STUDI MENGENAI TEKNIK IMPROVISASI DALAM ALGORITMA KRIPTOGRAFI KLASIK DAN IMPLEMENTASINYA

Hardani Maulana – NIM : 13503077

Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if13077@students.if.itb.ac.id

ABSTRAKSI

Makalah ini membahas mengenai studi teknik improvisasi yang dapat digunakan dalam implementasi algoritma kriptografi klasik. Pembahasan yang dilakukan adalah pada beberapa teknik improvisasi yang dapat digunakan dalam algoritma kriptografi klasik dan juga implementasi dari teknik improvisasi tersebut dalam beberapa algoritma kriptografi klasik. Pada penggunaannya sebelum zaman komputerisasi, teknik improvisasi ini dapat meningkatkan kerumitan penyandian yang didapatkan dari sebuah algoritma kriptografi klasik walaupun hanya dengan menggunakan alat kertas dan alat tulis.

Teknik improvisasi yang cukup terkenal adalah *columnar transposition, playfair,* dan *straddling checkerboard.* Teknik tersebut sering dipakai dalam algoritma kriptografi yang rumit. Selain itu masih ada beberapa teknik lainnya yang dapat dipelajari. Teknik-teknik tersebut rata-rata merupakan pengembangan dari dua teknik utama dalam kriptografi, substitusi dan transposisi. Beberapa algoritma kriptografi klasik yang telah menggunakan teknik improvisasi adalah VIC *cipher,* SECOM *cipher,* dan PPC-xx. Algoritma-algoritma tersebut terkenal cukup aman pada zamannya karena algoritma tersebut yang cukup kompleks.

Kriptografi klasik merupakan awal dari perkembangan kriptografi yang pada zaman modern ini telah semakin berkembang dan sangat berguna sebagai teknik penyandian informasi. Apalagi dengan semakin tingginya penggunaan jaringan dan alur informasi data yang berpindah menuntut teknik penyandian yang lebih baik lagi. Semakin kompleks sebuah algoritma kriptografi, maka akan semakin sulit dipecahkan. Teknik improvisasi dapat berperan dalam hal ini. Kriptografi modern yang digunakan saat ini sebenarnya juga masih menerapkan teknik substitusi dan transposisi layaknya algoritma klasik. Namun kriptografi modern berjalan dalam pemrosesan bit, bukan hanya karakter seperti algoritma klasik.

Pengembangan dan pengimplementasian yang tepat dari teknik-teknik improvisasi dalam penciptaan sebuah algoritma kriptografi dapat menghasilkan *cipher* dengan tingkat keamanan tinggi. Apalagi dengan teknologi masa kini yang menghasilkan kriptografi modern dengan mesin komputer. Karena itu perlu dilakukan pengkajian yang lebih dalam mengenai beberapa teknik tersebut serta melihat pengimplementasiannya dalam algoritma yang sudah ada. Dengan demikian dapat menjadi dasar pengetahuan yang berharga dalam pengembangan teknologi kriptografi.

Kata kunci: kriptografi klasik, teknik improvisasi, *cipher*

1. Pendahuluan

Dalam dunia kriptografi, terdapat dua klasisifikasi yaitu kriptografi klasik dan kriptografi modern. Algoritma kriptografi klasik merupakan teknik kriptografi yang digunakan pada awal mula sejarah kriptografi. Penggunaannya berbasis pada karakter (seperti ”A-Z”), dan diimplementasikan dengan tangan atau mesin sederhana. Skema klasik yang digunakan dalam pembuatan algoritma kriptografi klasik pada umumnya merupakan skema yang sederhana, karena awalnya hanya dibuat dengan menggunakan tangan. Sehingga pada umumnya kriptografi klasik mudah diserang dengan teknik-teknik kriptanalisis standar seperti analisis frekuensi. Dalam perkembangannya muncullah mesin sederhana yang digunakan sebagai alat bantu penggunaan

kriptografi klasik ini untuk meningkatkan tingkat kerumitan algoritma yang digunakan.

Teknik kriptografi klasik dibagi menjadi dua, yaitu dengan teknik transposisi dan substitusi. Untuk penggunaannya lebih lanjut agar menghasilkan skema yang lebih kompleks digunakan beberapa teknik improvisasi dari teknik-teknik tersebut. Beberapa teknik yang bisa digunakan diantaranya adalah *homophonic*, *nomenclator*, *polygraphic*, *fractination*, *straddling checkerboard*, dan masih banyak lagi. Pembuatan algoritma kriptografi klasik dengan menggunakan teknik improvisasi ini nantinya dapat juga diimplementasikan ataupun dijadikan sebagai ide dalam pembuatan kriptografi modern. Sehingga menciptakan algoritma kriptografi yang tingkat keamanannya tinggi.

Sejauh ini ada beberapa *cipher* buatan tangan (disebut *pencil and paper cipher*) yang cukup kompleks dan terbilang cukup aman. Beberapa diantaranya adalah VIC *cipher*, SECOM *cipher*, dan PPC-xx. *Cipher-cipher* tersebut menggunakan teknik-teknik improvisasi dalam algoritma kriptografi klasik. Sehingga menghasilkan *cipher* yang cukup kompleks. C*ipher-cipher* tersebut membuktikan betapa kuatnya sebuah teknik enkripsi yang bisa didapatkan walaupun tanpa bantuan mesin ataupun program komputer.

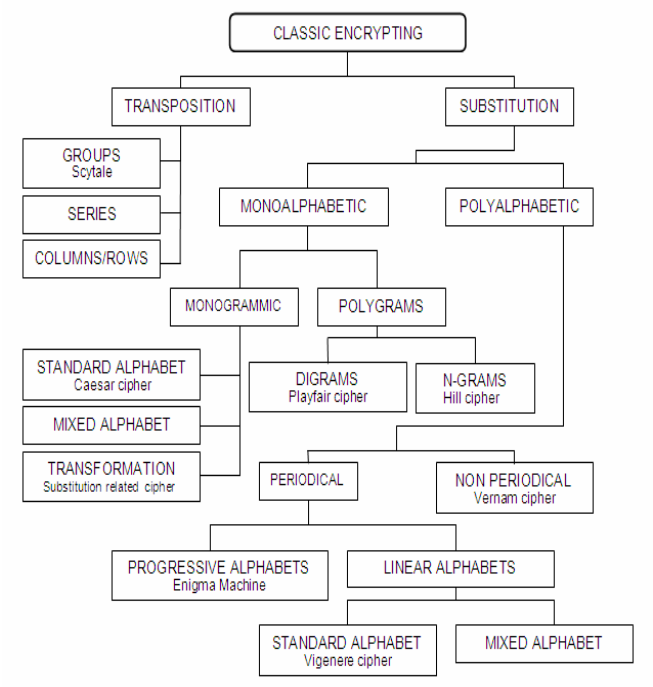
Sedangkan algoritma kriptografi yang berkembang pada zaman modern ini adalah kriptografi modern, yang beroperasi dalam bit atau *byte*, tidak seperti kriptografi klasik yang hanya beroperasi pada karakter. Namun pada prinsipnya metode yang digunakan pada kriptografi modern digunakan pula pada kriptografi klasik, namun dengan bantuan komputer dapat dibuat sedemikian rupa sehingga menjadi lebih rumit.

2. Klasifikasi Kriptografi Klasik

Enkripsi adalah teknik penyembunyian pesan sehingga tidak dapat terbaca oleh pihak yang tidak berhak. Sehingga, tujuan dasarmya adalah untuk mengelola keamanan data dalam lingkungan jalur transmisi atau penyimpanan data yang kita lihat tidak aman. Sebagai teknik perlindungan, akan digunakan metode atau algoritma untuk mengenkripsi informasi. Selanjutnya teknik enkripsi diklasifikasikan menjadi kriptografi klasik dan modern seperti yang telah dijelaskan pada bab pendahuluan.

Kriptografi klasik adalah metode enkripasi yang digunakan tanpa bantuan mesin. Teknik substitusi dan transposisi digunakan secara terpisah dan diaplikasikan pada karakter dari plainteks. Atau disebut juga beroperasi pada mode karakter. Teknik kriptografi jenis ini digunakan dengan orientasi kunci rahasia dan juga algoritma rahasia yang sebenarnya tergantung pula kepada kunci rahasia. Operasi enkripsi dilakukan dalam bentuk karakter, yang pada umumnya karakter alfabet, dan ditransmisikan serta disimpan dalam format yang sama.

Gambar berikut ini menunjukkan klasifikasi dari algoritma kriptografi klasik dan caontohnya yang diajukan oleh *Shannon*. Kriptografi klasik diklasifikasikan berdasarkan yang menggunakan teknik substitusi dan teknik transposisi.



3. Teknik Improvisasi Kriptografi Klasik

3.1. *Playfair*

Salah satu sistem poligraf yang paling terkenal adalah teknik *playfair cipher*. Cara kerjanya adalah dengan menggunakan kotak 5x5 yang berisi alfabet seperti berikut:

T X V H R
L K M U P

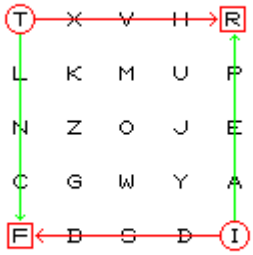
N Z O J E
C G W Y A
F B S D I

dengan menghilangkan sebuah huruf (karena jumlahnya hanya 25) menggunakan aturan: misal huruf Q direpresentasikan oleh KW; atau perlakukan I dan J, atau U dan V, sebagai satu huruf yang sama.

Selanjutnya, sepasang huruf dikonversikan menjadi cipherteks dengan menggunakan satu dari tiga aturan berikut yang mungkin dilakukan:

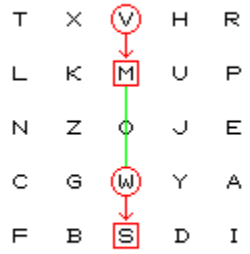
Aturan pertama: Bila dua huruf tidak terletak pada baris dan kolom yang sama, maka kedua huruf diganti dengan huruf yang berada pada baris yang sama dengan plainteks pertama dan kolom yang sama dengan plainteks kedua. Contoh: TI menjadi RF,, TW menjadi VC, KA menjadi PG, UB memjadi KD, WX menjadi GV.

T------>*R* **T**-->*V* H R
| K M U | | K | U P
| Z O J | | Z | J E
| G W Y | *C*<--**W** Y A
F<------**I** F B S D I



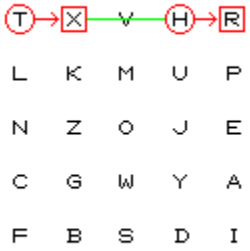
Aturan kedua: Bila dua huruf terletak pada kolom yang sama, maka kedua huruf diganti dengan huruf yang berada di bawah huruf tersebut, bila sudah berada di baris paling bawah maka putar lagi dari baris yang paling atas. Contoh: VW menjadi MS,, TN menjadi LC, TL menjadi LN, TF menjadi LT, KB menjadi ZX.

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



Aturan ketiga: Bila dua huruf terletak pada baris yang sama, maka kedua huruf diganti dengan huruf yang berada di kanan huruf tersebut, bila sudah berada di baris paling kanan maka putar lagi dari kolom yang paling kiri. Contoh: TH menjadi XR,, KP menjadi ML, NZ menjadi ZO.

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



Huruf kembar tidak diperbolehkan menjadi pasangan, maka harus dipisahkan dengan menyisipkan huruf yang berfungsi sebagai *null* (misalnya huruf X) di antara huruf tersebut.

Bila *playfair cipher* digunakan di computer, mungkin sebagai kombinasi dengan *cipher* lainnya, maka dapat dengan mudah membuat aturan dari huruf kembar, seperti menggunakan huruf yang berada satu baris di bawah dan satu kolom di kanan huruf tersebut lalu

melipatgandakannya menjadi dua. Misalnya EE menjadi CC.

3.2. *Bifid* dan *Trifid* dengan *seriation*

Teknik ini merupakan pengembangan dari teknik *playfair*. Dengan menggunakan kotak 5x5 seperti pada persoalan di atas, namun untuk setiap baris dan kolom diberikan nomor seperti berikut ini:

```
   1 2 3 4 5
   ---------
1) T X V H R
2) L K M U P
3) N Z O J E
4) C G W Y A
5) F B S D I
```

Lalu langkah berikutnya adalah membagi pesan menjadi panjang tertentu, misalkan lima huruf. Lalu tulis baris dan kolom koordinat setiap huruf pada kotak 5x5 seperti berikut ini:

```
THISI SMYSE CRETM ESSAG E
11555 52453 41312 35544 3
14535 33435 15513 53352 5
```

Selanjutnya urutkan setiap grup lima angka tadi dan mengubah setiap pasangan bilangan menjadi sebuah huruf: sehingga dibaca 11555 14535 52453 33435... lalu ubah sesuai huruf yang berkorespondansi dengan 11, 55, 51, 45, 35, 52, dan seterusnya.

```
1155514535 5245333435 4131215513
 T I F A E  B A O J E  C N L I V
3554453352 35
 E D A O B  E
```

Ini adalah *Bifid cipher*, dan prinsip umum dari bentuk *cipher* ini disebut *seriation.*. Teknik ini merupakan salah satu *pencil-and-paper ciphers* yang cukup aman dan masih dipakai dalam permainan *puzzle.* Tidak sulit untuk membuat *cipher* ini menjadi lebih kompleks, yaitu dengan metode *fractionation*, yaitu membagi huruf menjadi kelompok yang lebih kecil lagi. Dengan dua simbol dari 1 hingga 5 memberikan 25 huruf, tiga simbol dari 1 hingga 3 memberikan 27 huruf, dan lima bit memberikan 32 karakter alfabet.

Trifid, menggunakan 27 huruf alphabet yang direpresentasikan dengan tiga symbol dari 1 hingga 3:

```
W 111   M 121   Z 131   N 211   O 221   L
231   C 311   T 321   U 331
A 112   & 122   Y 132   E 212
V 222   P 232   X 312   J 322
G 332   K 113   B 123   H 133
Q 213   R 223   S 233   I 313
F 323   D 333
```

Untuk mengenkripsi pesan seperti berikut ini:

```
THISISM YSECRET MESSAGE
3132321 1223223 1222132
2313132 3311212 2133131
1333331 2321321 1233222
```

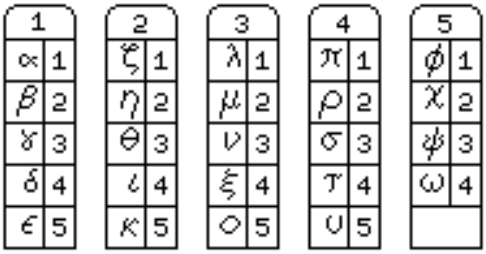
Selanjutnya simbol juga dibaca secara horizontal lalu vertikal, dan menghasilkan cipherteks berikut:

```
313 232 123 131 321 333 331
 I   P   B   Z   T   D   U

122 322 333 112 122 321 321
 &   J   D   A   &   T   T

122 213 221 331 311 233 222
 &   Q   O   U   C   S   V
```

Merepresentasikan huruf sebagai kombinasi dua grup 1 hingga 5 diajukan oleh Polybius dan menjadi metode umum dari komunikasi. Bentuknya adalah seperti berikut:



dengan huruf alfabet Yunani yang ditempatkan pada lima tablet bernomor, dan setiap huruf diberi nomor pada tablet.

Bentuk lain dalam membagi karakter menjadi kumpulan yang lebih kecil, seperti ASCII atau kode morse juga dikembangkan untuk

penggunaan komunikasi dalam tipe *channel* yang berbeda.

3.3. *Straddling Checkerboard*

Beberapa *cipher* yang digunakan oleh mata-mata Soviet menggunakan kotak seperti berikut ini:

```
    9 8 2 7 0 1 6 4 3 5
    -------------------
    A T   O N E   S I R
2   B C D F G H J K L M
6   P Q U V W X Y Z . /
```

Delapan huruf yang paling sering muncul dalam bahasa Inggris ditranslasikan kepada sebuah digit bilangan. Dua bilangan yang tidak dipakai dalam langkah pertama menjadi kombinasi dua bilangan untuk karakter sisa. Ini adalah contoh dari kode bervariabel panjang dengan properti prefix. Untuk karakter sisa memerlukan dua digit angka yang terdiri dari digit kolom dan baris. Setelah itu setiap kode yang tercipta dari bilangan tersebut dipisahkan dengan spasi. Inilah yang disebut sebagai properti prefix.

Sehingga digit kedua dari kode yang terdiri dari dua kombinasi bilangan akan menciptakan sebuah pengertian tersendiri yang tidak membingungkan. Sehingga konsep ini dapat bekerja dan digunakan dengan baik.

Sehingga untuk pesan SENDMONEY akan menjadi 4 1 0 22 52 7 0 1 66, atau, 41022 52 701 66 karena spasi yang digunakan untuk menunjukkan kapan dimulai tidak dibutuhkan. Bilangan pertama akan merepresentasikan apakah sebuah huruf disubstitusi menjadi satu atau dua buah bilangan.

Untuk kode yang lebih kompleks lagi adalah dengan menggunakan bilangan biner 0 dan 1, yang digunakan dalam bentuk data kompresi. Kode seperti ini yang paling terkenal adalah kode Huffman. Tapi bentuk ini hanya dapat diaplikasikan untuk kode yang simbolnya dimasukkan oleh algoritma yang spesifik.

Dalam VIC *cipher* yang digunakan oleh Reino Hayhanen, bilangan dibuat dengan *straddling checkerboard* yang kemudian dimasukkan ke dalam bentuk *columnar transposition* yang divariasikan dengan memilih area triangular dan mengisinya dengan plainteks.

3.4. *Fractionated Morse*

Kode morse adalah simbol dengan variable panjang yang terdiri dari titik (*dot*) dan garis bawah (*dash*), tapi tidak seperti *straddling checkerboard*, panjang dari simbol tidak tergantung dari *dot* dan *dash* di dalamnya. Namun spasi juga diperlukan sebagai tanda antar simbol.

Tapi pembagian menjadi beberapa fraksi masih memungkinkan menggunakan kode morse sebagai dasarnya. *Elementary Cryptanalysis*, by H. F. Gaines, memberikan *cipher* yang dirancang oleh M. E. Ohaver, disebut juga *mutilation cipher*. Cara bekerjanya adalah sebagai berikut:

Bagi pesan dalam kode morse menjadi dua bagian; kumpulan *dot* dan *dash*, serta bilangan yang menomori *dot* dan *dash* dalam merepresentasikan huruf. Lalu ambil bilangan, bagi menjadi n grup, dan balikkan posisi nomor dari setiap grup. Menggunakan bilangan yang telah transposisi sebagai petunjuk, dapat mengubah *string dot* dan *dash* menjadi huruf.

Tabel dari kode morse adalah sebagai berikut:

```
E  . CD he   I  .. DE [A]  S  ... D7 ra   H  .... C7 nu
                                          V  ...- B8 ku
                           U  ..- B3 u    F  ..-. C1 ti
                                          (1) ..-- C9 no
              A  .- B2 i   R  .-. C5 na   L  .-.. B6 ka
                                          (2) .-.- DB ro
                           W  .-- D4 ya   P  .--. C2 tu
                                          J  .--- A6 wo
T  - D1 mu   N  -. C0 ta   D  -.. CE ho   B  -... CA ha
                                          X  -..- CF ma
                           K  -.- DC wa   C  -.-. C6 ni
                                          Y  -.-- B9 ke
              M  -- D6 yo  G  --. D8 ri   Z  --.. CC hu
                                          Q  --.- C8 ne
                           O  --- DA re   (3) ---. BF sho
                                          (4) ---- BA ko

5       .....   5          6       -....   6
4       ....-   4          =       -...-   D2 me
(5)     ...-.              /       -..-.   D3 mo
3       ...--   3                  -..--   D5 yu
(6)     ..-..   C4 to      (c)     -.-..   B7 ki
Inter   ..-.-   D0 mi      Start   -.-.-   BB sa
        ..--.   DF [B]     (       -.--.   D9 ru
2       ..---   2                  -.---   B4 e
Wait    .-...   B5 o       7       --...   7
(9)     .-..-      yi      (e)     --..-   CB hi
+       .-.-.   DD n               --.-.   BC shi
        .-.--   C3 te      (f)     --.--   B1 a
        .--..      ye      8       ---..   8
(a)     .--.-   B0 -               ---.-   BD su
(b)     .---.   BE se      9       ----.   9
1       .----   1          0       -----   0
```

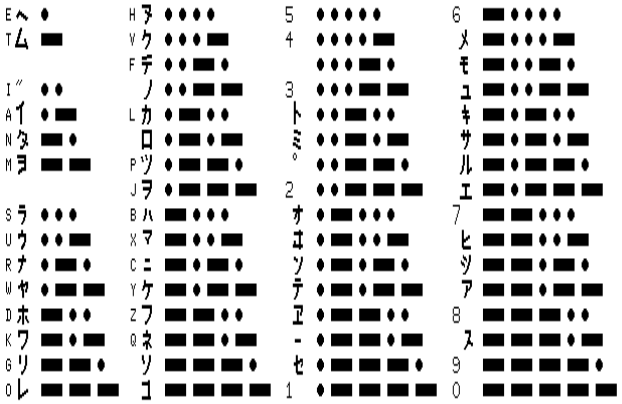
Dalam tabel tersebut terdapat dua tambahan tanda dalam bahasa Jepang:

[A] dua garis dalam kana (*nigori*), [B] lingkaran kecil dalam *kana* (*han-nigori*).

Terdapat juga aksen huruf dalam bahasa Turki:

(1) u umlaut (2) a umlaut, cedilla (3) o umlaut or other accent (4) ch, s cedilla (5) s hat (6) e primary accent (usually acute, grave in Italian) (9) e accent grave (a) a accent (b) j hat (c) c cedilla or accent (e) z accent grave (f) n tilde

Berikut ini adalah gambar penggunanaan seluruh *kana* dalam morse Jepang:



Walaupun dalam sistem aslinya menggunakan panjang grup sebagai kunci, sehingga tidak terlalu aman, namun konsep dasar yang digunakan cukup pintar dan orisinil. Panjang karakter dapat dengan mudah ditransposisi dengan teknik tertentu, lalu *dot* dan *dash* direpresentasikan dalam 0 dan 1, maka selanjutnya dapat dienkripsi dengan metode yang aplikatif.

3.5. *Columnar Transposition*

Langkah pertama dalam penggunaan teknik *columnar transposition* adalah dengan menggunakan kata kunci. Misalnya CONVENIENCE. Lalu me-*assign* bilangan ke setiap huruf dengan aturan: Pemberian angka dimulai dari satu kepada huruf pertama secara alfabet, dan diteruskan dengan nomor berikutnya untuk huruf yang sama atau urutan berikutnya dalam alfabet.

Lalu tulis pesan di bawah kata kunci dengan mengikuti kolom yang dibentuk oleh kata kunci. Sehingga menjadi seperti berikut:

```
C  O  N  V  E  N  I  E  N  C  E
1 10  7 11  3  8  6  4  9  2  5
--------------------------------
H  E  R  E  I  S  A  S  E  C  R
E  T  M  E  S  S  A  G  E  E  N
C  I  P  H  E  R  E  D  B  Y  T
R  A  N  S  P  O  S  I  T  I  O
N
```

Dengan membaca secara vertikal setiap kolom berdasarkan urutan angka pada kata kunci menghasilkan:

HECRN CEYI ISEP SGDI RNTO AAES RMPN SSRO EEBT ETIA EEHS

Untuk mempersulit spasi yang menunjukkan antar kolom yang digunakan tidak disertakan sehingga pesan menjadi:

HECRNCEYI ISEPSGDIRNTOAAESRMPN SSROEEBTETIAEEHS

Untuk membaca pesan ini, langkah yang harus dilakukan cukup sulit. Pertama harus dihitung jumlah huruf yang ada pada teks, dalam kasus ini 45 huruf, untuk menentukan jumlah huruf setiap kolom. Dengan informasi 45 huruf teks dan 11 huruf kata kunci, maka dapat ditentukan bahwa kolom pertama berisi lima huruf dan kolom lainnya berisi empat huruf.

Metode varian dari transposisi kolom yang dapat memproduksi *cipher* yang berbeda, terdapat pada buku yang ditulisi oleh General Luigi Sacco adalah sebagai berikut:

```
C  O  N  V  E  N  I  E  N  C  E
1 10  7 11  3  8  6  4  9  2  5
--------------------------------
H
E  R  E  I  S  A  S  E  C  R
E  T  M  E  S
S  A  G  E  E  N  C  I
P  H  E  R  E  D  B  Y  T  R  A
N  S  P  O  S  I  T
I  O  N
```

Setelah diurutkan berdasarkan indeks kata kunci setiap kolom menghasilkan:

HEESPNI RR SSEES EIY A SCBT
EMGEPN ANDI CT RTAHSO IEERO

Di sini, baris pertama hanya diisi hingga kolom dengan indeks kunci 1. Baris kedua diisi hingga kolom dengan indeks kunci 2, dan seterusnya. Metode ini melahirkan bentuk transposisis yang tidak biasa dibandingkan transposisi kolom biasa. Tentu saja hal ini dapat menambah kerumitan sebuah algoritma kriptografi.

Berbagai macam metode untuk memodifikasi transposisi kolom yang biasa untuk menciptakan variasi hasil enkripsi telah dilakukan dari waktu ke waktu.

3.6. *Turning Grille*

Pada Perang Dunia I, Jerman menggunakan sebuah papan *grille* kotak-kotak dengan sejumlah lubang yang sama pada sisi bilangan ganjil dan bilangan genap. Untuk itu kotak tengah ditandai untuk mengindikasikan bahwa kotak tersebut hanya digunakan dalam satu posisi *grille*.

Contoh dari *turning grille* dan penggunaannya:

Nomor grid:

```
 1  2  3  4  5 16 11  6  1
 6  7  8  9 10 17 12  7  2
11 12 13 14 15 18 13  8  3
16 17 18 19 20 19 14  9  4
 5 10 15 20  X 20 15 10  5
 4  9 14 19 20 19 18 17 16
 3  8 13 18 15 14 13 12 11
 2  7 12 17 10  9  8  7  6
 1  6 11 16  5  4  3  2  1
```

Layout:

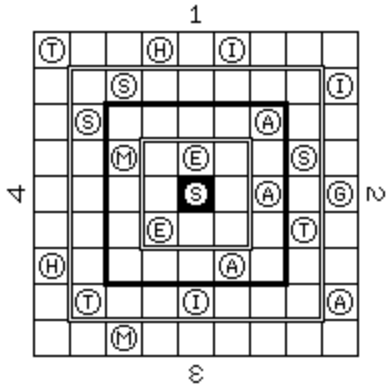
```
O - - O - O - - -  1     4  16
- - O - - - - - O     8          2
- O - - - - O - -   12        13
- - O - O - - O -     18  20     9
- - - - X - O - O          X  15   5
- - - O - - - O -       19       17
O - - - - O - - -  3        14
- O - - O - - - O    7     10       6
- - O - - - - - -     11
```

Masukkan pesan sesuai layout:

<u>Posisi pertama</u>

```
T    H  I        O - - O - O - - -
   S         I    - - O - - - - - O
 S        A       - O - - - - O - -
   M  E    S     - - O - O - - O -
     S  A  G     - - - - O - O - O
   E      T      - - - O - - - O -
 H       A       O - - - - O - - -
  T   I     A    - O - - O - - - O
    M             - - O - - - - - -
```

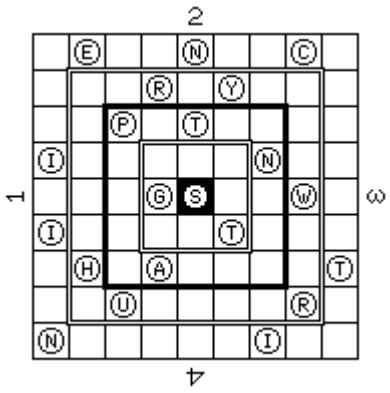
(this is a message that I am)

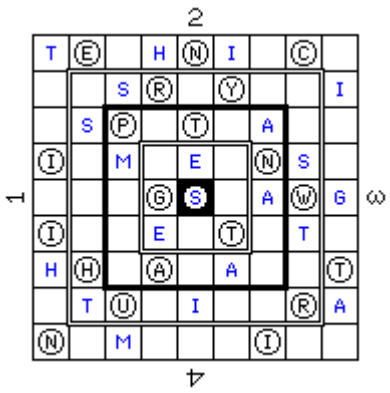


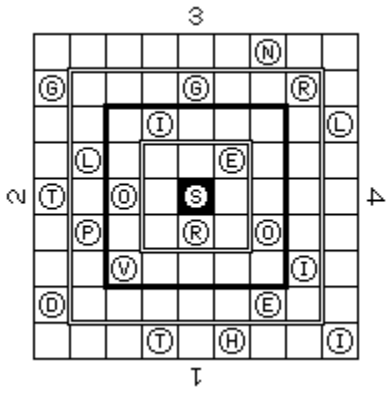
<u>Posisi kedua</u> diperoleh dengan memasukkan pesan berikutnya ke dalam layout yang didapat dari transposisi 90 derajat berlawanan arah jarum jam:

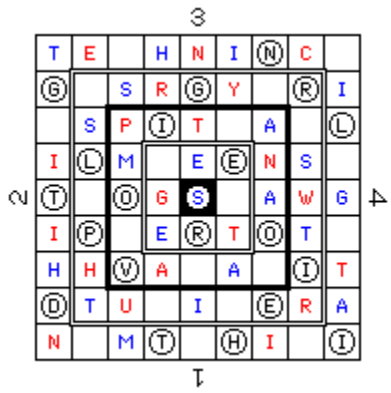
```
t E  h N i  C    - O - - O - - O -
   s R  Y   i    - - - O - O - - -
 s P  T  a       - - O - O - - - -
I  m  e  N s     O - - - - - O - -
     G s  a W g  - - - O . - - O -
I   e  T  t      O - - - - O - - -
h H  A  a  T     - O - O - - - - O
 t U  i   R a    - - O - - - - O -
N  m     I       O - - - - - O - -
```

(encrypting with a turni)









Posisi ketiga

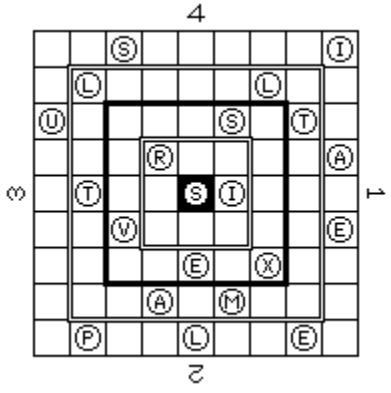
```
t e  h n i N c  - - - - - - O - -
G  s r G y  R i O - - - O - - O -
  s p I t  a  L - - - O - - - - O
i L m  e E n s  - O - - - O - - -
T  O g s  a w g O - O - . - - - -
i P  e R t O t  - O - - O - O - -
h h V a  a  I t - - O - - - - O -
D t u  i  E r a O - - - - - O - -
n  m T  H i  I - - - O - O - - O
```

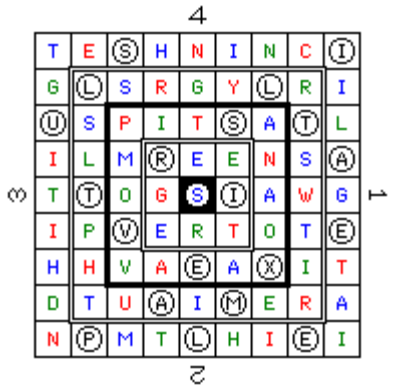
(ng grille to provide thi)

Posisi keempat

```
t e S h n i n c I - - O - - - - - O
g L s r g y L r i - O - - - - O - -
U s p i t S a T l O - - - - O - O -
i l m R e e n s A - - - O - - - - O
t T o g s I a w g - O - - . O - - -
i p V e r t o t E - - O - - - - - O
h h v a E a X i t - - - - O - O - -
d t i A i M e r a - - - O - O - - -
n P m t L h i E i - O - - O - - O -
```

(s illustrative example)





Untuk menghasilkan hasil enkripsi:

TESHN INCIG LSRGY LRIUS PITSA TLILM
REENS AITOG SIAWG IPVER TOTEH HVAEA
XITDT IAIME RANPM TLHIE I

Ada dua penggunaan penting dari transposisi yang berhubungan dengan substitusi *cipher*.

Transposisi bisa digunakan untuk menghasilkan huruf acak pada alfabet yang dapat digunakan pada substitusi.

4. Implementasi Teknik Improvisasi dalam *Plain and Paper Cipher*

4.1. VIC *Cipher*

VIC cipher merupakan *pencil and paper cipher* yang digunakan oleh mata-mata Uni Soviet Reino Hayhanen. Beberapa sumber mengatakan bahwa VIC chiper merupakan *pencil and paper cipher* yang paling kompleks yang pernah dibuat. Walaupun tidak sekompleks dan seaman *stream cipher* dan *block cipher* yang dioperasikan komputer modern, namun *cipher* ini menunjukkan kemampuan enkripsi yang kuat tanpa menggunakan mesin apapun. Dari penemuan *cipher* ini di tahun 1953, seluruh percobaan untuk memecahkan kode pesan berakhir dengan kegagalan. Hingga akhirnya pada tahun 1957 Hayhanen sendiri yang mengungkapkan rahasia teknik dekripsi pesan dari algoritma tersebut. VIC *cipher* menggunakan teknik penggenarasi bilangan acak dengan *chain addition, straddling checkerboard,* dan *disrupted double transposition*.

VIC *cipher* dimulai dengan cara membuat sepuluh bilangan *pseudorandom*. Agen mata-mata harus mengingat enam digit angka (untuk memudahkan biasanya diambil dari tanggal) dan 20 huruf dari frase kunci (untuk memudahkan misalnya awal dari lagu yang populer), serta lima bilangan acak yang digunakan sebagai bilangan indikator.

Misalkan tanggal yang digunakan adalah tanggal 4 Juli 1776, sehingga digit yang didapatkan (berdasarkan cara penulisan internasional) adalah 741776. Kemudian bilangan acak yang diambil adalah 77651.

Langkah pertama adalah dengan melakukan pengurangan digit per digit tanpa nilai bawaan (*carries*) pada lima digit pertama dari tanggal dengan bilangan indikator:

```
   77651
(-) 74177
-----------
   03584
```

Langkah kedua adalah menentukan 20 huruf frase dan mengubahnya menjadi 20 bilangan dengan cara membaginya menjadi dua bagian dan setiap bagian tersebut diberikan nomor urutan kemunculan huruf pada alfabet dari 1 untuk yang paling pertama hingga 0 untuk yang paling terakhir. Misalnya untuk frase kunci "I dream of Jeannie with t", langkah tersebut melakukan proses:

```
IDREAMOFJE ANNIEWITHT
6203189574 1674205839
```

Hasil dari langkah pertama (03584) kemudian diekspansi menjadi sepuluh bilangan melalui proses yang disebut *chain addition.* Cara kerjanya adalah sebagai berikut: Dimulai dengan sekelompok bilangan (pada kasus ini adalah lima digit bilangan, dan berikutnya nanti akan digunakan pada kelompok sepuluh bilangan), tambahkan dua digit pertama dari kelompok bilangan tersebut dan ambil hanya digit terakhir dari hasil penjumlahan kemudian tambahkan di akhir kelompok bilangan. Selanjutnya ulangi proses untuk dua bilangan berikutnya. Sehingga dari bilangan 03584 didapatkan bilangan sepuluh digit 0358**38327**.

Hasil tersebut ditambahkan digit per digit tanpa nilai bawaan dengan sepuluh bilangan pertama yang diproduksi frase kunci seperti berikut:

```
   6 2 0 3 1 8 9 5 7 4
(+)0 3 5 8 4 3 8 3 2 7
 -------------------------
   6 5 5 1 5 1 7 8 9 1
```

Sepuluh digit ini kemudian dikodekan dengan mengurutkan kesepuluh bilangan dari 1 hingga 0 sebagai sepuluh.

Menggunakan kode: 1 2 3 4 5 6 7 8 9 0
1 6 7 4 2 0 5 8 3 9

6 5 5 1 5 1 7 8 9 1
menjadi 0 2 2 1 2 1 5 8 3 1

Sepuluh digit ini digunaka untuk menggenerasi 50 bilangan pseudorandom dengan teknik *chain addition* untuk proses enkripsi:

```
 0 2 2 1 2 1 5 8 3 1
---------------------
 2 4 3 3 3 6 3 1 4 3
 6 7 6 6 9 9 4 5 7 9
 3 3 2 5 8 3 9 2 6 2
 6 5 7 3 1 2 1 8 8 8
 1 2 0 4 3 3 9 6 6 9
```

Baris terakhir dari 50 pseudorandom tersebut digunakan kembali untuk permutasi digit 1 hingg 9 seperti berikut ini:

```
 1 2 0 4 3 3 9 6 6 9
---------------------
 1 2 0 5 3 4 8 6 7 9
```

Dan digit tadi digunakan sebagai indeks dari *straddling checkerboard*:

```
 1 2 0 5 3 4 8 6 7 9
 -------------------
 A T   O N E   S I R
 -------------------
0 B C D F G H J K L M
8 P Q U V W X Y Z . /
```

Selanjutnya dengan *straddling checkerboard* ini dapat dimulai mengenkripsi pesan.

Misalkan pesan yang akan disampaikan adalah sebagai berikut:

“We are pleased to hear of your success in establishing your false identity. You will be sent some money to cover expenses within a month.”

Dengan mengkonversinya ke dalam table, maka akan didapatkan:

```
W EAREP L EASED TOH EAROF Y OU
RSU C C ESSINESTAB L ISH ING
83419481074164002504419505885809 6
80020246673462101077604730 3
```

```
Y OU RF AL SEID ENTITY Y OU W IL
L B ESENTSOM EM ONEY TOC O
88580905107647004327288885808370 7
07014643265094095348825025
```

```
V EREX P ENSESW ITH INAM ONTH
85494848143646837204731095320 4
```

Untuk contoh ini, diberikan nomor rahasia kepada agen. Dan nomor ini digunakan untuk membentuk lebar dari tabel transposisi yang akan digunakan untuk mentransposisi bilangan yang didapatkan di atas. Dua bilangan tidak sama terakhir pada baris terakhir dari 50 bilangan acak, dalam contoh ini 6 dan 9, ditambahkan dengan nomor rahasia dan hasilnya adalah jumlah kolom dalam dua transposisi akan dilakukan. Dalam kasus ini 8+6, atau 14, dan 8+9, atau 17.

Dua transposisi diambil dengan membaca 50 bilangan dan memasukkannya ke dalam kolom transposisi dengan sepulu bilangan kunci. Sehingga didapatkan tabel berikut ini:

```
 0 2 2 1 2 1 5 8 3 1
---------------------
 2 4 3 3 3 6 3 1 4 3
 6 7 6 6 9 9 4 5 7 9
 3 3 2 5 8 3 9 2 6 2
 6 5 7 3 1 2 1 8 8 8
 1 2 0 4 3 3 9 6 6 9
```

Dibaca dengan aturan urutan indeks seperti sebelumnya:

36534 69323 39289 47352 36270 39813 4

berhenti ketika mendapatkan 31 digit yang dibutuhkan.

Transposisi pertama menggunakan 14 bilangan pertama sebagai kunci dari transposisi kolom yang telah dijelaskan pada teknik improvisasi. Maka didapatkan hasil sebagai berikut:

36534693233928

83419481074164
00250441950588
58096800202466
73462101077604
73038858090510
76470043272888
85808370707014
64326509409534
88250258549484
81436468372047
3109532049

Didapatkan 149 digit. Agar dapat memenuhi pembagian grup yang tepat banyaknya maka ditambahkan satu digit *null*.

Sehingga, didapatkan bentuk pesan dengan kelompok sepuluh bilangan sebagai berikut:

09200274534 6860181384 80577786883 15963702539 11018309880
75079700479 4027027992 90628086065 42040483240 30833654811
44818035243 4864084447 84005470562 1546580540

Sisa 17 bilangan dari 31 yang telah kita baca sebelumnya, 9 47352 36270 39813 4, adalah kunci dari transposisi yang kedua. Bilangan tersebut akan mengindikasikan urutan kolom yang akan dituliskan dengan urutan segitiga.

Transposisi kedua menggunakan area triangular pertama berawal dari kolom pertama yang akan dibaca paling pertama (memiliki indeks paling kecil), dan dilanjutkan ke baris berikutnya. Pada baris pertama dituliskan sampai satu kolom sebelum indeks 1, lalu berikutnya dituliskan hingga kolom berikutnya, dan terus maju hingga bertemu akhir kolom. Setelah bertemu akhir kolom maka baris berikutnya berulang kembali dari kolom pertama, dan seterusnya.

Akhirnya didapatkan blok transposisi sebagai berikut:

94735236270398134

09200274534686
018138480577786
8831596370253911
01830988075079700
47940
270279
9290628
08606542
040483240

selanjutnya tempat kosong diisikan dengan sisa pesan yang belum terbaca. Sehingga kolom transposisi terisi sebagai berikut:

94735236270398134

09200274534686**308**
018138480577786**33**
883159637025391**16**
018309880750797**00**
4794**054811448180 3**
2702**795243486408 4**
9290**6284478400 547**
0860**6542056215 465**
0404**83248054 0**

Lalu dibaca sesuai urutan indeks dan hasil enkripsi akhir adalah sebagai berikut:

36178054 289959253 507014400 011342004 746845842 675048425
03100846 918177284 83603475 035007668 483882424 283890960
350713758 689914050 008042900 873786014 472544860

Terakhir, bilangan terakhir pada tanggal yang belum dipakai, yaitu 6, menunjukkan bilangan indikator disisipkan pada grup bilangan hasil enkripsi dengan posisi enam grup sebelum akhir. Sehingga pesan yang ditransmisikan adalah sebagai berikut:

36178 05428 99592 53507 01440 00113 42004 74684 58426 75048
42503 10084 69181 77284 83603 47503 50076 68483 88242 42838
90960 35071 37586 89914 05000 77651 80429 00873 78601 44725
44860

4.2. SECOM *Cipher*

SECOM cipher adalah *cipher* sederhana untuk mengenkripsi pesan yang menggunakan teknik-teknik: mengkalkulasi digit frase kunci, *straddling checkerboard*, dan *two columnar transpositions*. Kombinasi dari pengelompokan

dengan *checkerboard* dan transposisi yang mengacaukan posisi membuat SECOM menjadi sebuah metode enkripsi yang kuat.

Langkah enkripsi yang digunakan pada SECOM *cipher* akan ditunjukkan dalam contoh berikut ini:

Plainteks:

RV TOMORROW AT 1400PM TO COMPLETE TRANSACTION USE DEADDROP AS USUAL

Key Phrase:

MAKE NEW FRIENDS BUT KEEP THE OLD

Ambil 20 huruf pertama dari frase kunci dan bagi menjadi dua bagian. Untuk setiap bagian diurutkan dalam kemunculan pada alfabet dengan 1 untuk kelompok huruf pertama dan 0 untuk kelompok huruf yang terakhir.

Dengan kunci “Make new friends but kee” maka dihasilkan:

```
MAKENEWFRI ENDSBUTKEE
7162830495 3728109645
```

Selanjutnya 10 digit yang terbentuk ditambhankan tanpa mengindahkan bawaan, sehingga didapatkan hasil seperti berikut:

```
 7162830495
+3728109645
 ----------
 0880939030
```

Hasil berikut ini diekspan seperti dalam teknik VIC *cipher* sehingga didapatkan 50 bilangan pseudorandom dengan teknik *chain addition.*

```
0880939030
----------
8689229338
4471412612
8185538730
9930815039
8238965327
```

Ambil baris terakhir, dan bilangan tersebut diurutkan dari 1 hingga 0. Bilangan yang didapatkan digunakan sebagai indeks pada *straddling checkerboard*.

```
8238965327
8139065427
```

Dengan menggunakan huruf berfrekuensi tinggi, ESTONIA, menghasilkan kosong pada huruf ke-3, 6, dan 9. Lalu lengkapi dengan huruf lainnya:

```
B C D F G H J K L M
P Q R U V W X Y Z *
1 2 3 4 5 6 7 8 9 0
```

Maka akan didapatkan *straddling checkerboard* yang lengkap. Awal penulisan ditandai dengan garis bawah.

```
 | 8 1 3 9 0 6 5 4 2 7
 +-------------------
 | E S   T O   N I   A
3| L M B C D F G H J K
6| W X Y Z * P Q R U V
2| 0 1 2 3 4 5 6 7 8 9
```

Selanjutnya plainteks dikonversikan sesuai dengan *straddling checkerboard*:

```
R V * TOM OR R OW * AT* 1 4 0 0 P
M * TO* C OM P L ETE*
646760903106464068607960212028286
631609060390316638898 60

TR ANSAC TION* U SE* D EAD D R OP
* AS* U SU AL
964751739940560621860308730306406
660716062162738
```

Untuk menentukan jumlah kolom yang digunakan dalam kolom pada dua transposisi, ambil dua bilangan terakhir dari 50 bilangan pseudorandom. Jumlahkan, bila masih belum lebih besar dari sembilan maka tambahkan kembali dengan bilangan sebelumnya. Lakukan hingga didapatkan hasil melebihi 9. Bentuk dua bilangan seperti itu untuk kemudian ditentukan sebagai jumlah kolom dalam dua kali transposisi kolom. Akhirnya didapatkan:

```
....815039
8238965327
```

Transposisi pertama dilakukan dengan:

7 + 3 + 2 = 12 kolom

Transposisi kedua dilakukan dengan:

5 + 6 = 11 kolom

Ambil 10 bilangan pertama dari frase kedua dari kunci, dan ditambahkan dengan 10 digit yang diambil dari *straddling checkerboard*. Berikutnya kedua kelompok bilangan tersebut ditambahkan tanpa mengindahkan bawaan yang dihasilkan. Sehingga menhasilkan proses sebagai berikut:

```
 3728109645 kunci
+8139065427 checkerboard
 ----------
 1857164062 hasil
```

Kunci untuk transposisi digunakan dengan melakukan transposisi kepada 50 bilangan pseudorandom. Pembacaan kolom berdasarkan urutan indeks dari hasil penjumlahan yang tadi baru saja dilakukan. Sehingga menghasilkan:

```
 1857164062
 ----------
 8689229338
 4471412612
 8185538730
 9930815039
 8238965327
```

Bilangan hasil transposisi diambil 23 (jumlah 12 kolom dan 11 kolom yang akan digunakan dalam transposisi). Maka didapatkan 23 bilangan sebagai berikut:

```
848982458982 09792855878
```

Transposisi pertama adalah transposisi kolom sederhana. Untuk transposisi pertama ini menggunakan 12 dari 23 digit yang berfungsi sebagai kunci. Blok transposisi diisi dengan bilangan plainteks yang telah dikonversi oleh *straddling checkerboard*. Pada fase ini ditambahkan bilangan *null* untuk melengkapi kelompok bilangan agar dapat dikelompokkan dalam kelompok 5 bilangan.

```
848982458982
------------
646760903106
464068607960
212028286631
609060390316
638898609647
517399405606
218603087303
064066607160
621627380
```

Selanjutnya dibaca berdasarkan urutan kolom yang ditentukan dari indeks setiap kolom. Sehingga menghasilkan hasil sebagai berikut:

```
088089367   60167630   461031162
962364063 008900808 642665206
642987841   662699062   376095770
06314006 700083606 19636631
```

Transposisi kedua menggunakan transposisi kolom dengan 11 bilangan kunci dari 23 bilangan kunci transposisi. Area triangular pertama berawal dari kolom pertama yang akan dibaca paling pertama (memiliki indeks paling kecil), dan dilanjutkan ke baris berikutnya. Pada baris pertama dituliskan sampai satu kolom sebelum indeks 1, lalu berikutnya dituliskan hingga kolom berikutnya, dan terus maju hingga bertemu akhir kolom. Setelah bertemu akhir kolom maka baris berikutnya berulang kembali dari kolom pertama, dan seterusnya.

Lima blok terakhir diisi dengan X agar tidak diisi. Hal ini dikarenakan panjang plainteks adalah 105 sedangkan banyak blok adalah 110 (11 kolom kali 10 baris). Maka didapatkan hasil kolom transposisi sebgai berikut:

```
09792855878
-----------
0880
89367
601676
3046103
11629623
640630089
0080864266
52066429878
416626
990623XXXXX
```

Sisa blok yang kosong diisi dengan plainteks yang tersisa:

```
09792855878
-----------
0880760957 7
8936700631 4
6016760067 0
3046103008 3
1162962360 6
6406300891 9
0080864266 6
5206642987 8
4166263663 1
990623XXXXX
```

Selanjutnya kembali dilakukan pembacaan kolom secara terurut berdasarkan indeks kolom:

```
7771938622  000320423  960038296
8314608060 717801673 6060606463
536069686  740369681  8900140219
0666260666 0863160549
```

Selanjutnya dibentuk hasil enkripsi dalam bentuk lima kelompok bilangan. Hasilnya adalah sebagai berikut:

```
77719  38622  00032  04239  60038
29683
14608  06071  78016  73606  06064
63536
06968  67403  69681  89001  40219
06662
60666 08631 60549
```

Untuk melakukan proses dekripsi:

Untuk melakukan dekripsi pesan, digunakan frase kunci untuk mengkalkulasi digit pada *checkerboard* dan kunci pada dua transposisi. Selanjutnya dilakukan transposisi secara terbalik.

Dibuat blok untuk untuk transposisi kedua. Dengan jumlah kolom dan area triangular yang sesuai. Selanjutnya masukkan pesan enkripsi ke dalam kolom sesuai dengan kunci transposisi. Selanjutnya dibaca baris per baris.

Hasilnya dimasukkan ke dalam blok transposisi pertama dengan kolom yang seusai pula beserta kunci transposisi pertama. Selanjutnya dibaca kembali baris per baris.

Hasil urutan langkah tadi dikonversi ke plainteks dengan menggunakan *straddling checkerboard.*

5. Analisis Penggunaan Teknik Improvisasi dalam Algoritma Klasik

Teknik-teknik improvisasi yang ada sebenarnya hanya melakukan modifikasi pada proses substitusi dan transposisi yang sudah ada. Namun seringkali menggunakan bantuan strutur data bentukan seperti tabel ataupun matriks.

Untuk meningkatkan keefektifan teknik improvisasi substitusi dapat dilakukan dengan melakukan sistem pencarian atau pengindeksan yang dinamis. Tidak hanya berdasarkan indeks pada kolom atau baris.

Sedangkan untuk teknik transposisi dapat digunakan teknik pengacakan urutan berdasarkan kunci ataupun aturan tertentu. Selain itu dapat juga dilakukan proses atau aturan tertentu dalam pengisian kolom transposisi.

Berdasarkan studi yang telah dilakukan mengenai teknik improvisasi, didapatkan beberapa analisis:

1. Penggunaan teknik improvisasi yang paling umum dalam sebuah *cipher* sederhana adalah *straddling checkerboard* dan *columnar transposition*.
2. Pengacakan kunci menjadi bentuk-bentuk yang berbeda merupakan sebuah langkah yang baik dalam pembuatan sebuah alogoritma kriptografi.
3. Pengelompokan pesan menjadi kelompok huruf-huruf yang sama dapat meningkatkan keamanan algoritma. Hal ini dikarenakan jumlah kolom transposisi dapat disembunyikan.
4. Pada umumnya transposisi dan substitusi dapat digunakan secara paralel dalam urutan langkah sebuah algoritma. Namun untuk meningkatkan tingkat kekompleksan lebih baik menggunakan substitusi dahulu, baru kemudia transposisi karena hal tersebut dapat merepotkan proses balikan yang dilakukan oleh kriptanalis.
5. Teknik improvisasi dapat diimplementasikan dalam kriptografi modern dan dapat menghasilkan bilangan yang lebih kompleks karena beroperasi dalam bit atau *byte.*

Teknik-teknik improvisasi dapat digunakan juga dalam perkembangan kriptografi saat ini, yaitu untuk kriptografi modern. Untuk pengimplementasian dalam kriptografi yang ada pada saat ini, penulis menyarankan penggunaan teknik *straddling checkerboard* serta penggenerasian bilangan pseudorandom. Dengan begitu tingkat kompleksitas sebuah algoritma kriptografi dapat menjadi lebih tinggi.

DAFTAR PUSTAKA

[1] http://users.telenet.be/d.rijmenants/
Tanggal akses: 27 September 2006 Pukul 11.00

[2] http://www.quadibloc.com/crypto/
Tanggal akses: 27 September 2006 Pukul 11.00

[3] http://en.wikipedia.org/
Tanggal akses: 27 September 2006 Pukul 11.00

[4] http://www.hypermaths.org/
Tanggal akses: 27 September 2006 Pukul 11.00

[5] http://rijmenants.blogspot.com/
Tanggal akses: 27 September 2006 Pukul 11.00

[6] http://www.criptored.upm.es/
Tanggal akses: 28 September 2006 Pukul 10.00

[7] http://www.mail.informatika.org/~rinaldi