhir.
      Hasilnya:
      Kelompok 1 (Posisi 1-9): UBE ORA NIA
      Kelompok 2 (Posisi 10-17): DHN USI NT

   c. Melakukan tahap b untuk tiap kelompok pada tahap b.
      Hasilnya →
      Bagian 1 (ganjilganjil): UBEOR
      Bagian 2 (ganjilgenap): ANIA
      Bagian 3 (genapganjil): DHNU
      Bagian 4 (genapgenap): SINT

   d. Menggabungkan keempat bagian yang telah terbentuk diatas pada posisi semula. Caranya dengan menggabungkan bagian 1 dan 2 terlebih dahulu, lalu bagian 3 dan 4, baru mwnggabungkan semuanya.
      Hasilnya →
      Bagian 1 dan 2 (Ganjil) → UABNEIOAR
      Bagian 3 dan 4 (Genap) → DSHINNUT
      Penggabungan keduanya →
      UDASBHNIENINOUATR

2. Menjalankan *Columnar transposition* dekripsi
   Dengan menggunakan kata kunci "KAMU", kita dapat mendekripsi cipherteks menjadi plainteks.

Pertama, kita tentukan posisi abjad huruf-huruf pada kunci "KAMU", yaitu: 2 1 3 4.

Kedua, kita bagi cipherteks menjadi 4 bagian. Empat karena kunci terdiri dari 4 huruf. Butuh cara tersendiri untuk menentukan anggota tiap bagian jika jumlah huruf pada pesan bukan merupakan kelipatan dari jumlah huruf pada kunci. Jika kita bagi 17 dan 4 hasilnya adalah 4 dan sisa 1. Berarti ada satu bagian yang jumlah hurufnya ada 5. Bagian yang memliki anggota 5 huruf adalah kelompok 2 karena kelompok 2 mewakili huruf 'K' yang merupakan huruf pertama pada kunci. Maka hasil pembagiannya adalah sebagai berikut:
Bagian 1 (mewakili huruf 'A'): UDAS
Bagian 2 (mewakili huruf 'K'): BHNIE
Bagian 3 (mewakili huruf 'M'): NINO
Bagian 4 (mewakili huruf 'U'): UATR

Ketiga, kita susun bagian-bagian tersebut dimana tiap bagian membentuk satu kolom dengan huruf-huruf pada kunci diurutkan pada *header* kolom. Hasilnya adalah sebagai berikut:

'K'	'A'	'M'	'U'
B	U	N	U
H	D	I	A
N	A	N	T
I	S	O	R
E			

Setelah itu, kita baca pesan tersebut per *row*, sehingga didapat plainteks yang dicari, yaitu:
"Bunuh dia nanti sore"

3.4 Perbandingan cipherteks hasil modifikasi dengan sebelum modifikasi

Dapat dilihat bahwa cipherteks yang dihasilkan menggunakan tambahan fungsi lebih rumit dan sulit ditebak dibandingkan dengan cipherteks yang dihasilkan *columnar transposition* biasa. Hal ini disebabkan karena setelah dimodifikasi, *columnar transposition* tidak hanya menggunakan permainan kunci tapi aturan pergeseran tanpa menggunakan kunci. Biasanya jika telah ditemukan bahwa suatu plainteks telah dienkripsi menggunakan kunci, kriptanalis akan mengira plainteks dapat ditemukan hanya dengan menggunakan kunci. Dengan begitu kriptanalis harus memutar otak lebih keras untuk memecahkan cipherteks hasil enkripsi menggunakan modifikasi ini.

4 KESIMPULAN

Dari berbagai macam pembahasan dan penelitian yang telah dilakukan untuk membuat makalah ini, penulis dapat mengambil kesimpulan, yaitu:

1. *Columnar transposition* merupakan salah satu teknik kriptografi klasik yang menggunakan pergeseran posisi menggunakan kata kunci sebagai inti dari algoritma untuk emkripsi dan dekripsi teks.
2. Fungsi yang dibuat untuk memodifikasi *Columnar transposition* juga menggunakan perpindahan posisi tanpa kunci dalam implementasinya.
3. Modifikasi terhadap *Columnar transposition* menggunakan fungsi rancangan penulis telah menghasilkan cipherteks yang jauh lebih rumit dan sulit dipecahkan karena menggunakan perpaduan transposisi menggunakan kunci dan tanpa kunci.

DAFTAR REFERENSI

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

[2] Forouzan, Behrouz, *Cryptography and Network Security*, McGraw-Hill, 2008.

[3] http://en.wikipedia.org/wiki/Transposition_Chiper