SOLITAIRE CIPHER

Taufik Ramadhany – NIM : 13503112

Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if13112@students.if.itb.ac.id

Abstrak

Makalah ini akan membahas teknik enkripsi, teknik dekripsi, dan contoh implementasi sederhana algoritma Solitaire Cipher. Solitaire Cipher adalah algoritma kriptografi klasik yang menggunakan kartu remi sebagai perantaranya. Jenis algoritma ini menggunakan urutan kartu remi sebagai kunci yang akan diberikan kepada penerima cipherteks secara aman. Sedangkan untuk melakukan proses enkripsi dan dekripsi dari algoritma Solitaire ini urutan kartu diubah dengan urutan dan aturan tertentu. Implementasi dari algoritma ini juga akan disertakan di bagian makalah ini lengkap dengan contohnya.

Selain penggunaan algoritma tersebut, makalah initerlebih dahulu akan membahas hal-hal lain seperti sejarah penciptaan dan informasi terkait dengan algoritma yang bersangkutan. Sejarah algoritma kriptografi ini akan dijelaskan dari latar belakang terciptanya sampai dengan orang yang menciptakan algoritma Solitaire Cipher.

Sebagai penutup makalah, kelebihan algoritma Solitaire Cipher ini akan dijelaskan serta kelemahannya. Kemudian algoritma ini akan dibandingkan dengan algoritma klasik lainnya yang sejenis. Di luar cakupan yang telah disebutkan di atas, makalah ini tidak akan membahas perbandingan algoritma kriptografi ini dengan algoritma lain yang berbeda konsep.

***Kata kunci**: Solitaire Cipher, algoritma kriptografi klasik*

1. Pendahuluan

Secara garis besar algoritma kriptografi terbagi menjadi dua bagian yaitu kriptografi klasik dan kriptografi modern. Algoritma klasik adalah algoritma kriptografi yang umumnya digunakan tanpa membutuhkan alat komputasi tertentu dan sangat sederhana. Algoritma klasik ini biasanya berbasis kepada karakter dan bias dipecahkan hanya dengan bantuan secarik kertas dan sebuah alat tulis. Pada algoritma klasik pemecahan ini lebih berfokus pada kemampuan pikiran sang kriptanalis.

Di sisi lain, algoritma modern sangat membutuhkan komputer untuk melakukan enkripsi ataupun dekripsi dan lebih menitikberatkan pada modifikasi bit dari informasi yang dikirimkan. Hal ini karena algoritma modern lebih berkutat pada operasi matematika rumit yang dilakukan dan tidak mungkin ditangani oleh seorang kriptanalis tanpa bantuan alat komputasi. Pada saat sekarang ini algoritma kriptografi klasik memang sudah sangat jarang digunakan karena mudah untuk dipecahkan, namun algoritma klasik tetap perlu dipelajari sebagai dasar dari algoritma kriptografi modern.

Salah satu algoritma yang termasuk ke dalam algoritma kriptografi klasik adalah Solitaire Cipher. Algoritma Solitaire ini diciptakan oleh Bruce Schneier, seorang pakar keamanan yang juga menciptakan algoritma Blowfish pada tahun 1999. Solitaire Cipher ini termasuk ke dalam algoritma kriptografi berbasis substitusi yaitu algoritma yang mengganti satu atau beberapa karakter dengan karakter lain.

Latar belakang terciptanya algoritma kriptografi Solitaire Cipher ini cukup unik. Bruce Schneier menciptakan algoritma ini untuk digunakan dalam novel Cryptonomicon karangan Neal Stephenson. Dalam novel ini, algoritma ini dikenal dengan nama Pontifix. Dalam novel tersebut, Solitaire Cipher ini digunakan oleh agen rahasia Soviet yang sangat berisiko jika mengirim pesan menggunakan alat bantu lain seperti komputer. Menurut Bruce, algoritma ini sangat mudah digunakan karena hanya membutuhkan satu set kartu dan seperangkat alat tulis.

Sebelum pesan akan disandikan, pengirim dan penerima pesan harus memiliki perjanjian

mengenai beberapa hal dalam proses enkripsi supaya tingkat keamanan dari kriptografi ini lebih kuat. Perjanjian ini mencakup cara pengurutan kartu jika tidak ada kunci serta letak karakter yang digunakan untuk menyembunyikan pola enkripsi.

Tahap pertama untuk mengenkripsi dengan algoritma Solitaire Cipher ini adalah penyusunan kartu awal yang sesuai dengan kunci. Jika tidak ada kunci yang diberikan, perjanjian antara pengirim dan penerima pesan akan berlaku untuk menyusun kartu supaya proses enkripsi pesan bisa dilanjutkan.

Tahap kedua adalah proses pembangkitan huruf aliran kunci(*keystream letters*). Ada 6 langkah yang harus dilakukan, yang kemudian menghasilkan sebuah huruf pada akhir tahap ini. Tahap kedua ini dapat diulangi sesuai dengan panjang aliran kunci yang diinginkan. Misalnya jika ingin mendapatkan aliran kunci sepanjang 10 karakter, maka tahap kedua ini dilakukan 10 kali.

Tahap kedua dan ketiga adalah inti dari algoritma Solitaire Cipher ini. Dengan acaknya urutan kartu, maka kriptanalis tidak mempunyai informasi yang cukup untuk memecahkan cipher. Proses enkripsi ini diakhiri secara sederhana ketika beberapa karakter yang totalnya sama dengan panjang aliran kunci ditambahkan dengan aliran kunci. Pada tahap ketiga ini, pesan biasanya dibagi ke kelompok 5 huruf. Jika ada huruf yang kosong, maka diisi dengan huruf X.

Algoritma Solitaire Cipher ini memiliki tingkat keamanan yang tinggi. Dengan *keystream* yang mempunyai panjang yang sama dengan plainteks, maka algoritma ini bisa dikatakan hampir menyerupai One Time Pads yang tidak bisa dipecahkan. Sebaliknya apabila keystream yang digunakan pendek, maka algoritma ini mudah dipecahkan dengan metode Kasiski seperti Algoritma Vigenere.

2. Implementasi Algoritma Solitaire

Sebelum proses enkripsi dan dekripsi dilakukan, ada beberapa hal yang harus dijelaskan terlebih dahulu.

Pada satu set kartu remi, ada dua buah joker yang tersedia. Karena itu, harus ada pembedaan. Pembedaan ini dapat dilakukan berdasarkan warna joker atau ukuran gambar. Sehingga selanjutnya joker berwarna akan disebut joker A(atau A saja), sedangkan joker lain akan disebut sebagai joker B(atau B saja).

2.1 Teknik Enkripsi

2.1.1 Pengurutan Awal Kartu

Sesuai dengan penjelasan pada bagian pendahuluan, langkah pertama yang harus dilakukan ketika ingin mengenkripsi adalah dengan mengatur urutan kartu. Pengurutan awal kartu ini bergantung kepada ada atau tidaknya kunci yang digunakan.

Jika tidak ingin menggunakan kunci, maka urutan awal kartu ini ditentukan oleh perjanjian antara pengirim pesan dengan penerima. Urutan awal kartu ini dapat berupa urutan dari nilai terkecil ke nilai terbesar, dengan anggapan bahwa kartu As sampai dengan kartu King keriting(*clubs*) untuk nilai satu sampai tiga belas, nilai empat belas sampai dua puluh enam untuk wajik(*diamonds*), nilai dua puluh tujuh sampai tiga puluh sembilan untuk hati(*hearts*) dan sisanya untuk kartu yang jenisnya pohon(*spades*). Jika digambarkan akan terlihat seperti ini

```
1 2 3 4 5 6 7 8 9 10 ...49
50 51 52 A B
```

Urutan awal juga dapat dikombinasikan dengan deret aritmatika seperti contoh di bawah ini

```
1 4 7 10 13..49 52 2
5...45 48 51 54
```

Untuk proses enkripsi yang menggunakan kunci, cara pengurutan kartu ini menjadi lebih rumit. Kunci biasanya diberikan dalam bentuk kata/kalimat yang memiliki arti. Contohnya jika kunci enkripsi adalah *SOLITAIRE*, maka urutan kartu diatur dengan mempertimbangkan masing-masing karakter dari kunci enkripsi yang diberikan. Proses untuk membangkitkan urutan kartu dengan kunci:

1. Ambil sebuah karakter dari kata kunci. Konversikan karakter tersebut menjadi sebuah bilangan sesuai dengan urutannya. Jadi untuk karakter K, nilai karakter tersebut adalah 11 atau nilai 20 untuk karakter T. Untuk selanjutnya nilai karakter ini disebut dengan variabel `cut_size`.
2. Lakukan enam langkah untuk mendapatkan huruf aliran kunci(*keystream letter*) yang akan dijelaskan pada bagian selanjutnya. Berbeda dengan langkah yang dilakukan ketika enkripsi, untuk proses yang dilakukan pada bagian ini nilai keluaran tidak penting. Hal ini karena langkah tersebut dilakukan hanya untuk mengacak posisi kartu.
3. Lakukan *triple cut*. *Triple cut* lebih lanjut akan dijelaskan pada bagian berikutnya. Pada tahap ini, posisi joker tidak berpengaruh. Parameter posisi untuk *triple cut* kali ini adalah 1 dan 54-`cut_size`.

Jadi kartu yang berada di sebelah kiri dari kartu pertama ditukarkan dengan kartu yang berada di sebelah kanan kartu yang posisinya 54-`cut_size`. Dengan kata lain, sejumlah `cut_size` kartu terakhir dipindahkan ke bagian awal urutan kartu.

4. Lakukan pemindahan kartu berikutnya, dengan mengganti posisi 52 kartu pertama dengan kartu terakhir. Kartu ke-53 tetap pada posisinya.

Langkah-langkah di atas diulangi sebanyak jumlah karakter yang ada pada kunci.

2.1.2 Pembangkitan Huruf Aliran Kunci (Keystream Letters)

Proses pembangkitan huruf aliran kunci ini dibagi lagi menjadi 6 langkah. Tahap ini akan menghasilkan sebuah huruf yang kemudian sebagai kunci kedua. Langkah-langkah yang harus dilakukan sebagai berikut:

1. Cari joker A. Lalu pindahkan kartu joker A ini satu langkah ke belakang. Dalam kata lain, ganti kartu joker A dengan kartu di bawahnya. Jika joker A merupakan kartu terbawah, pindahkan ke posisi kedua(di bawah kartu paling atas). Contohnya jika urutan awal seperti di bawah ini

   `A 7 2 B 9 4 1,`

   maka urutan selanjutnya adalah

   `7 A 2 B 9 4 1.`
2. Cari joker B. Lalu pindahkan kartu joker B ini dua langkah ke belakang. Dalam kata lain, ganti kartu joker B dengan kartu kedua di bawahnya. Jika joker B merupakan kartu terbawah, pindahkan ke posisi ketiga. Jika joker B merupakan kartu kedua dari bawah, maka pindahkan kartu joker B tersebut kedua. Contohnya jika urutan sebelumnya

   `3 A B 8 9 6,`

   maka setelah langkah kedua posisi kartu seharusnya adalah

   `3 A 8 9 B 6.`
3. Lakukan *triple cut*. Yaitu ganti kartu-kartu yang berada di bagian kiri kartu joker pertama dengan kartu-kartu di bagian kanan dari kartu joker kedua. Perlu diperhatikan bahwa joker pertama adalah joker yang berada di posisi lebih tinggi dari kartu joker lain, tidak penting apakah itu joker A atau B. Perlu diperhatikan juga bahwa posisi kartu-kartu yang berada di antara kedua joker tidak berubah. Jika salah satu atau kedua joker berada di posisi ujung, proses *triple cut* tetap dilakukan. Contoh kasus ketika posisi awal

   `2 4 6 B 5 8 7 1 A 3 9,`

   maka setelah triple cut posisi akhir adalah

   `3 9 B 5 8 7 A 2 4 6.`

   Jika posisi awal

   `B 5 8 7 1 A 3 9,`

   maka posisi akhir adalah

   `3 9 B 5 8 7 A.`

   Jika posisi awal

   `B 8 5 7 1 A,`

   maka posisi tidak berubah.
4. Lakukan *count cut*. Lihat kartu terbawah dan konversikan kartunya menjadi sebuah bilangan(misal : n). Pengonversian nilai kartu ini dicontohkan pada bagian pengurutan awal kartu, dengan kedua joker bernilai 53. Ambil n kartu pertama dan pindahkan ke posisi kedua dari bawah. Jika kondisi awal kartu adalah

   `7 28 9 4 44...53 3.`

   Dapat diketahui bahwa nilai kartu terbawah adalah 3. Setelah 3 kartu teratas dipindahkan ke posisi kedua dari bawah, maka posisi kartu akan menjadi

   `4 44...53 7 28 9 3.`
5. Temukan kartu keluaran(*output card*) dengan melihat kartu teratas dan konversikan menjadi bilangan(seperti di langkah 4). Maka kartu keluaran adalah kartu ke `n+1`, dengan kartu teratas dihitung sebagai 1. Catat kartu ini, tapi jangan mengubah susunan kartu yang ada. Proses diabaikan dan diulangi dari langkah 1 jika kartu keluaran yang ditemukan adalah joker.
6. Dari kartu keluaran yang dihasilkan langkah 5, konversikan menjadi bilangan. Bilangan ini adalah bilangan keluaran(*output number*). Ada aturan mengenai konversi nilai ini. Untuk jenis keriting dan wajik, nilai kartu As sampai kartu King adalah 1 sampai 13. Sedangkan untuk dua jenis lain nilainya berkisar dari 14 sampai 26. Hal ini dilakukan supaya setiap bilangan bisa merepresentasikan sebuah huruf yang bersesuaian.

Setelah 6 langkah tersebut berhasil dilakukan, proses ini dapat diulangi sesuai dengan jumlah kunci aliran yang diinginkan.

Ada berbagai versi dalam penentuan panjang keystream. Bruce Schneier sendiri lebih condong untuk menggunakan *keystream* sepanjang 10 karakter. Di sisi lain ada orang yang menggunakan *keystream* sepanjang *plainteks*. Pada makalah ini, penulis memilih menggunakan *keystream* sepanjang 10 karakter.

Pada tahap pembangkitan keystream ini, tingkat keamanan algoritma bisa ditingkatkan dengan memasukkan nilai kartu joker sebagai keystream. Hal ini terjadi apabila pada akhir proses kelima di atas kartu keluaran yang didapatkan adalah kartu joker.

2.1.3 Penjumlahan Pesan dengan Kunci Aliran

Pada proses ini, kunci aliran dijumlahkan dengan pesan yang akan dikirimkan. Jika pesan yang akan dikirimkan adalah

```
WELCOME
```

dan kunci aliran adalah

```
4 23 10 24 8 25 18 6 4 9,
```

maka pesan diatur terlebih dahulu sehingga menjadi

```
WELCO MEXXX
```

Proses penjumlahan akan berjalan seperti berikut(menggunakan modulo 26)

```
W + 4  = A
E + 23 = B
L + 10 = V
```

dan seterusnya. Maka cipherteks yang dihasilkan adalah

```
ABVAW JWDBE.
```

2.2 Teknik Dekripsi

Untuk mendekripsi sebuah pesan yang telah dienkripsi dengan Solitaire Cipher, proses-proses yang ditempuh hampir sama dengan proses untuk enkripsi. Yang harus dilakukan untuk proses dekripsi adalah menemukan kunci aliran berdasarkan kunci posisi kartu yang diberikan. Setelah kunci aliran didapatkan, pesan kemudian dikurangi dengan kunci aliran. Lengkapnya akan dijelaskan sebagai berikut

2.2.1 Pengurutan Awal Kartu

Sama dengan langkah yang harus dilakukan untuk enkripsi sebuah pesan, langkah pertama yang harus dilakukan ketika ingin mendekripsi adalah dengan mengatur urutan kartu. Pengurutan awal kartu ini bergantung kepada ada atau tidaknya kunci yang diberikan.

Jika kunci tidak ada, seperti enkripsi maka urutan awal kartu ini ditentukan oleh perjanjian antara pengirim pesan dengan penerima. Urutan awal kartu ini juga sama dengan sebelumnya, yaitu dapat berupa urutan dari nilai terkecil ke nilai terbesar, dengan anggapan bahwa kartu As sampai dengan kartu King keriting(*clubs*) untuk nilai satu sampai tiga belas, nilai empat belas sampai dua puluh enam untuk wajik(*diamonds*), nilai dua puluh tujuh sampai tiga puluh sembilan untuk hati(*hearts*) dan sisanya untuk kartu yang jenisnya pohon(*spades*).

2.2.2 Pembangkitan Huruf Aliran Kunci (Keystream Letters)

Enam langkah yang harus dilakukan pada proses enkripsi juga dilakukan ketika dekripsi sebuah pesan. Singkatnya enam langkah tersebut dapat dijelaskan di bawah ini:

1. Cari joker A. Lalu pindahkan kartu joker A ini satu langkah ke belakang. Dalam kata lain, ganti kartu joker A dengan kartu di bawahnya. Jika joker A merupakan kartu terbawah, pindahkan ke posisi kedua(di bawah kartu paling atas).
2. Cari joker B. Lalu pindahkan kartu joker B ini dua langkah ke belakang. Dalam kata lain, ganti kartu joker B dengan kartu kedua di bawahnya. Jika joker B merupakan kartu terbawah, pindahkan ke posisi ketiga. Jika joker B merupakan kartu kedua dari bawah, maka pindahkan kartu joker B tersebut kedua.
3. Lakukan *triple cut*. Yaitu ganti kartu-kartu yang berada di bagian kiri kartu joker pertama dengan kartu-kartu di bagian kanan dari kartu joker kedua. Perlu diperhatikan bahwa joker pertama adalah joker yang berada di posisi lebih tinggi dari kartu joker lain, tidak penting apakah itu joker A atau B. Perlu diperhatikan juga bahwa posisi kartu-kartu yang berada di antara kedua joker tidak berubah. Jika salah satu atau kedua joker berada di posisi ujung, proses *triple cut* tetap dilakukan.
4. Lakukan *count cut*. Lihat kartu terbawah dan konversikan kartunya menjadi sebuah bilangan(misal : n). Pengonversian nilai kartu ini dicontohkan pada bagian pengurutan awal kartu, dengan kedua joker bernilai 53. Ambil n kartu pertama dan pindahkan ke posisi kedua dari bawah.
5. Temukan kartu keluaran(*output card*) dengan melihat kartu teratas dan konversikan menjadi bilangan(seperti di langkah 4). Maka kartu keluaran adalah kartu ke n+1, dengan n kartu teratas adalah 1. Catat kartu ini, tapi jangan mengubah susunan kartu yang ada. Proses diabaikan dan diulangi dari langkah 1 jika kartu keluaran yang ditemukan adalah joker.
6. Dari kartu keluaran yang dihasilkan langkah 5, konversikan menjadi bilangan. Bilangan ini adalah bilangan keluaran(*output number*). Aturan konversi nilai sama dengan enkripsi. Nilai keluaran ini berkisar 1-26,

sehingga untuk nilai kartu di atas 26 nilai keluarannya adalah nilai kartu-26.

Setelah 6 langkah tersebut berhasil dilakukan, proses ini dapat diulangi sesuai dengan jumlah kunci aliran yang diinginkan.

2.2.3 Pengurangan Cipherteks dengan Keystream

Pada tahap ini, setiap karakter cipherteks dikurangi dengan *keystream* yang ada. Hasilnya adalah karakter plainteks. Jika jumlah karakter plainteks tidak habis dibagi dengan jumlah karakter pada *keystream*, maka pada karakter sisa akan didapatkan karakter X.

2.3 Contoh Implementasi

Untuk contoh implementasi ini, pesan dan kunci yang akan digunakan harus ditentukan terlebih dahulu.

Pesan :

```
SOLITAIRE
```

Kunci yang digunakan :

```
PONTIFIX
```

2.3.1 Pengurutan kartu awal

Sesuai dengan langkah-langkah enkripsi yang diberikan pada bagian sebelumnya, maka hal pertama yang harus dilakukan adalah mengurutkan kartu sesuai dengan kunci yang diberikan.

Kunci :

```
PONTIFIX
```

Untuk pengurutan kartu awal ini, langkah yang harus dilakukan adalah

1. Ambil sebuah karakter dari kata kunci. Untuk contoh implementasi pertama(huruf P) maka

   ```
   cut_size = 16
   ```

2. Lakukan enam langkah untuk mendapatkan huruf aliran kunci yang telah dijelaskan. Dari contoh sebelumnya, maka pengurutan kartu dimulai. Urutan kartu awal dari nilai terkecil ke nilai terbesar. Perlu diingat kembali bahwa nilai 1-13 diberikan untuk kartu As – kartu King keriting(*clubs*) secara berurutan. Nilai 14-26 untuk kartu berjenis wajik(*diamonds*), nilai 27-39 untuk kartu hati(*hearts*) dan nilai 40-52 untuk kartu pohon(*spades*).

   ```
    1  2  3  4  5  6  7  8  9
   10 11 12 13 14 15 16 17 18
   19 20 21 22 23 24 25 26 27
   28 29 30 31 32 33 34 35 36
   37 38 39 40 41 42 43 44 45
   46 47 48 49 50 51 52  A  B
   ```

   Langkah pertama adalah pemindahan joker A. Maka susunan kartu akan menjadi

   ```
    1  2  3  4  5  6  7  8  9
   10 11 12 13 14 15 16 17 18
   19 20 21 22 23 24 25 26 27
   28 29 30 31 32 33 34 35 36
   37 38 39 40 41 42 43 44 45
   46 47 48 49 50 51 52  B  A
   ```

   Langkah kedua adalah pemindahan joker B. Susunan kartu akan berubah menjadi

   ```
    1  B  2  3  4  5  6  7  8
    9 10 11 12 13 14 15 16 17
   18 19 20 21 22 23 24 25 26
   27 28 29 30 31 32 33 34 35
   36 37 38 39 40 41 42 43 44
   45 46 47 48 49 50 51 52  A
   ```

   Langkah selanjutnya adalah *triple cut* yang akan menjadikan susunan kartu seperti berikut

   ```
    B  2  3  4  5  6  7  8  9
   10 11 12 13 14 15 16 17 18
   19 20 21 22 23 24 25 26 27
   28 29 30 31 32 33 34 35 36
   37 38 39 40 41 42 43 44 45
   46 47 48 49 50 51 52  A  1
   ```

   Langkah keempat adalah *count cut* yang akan memindahkan 1 kartu pertama. Posisi kartu selanjutnya

   ```
    2  3  4  5  6  7  8  9 10
   11 12 13 14 15 16 17 18 19
   20 21 22 23 24 25 26 27 28
   29 30 31 32 33 34 35 36 37
   38 39 40 41 42 43 44 45 46
   47 48 49 50 51 52  A  B  1
   ```

   Setelah *count cut* ini, proses pembangkitan aliran kunci untuk penyusunan kartu sesuai kunci telah selesai.

3. Lakukan *triple cut*. Sejumlah cut_size kartu awal diganti dengan kartu terakhir. Dari hasil di nomor dua, maka posisi urutan kartu berikutnya didapatkan dengan mengganti 16 kartu pertama dengan kartu terakhir.

   ```
    1 18 19 20 21 22 23 24 25
   26 27 28 29 30 31 32 33 34
   35 36 37 38 39 40 41 42 43
   44 45 46 47 48 49 50 51 52
    A  B  2  3  4  5  6  7  8
    9 10 11 12 13 14 15 16 17
   ```

4. Lakukan pemindahan kartu berikutnya, dengan meletakkan kartu pertama sebagai

kartu paling bawah. Posisi kartu lain tidak diubah

```
18 19 20 21 22 23 24 25 26
27 28 29 30 31 32 33 34 35
36 37 38 39 40 41 42 43 44
45 46 47 48 49 50 51 52  A
 B  2  3  4  5  6  7  8  9
10 11 12 13 14 15 16 17  1
```

Dengan demikian proses untuk mendapatkan susunan kartu menurut karakter pertama dari kunci telah dilakukan. Langkah-langkah di atas diulangi untuk semua karakter lain dari kata kunci. Selanjutnya akan dicontohkan pengaturan kunci untuk karakter kedua, yaitu O. Susunan kartu awal untuk karakter O ini diambil dari susunan yang dihasilkan untuk pengaturan kartu berdasarkan karakter P. Maka susunan awal pengaturan kunci untuk karakter O ini adalah

```
18 19 20 21 22 23 24 25 26
27 28 29 30 31 32 33 34 35
36 37 38 39 40 41 42 43 44
45 46 47 48 49 50 51 52  A
 B  2  3  4  5  6  7  8  9
10 11 12 13 14 15 16 17  1
```

Langkah-langkahnya adalah:

1. Penentuan cut_size

   ```
   cut_size = 15
   ```

2. Enam langkah mendapatkan aliran kunci.

   Hasil dari penggeseran joker A:

   ```
   18 19 20 21 22 23 24 25 26
   27 28 29 30 31 32 33 34 35
   36 37 38 39 40 41 42 43 44
   45 46 47 48 49 50 51 52  B
    A  2  3  4  5  6  7  8  9
   10 11 12 13 14 15 16 17  1
   ```

   Hasil dari penggeseran joker B:

   ```
   18 19 20 21 22 23 24 25 26
   27 28 29 30 31 32 33 34 35
   36 37 38 39 40 41 42 43 44
   45 46 47 48 49 50 51 52  A
    2  B  3  4  5  6  7  8  9
   10 11 12 13 14 15 16 17  1
   ```

   Hasil dari *triple cut*:

   ```
    3  4  5  6  7  8  9 10 11
   12 13 14 15 16 17  1  A  2
    B 18 19 20 21 22 23 24 25
   26 27 28 29 30 31 32 33 34
   35 36 37 38 39 40 41 42 43
   44 45 46 47 48 49 50 51 52
   ```

   Hasil dari *count cut*:

   ```
   51  3  4  5  6  7  8  9 10
   11 12 13 14 15 16 17  1  A
    2  B 18 19 20 21 22 23 24
   25 26 27 28 29 30 31 32 33
   34 35 36 37 38 39 40 41 42
   43 44 45 46 47 48 49 50 52
   ```

3. *Triple cut*

   Hasil dari triple cut:

   ```
   52 17  1  A  2  B 18 19 20
   21 22 23 24 25 26 27 28 29
   30 31 32 33 34 35 36 37 38
   39 40 41 42 43 44 45 46 47
   48 49 50 51  3  4  5  6  7
    8  9 10 11 12 13 14 15 16
   ```

4. Pemindahan kartu pertama

   Hasilnya:

   ```
   17  1  A  2  B 18 19 20 21
   22 23 24 25 26 27 28 29 30
   31 32 33 34 35 36 37 38 39
   40 41 42 43 44 45 46 47 48
   49 50 51  3  4  5  6  7  8
    9 10 11 12 13 14 15 16 52
   ```

Penyusunan kartu untuk karakter ketiga(N):

Susunan kartu awal:

```
17  1  A  2  B 18 19 20 21
22 23 24 25 26 27 28 29 30
31 32 33 34 35 36 37 38 39
40 41 42 43 44 45 46 47 48
49 50 51  3  4  5  6  7  8
 9 10 11 12 13 14 15 16 52
```

Langkah yang dilakukan:

1. Penentuan cut_size

   ```
   cut_size = 14
   ```

2. Enam langkah mendapatkan aliran kunci.

   Hasil dari penggeseran joker A:

   ```
   17  1  2  A  B 18 19 20 21
   22 23 24 25 26 27 28 29 30
   31 32 33 34 35 36 37 38 39
   40 41 42 43 44 45 46 47 48
   49 50 51  3  4  5  6  7  8
    9 10 11 12 13 14 15 16 52
   ```

   Hasil dari penggeseran joker B:

   ```
   17  1  2  A 18 19  B 20 21
   22 23 24 25 26 27 28 29 30
   31 32 33 34 35 36 37 38 39
   40 41 42 43 44 45 46 47 48
   49 50 51  3  4  5  6  7  8
    9 10 11 12 13 14 15 16 52
   ```

Hasil dari *triple cut*:

```
20 21 22 23 24 25 26 27 28
29 30 31 32 33 34 35 36 37
38 39 40 41 42 43 44 45 46
47 48 49 50 51  3  4  5  6
 7  8  9 10 11 12 13 14 15
16 52  A 18 19  B 17  1  2
```

Hasil dari *count cut*:

```
22 23 24 25 26 27 28 29 30
31 32 33 34 35 36 37 38 39
40 41 42 43 44 45 46 47 48
49 50 51  3  4  5  6  7  8
 9 10 11 12 13 14 15 16 52
 A 18 19  B 17  1 20 21  2
```

3. *Triple cut*

Hasil dari triple cut:

```
 2 36 37 38 39 40 41 42 43
44 45 46 47 48 49 50 51  3
 4  5  6  7  8  9 10 11 12
13 14 15 16 52  A 18 19  B
17  1 20 21 22 23 24 25 26
27 28 29 30 31 32 33 34 35
```

4. Pemindahan kartu pertama, hasilnya:

```
36 37 38 39 40 41 42 43 44
45 46 47 48 49 50 51  3  4
 5  6  7  8  9 10 11 12 13
14 15 16 52  A 18 19  B 17
 1 20 21 22 23 24 25 26 27
28 29 30 31 32 33 34 35  2
```

Penyusunan berikutnya adalah penyusunan berdasarkan karater keempat, yaitu karakter T.
Susunan kartu awal untuk karakter T:

```
36 37 38 39 40 41 42 43 44
45 46 47 48 49 50 51  3  4
 5  6  7  8  9 10 11 12 13
14 15 16 52  A 18 19  B 17
 1 20 21 22 23 24 25 26 27
28 29 30 31 32 33 34 35  2
```

Langkah untuk menyusun kartu:

1. Penentuan cut_size

```
cut_size = 14
```

2. Enam langkah mendapatkan aliran kunci.

Hasil dari penggeseran joker A:

```
36 37 38 39 40 41 42 43 44
45 46 47 48 49 50 51  3  4
 5  6  7  8  9 10 11 12 13
14 15 16 52 18  A 19  B 17
 1 20 21 22 23 24 25 26 27
28 29 30 31 32 33 34 35  2
```

Hasil dari penggeseran joker B:

```
36 37 38 39 40 41 42 43 44
45 46 47 48 49 50 51  3  4
 5  6  7  8  9 10 11 12 13
14 15 16 52 18  A 19 17  1
 B 20 21 22 23 24 25 26 27
28 29 30 31 32 33 34 35  2
```

Hasil dari *triple cut*:

```
20 21 22 23 24 25 26 27 28
29 30 31 32 33 34 35  2  A
19 17  1  B 36 37 38 39 40
41 42 43 44 45 46 47 48 49
50 51  3  4  5  6  7  8  9
10 11 12 13 14 15 16 52 18
```

Hasil dari *count cut*:

```
19 17  1  B 36 37 38 39 40
41 42 43 44 45 46 47 48 49
50 51  3  4  5  6  7  8  9
10 11 12 13 14 15 16 52 20
21 22 23 24 25 26 27 28 29
30 31 32 33 34 35  2  A 18
```

3. *Triple cut*:

```
18  3  4  5  6  7  8  9 10
11 12 13 14 15 16 52 20 21
22 23 24 25 26 27 28 29 30
31 32 33 34 35  2  A 19 17
 1  B 36 37 38 39 40 41 42
43 44 45 46 47 48 49 50 51
```

4. Pemindahan kartu pertama

Hasilnya:

```
 3  4  5  6  7  8  9 10 11
12 13 14 15 16 52 20 21 22
23 24 25 26 27 28 29 30 31
32 33 34 35  2  A 19 17  1
 B 36 37 38 39 40 41 42 43
44 45 46 47 48 49 50 51 18
```

Penyusunan kartu untuk karakter kelima(I) dimulai dengan susunan kartu:

```
3  4  5  6  7  8  9 10 11
12 13 14 15 16 52 20 21 22
23 24 25 26 27 28 29 30 31
32 33 34 35  2  A 19 17  1
 B 36 37 38 39 40 41 42 43
44 45 46 47 48 49 50 51 18
```

Langkah untuk menyusun kartu:

1. Penentuan cut_size

```
cut_size = 9
```

2. Enam langkah mendapatkan aliran kunci.

Hasil dari penggeseran joker A:

```
 3  4  5  6  7  8  9 10 11
12 13 14 15 16 52 20 21 22
23 24 25 26 27 28 29 30 31
32 33 34 35  2 19  A 17  1
 B 36 37 38 39 40 41 42 43
44 45 46 47 48 49 50 51 18
```

Hasil dari penggeseran joker B:

```
 3  4  5  6  7  8  9 10 11
12 13 14 15 16 52 20 21 22
23 24 25 26 27 28 29 30 31
32 33 34 35  2 19  A 17  1
36 37  B 38 39 40 41 42 43
44 45 46 47 48 49 50 51 18
```

Hasil dari *triple cut*:

```
38 39 40 41 42 43 44 45 46
47 48 49 50 51 18  A 17  1
36 37  B  3  4  5  6  7  8
 9 10 11 12 13 14 15 16 52
20 21 22 23 24 25 26 27 28
29 30 31 32 33 34 35  2 19
```

Hasil dari *count cut*:

```
37  B  3  4  5  6  7  8  9
10 11 12 13 14 15 16 52 20
21 22 23 24 25 26 27 28 29
30 31 32 33 34 35  2 38 39
40 41 42 43 44 45 46 47 48
49 50 51 18  A 17  1 36 19
```

3. Triple cut

Hasil dari triple cut susunan kartu:

```
19 10 11 12 13 14 15 16 52
20 21 22 23 24 25 26 27 28
29 30 31 32 33 34 35  2 38
39 40 41 42 43 44 45 46 47
48 49 50 51 18  A 17  1 36
37  B  3  4  5  6  7  8  9
```

4. Pemindahan kartu pertama, hasilnya:

```
10 11 12 13 14 15 16 52 20
21 22 23 24 25 26 27 28 29
30 31 32 33 34 35  2 38 39
40 41 42 43 44 45 46 47 48
49 50 51 18  A 17  1 36 37
 B  3  4  5  6  7  8  9 19
```

Selanjutnya adalah penyusunan kartu berdasarkan karakter F. Susunan awal kartunya:

```
10 11 12 13 14 15 16 52 20
21 22 23 24 25 26 27 28 29
30 31 32 33 34 35  2 38 39
40 41 42 43 44 45 46 47 48
49 50 51 18  A 17  1 36 37
 B  3  4  5  6  7  8  9 19
```

1. Penentuan cut_size

```
cut_size = 6
```

2. Penggeseran joker A. Hasilnya:

```
10 11 12 13 14 15 16 52 20
21 22 23 24 25 26 27 28 29
30 31 32 33 34 35  2 38 39
40 41 42 43 44 45 46 47 48
49 50 51 18 17  A  1 36 37
 B  3  4  5  6  7  8  9 19
```

Penggeseran joker B.Hasilnya:

```
10 11 12 13 14 15 16 52 20
21 22 23 24 25 26 27 28 29
30 31 32 33 34 35  2 38 39
40 41 42 43 44 45 46 47 48
49 50 51 18 17  A  1 36 37
 3  4  B  5  6  7  8  9 19
```

Triple cut:

```
 5  6  7  8  9 19  A  1 36
37  3  4  B 10 11 12 13 14
15 16 52 20 21 22 23 24 25
26 27 28 29 30 31 32 33 34
35  2 38 39 40 41 42 43 44
45 46 47 48 49 50 51 18 17
```

Count cut:

```
14 15 16 52 20 21 22 23 24
25 26 27 28 29 30 31 32 33
34 35  2 38 39 40 41 42 43
44 45 46 47 48 49 50 51 18
 5  6  7  8  9 19  A  1 36
37  3  4  B 10 11 12 13 17
```

3. Triple cut

```
17 22 23 24 25 26 27 28 29
30 31 32 33 34 35  2 38 39
40 41 42 43 44 45 46 47 48
49 50 51 18  5  6  7  8  9
19  A  1 36 37  3  4  B 10
11 12 13 14 15 16 52 20 21
```

4. Hasil dari pemindahan kartu pertama

```
22 23 24 25 26 27 28 29 30
31 32 33 34 35  2 38 39 40
41 42 43 44 45 46 47 48 49
50 51 18  5  6  7  8  9 19
 A  1 36 37  3  4  B 10 11
12 13 14 15 16 52 20 21 17
```

Penyusunan berikutnya dimulai dengan susunan:

```
22 23 24 25 26 27 28 29 30
31 32 33 34 35  2 38 39 40
41 42 43 44 45 46 47 48 49
50 51 18  5  6  7  8  9 19
 A  1 36 37  3  4  B 10 11
12 13 14 15 16 52 20 21 17
```

1. Penentuan cut_size
   ```
   cut_size = 9
   ```
2. Hasil dari penggeseran joker A:
   ```
   22 23 24 25 26 27 28 29 30
   31 32 33 34 35  2 38 39 40
   41 42 43 44 45 46 47 48 49
   50 51 18  5  6  7  8  9 19
    1  A 36 37  3  4  B 10 11
   12 13 14 15 16 52 20 21 17
   ```

   Penggeseran joker B:
   ```
   22 23 24 25 26 27 28 29 30
   31 32 33 34 35  2 38 39 40
   41 42 43 44 45 46 47 48 49
   50 51 18  5  6  7  8  9 19
    1  A 36 37  3  4 10 11  B
   12 13 14 15 16 52 20 21 17
   ```

   Triple cut:
   ```
   12 13 14 15 16 52 20 21 17
    A 36 37  3  4 10 11  B 22
   23 24 25 26 27 28 29 30 31
   32 33 34 35  2 38 39 40 41
   42 43 44 45 46 47 48 49 50
   51 18  5  6  7  8  9 19  1
   ```

   Count cut:
   ```
   13 14 15 16 52 20 21 17  A
   36 37  3  4 10 11  B 22 23
   24 25 26 27 28 29 30 31 32
   33 34 35  2 38 39 40 41 42
   43 44 45 46 47 48 49 50 51
   18  5  6  7  8  9 19 12  1
   ```

3. Triple cut
   ```
    1 36 37  3  4 10 11  B 22
   23 24 25 26 27 28 29 30 31
   32 33 34 35  2 38 39 40 41
   42 43 44 45 46 47 48 49 50
   51 18  5  6  7  8  9 19 12
   13 14 15 16 52 20 21 17  A
   ```

4. Pemindahan kartu pertama
   ```
   36 37  3  4 10 11  B 22 23
   24 25 26 27 28 29 30 31 32
   33 34 35  2 38 39 40 41 42
   43 44 45 46 47 48 49 50 51
   18  5  6  7  8  9 19 12 13
   14 15 16 52 20 21 17  A  1
   ```

Selanjutnya adalah proses penyusunan kartu terakhir dengan karakter X. Susunan kartu awalnya sama dengan susunan terakhir yang dihasilkan oleh penyusunan kartu dengan karakter I, yaitu:

```
36 37  3  4 10 11  B 22 23
24 25 26 27 28 29 30 31 32
33 34 35  2 38 39 40 41 42
43 44 45 46 47 48 49 50 51
18  5  6  7  8  9 19 12 13
14 15 16 52 20 21 17  A  1
```

Langkah-langkah penyusunan kartu:

1. Penentuan nilai cut_size
   ```
   cut_size = 24
   ```
2. Empat langkah pembangkitan aliran kunci.
   Pertama, penggeseran joker A:
   ```
   36 37  3  4 10 11  B 22 23
   24 25 26 27 28 29 30 31 32
   33 34 35  2 38 39 40 41 42
   43 44 45 46 47 48 49 50 51
   18  5  6  7  8  9 19 12 13
   14 15 16 52 20 21 17  1  A
   ```

   Kedua, penggeseran joker B:
   ```
   36 37  3  4 10 11 22 23  B
   24 25 26 27 28 29 30 31 32
   33 34 35  2 38 39 40 41 42
   43 44 45 46 47 48 49 50 51
   18  5  6  7  8  9 19 12 13
   14 15 16 52 20 21 17  1  A
   ```

   Ketiga, triple cut:
   ```
    B 24 25 26 27 28 29 30 31
   32 33 34 35  2 38 39 40 41
   42 43 44 45 46 47 48 49 50
   51 18  5  6  7  8  9 19 12
   13 14 15 16 52 20 21 17  1
    A 36 37  3  4 10 11 22 23
   ```
   Keempat, *count cut*:
   ```
   47 48 49 50 51 18  5  6  7
    8  9 19 12 13 14 15 16 52
   20 21 17  1  A 36 37  3  4
   10 11 22  B 24 25 26 27 28
   29 30 31 32 33 34 35  2 38
   39 40 41 42 43 44 45 46 23
   ```

3. Triple cut
   ```
   23 37  3  4 10 11 22  B 24
   25 26 27 28 29 30 31 32 33
   34 35  2 38 39 40 41 42 43
   44 45 46 47 48 49 50 51 18
    5  6  7  8  9 19 12 13 14
   15 16 52 20 21 17  1  A 36
   ```

4. Pemindahan kartu pertama
   ```
   37  3  4 10 11 22  B 24 25
   26 27 28 29 30 31 32 33 34
   35  2 38 39 40 41 42 43 44
   45 46 47 48 49 50 51 18  5
    6  7  8  9 19 12 13 14 15
   16 52 20 21 17  1  A 36 23
   ```

Dengan demikian proses pengurutan kartu awal telah selesai. Susunan kartu yang terakhir dihasilkan sudah bisa digunakan untuk melakukan enkripsi pesan.

2.3.2 Pembangkitan aliran kunci(keystreans)

Setelah posisi urutan kartu didapatkan, baru kemudian proses inti dari enkripsi dilakukan.

Perbedaan antara proses pembangkitan aliran kunci pada tahap ini dengan tahap penyusunan kartu awal terletak pada keluarannya. Pada tahap penyusunan kartu awal, nilai dan kartu keluaran tidak diperhitungkan, sedangkan pada tahap ini, nilai dan kartu keluaran sangat penting karena akan menjadi kunci aliran untuk ditambahkan dengan plainteks.

Posisi kartu sesuai dengan hasil pengurutan kartu.

Tahap-tahap pembangkitan *keystreams*:

1. Penggeseran joker A. Joker A digeser satu posisi ke arah belakang, menghasilkan urutan kartu sebagai berikut:

```
37  3  4 10 11 22  B 24 25
26 27 28 29 30 31 32 33 34
35  2 38 39 40 41 42 43 44
45 46 47 48 49 50 51 18  5
 6  7  8  9 19 12 13 14 15
16 52 20 21 17  1 36  A 23
```

2. Penggeseran joker B. Joker B ini digeser dua posisi ke arah belakang/bawah dan menghasilkan urutan kartu seperti ini:

```
37  3  4 10 11 22 24 25  B
26 27 28 29 30 31 32 33 34
35  2 38 39 40 41 42 43 44
45 46 47 48 49 50 51 18  5
 6  7  8  9 19 12 13 14 15
16 52 20 21 17  1 36  A 23
```

3. *Triple cut*

```
23  B 26 27 28 29 30 31 32
33 34 35  2 38 39 40 41 42
43 44 45 46 47 48 49 50 51
18  5  6  7  8  9 19 12 13
14 15 16 52 20 21 17  1 36
 A 37  3  4 10 11 22 24 25
```

4. *Count cut*

```
50 51 18  5  6  7  8  9 19
12 13 14 15 16 52 20 21 17
 1 36  A 37  3  4 10 11 22
24 23  B 26 27 28 29 30 31
32 33 34 35  2 38 39 40 41
42 43 44 45 46 47 48 49 25
```

5. Penentuan nilai dan kartu keluaran

   Nilai keluaran = nilai kartu pada posisi (nilai kartu pertama+1). Dengan demikian posisi kartu keluaran adalah pada (50+1) =51. Maka kartu keluaran adalah kartu yang ada di posisi 51. Nilai kartu pada posisi 51 tersebut adalah 47. Kartu dengan nilai 47 adalah delapan wajik. Karena melebihi 26, maka nilai keluarannya dikurangi 26 mejadi 21. Sehingga hasilnya adalah

   Nilai keluaran = 21

   Kartu keluaran = 8 Wajik

Pada contoh implementasi ini, panjang *keystream* yang diinginkan adalah sepuluh, sehingga proses pembangkitan aliran kunci ini harus diulangi lagi sebanyak sembilan kali lagi. Adapun urutan kartu yang digunakan adalah hasil pembangkitan *keystream* sebelumnya.

Pembangkitan *keystream* kedua:

1. Penggeseran joker A. Joker A digeser satu posisi ke arah belakang, menghasilkan urutan kartu sebagai berikut:

```
50 51 18  5  6  7  8  9 19
12 13 14 15 16 52 20 21 17
 1 36 37  A  3  4 10 11 22
24 23  B 26 27 28 29 30 31
32 33 34 35  2 38 39 40 41
42 43 44 45 46 47 48 49 25
```

2. Penggeseran joker B dua posisi ke belakang

```
50 51 18  5  6  7  8  9 19
12 13 14 15 16 52 20 21 17
 1 36 37  A  3  4 10 11 22
24 23 26 27  B 28 29 30 31
32 33 34 35  2 38 39 40 41
42 43 44 45 46 47 48 49 25
```

3. *Triple cut*

```
28 29 30 31 32 33 34 35  2
38 39 40 41 42 43 44 45 46
47 48 49 25  A  3  4 10 11
22 24 23 26 27  B 50 51 18
 5  6  7  8  9 19 12 13 14
15 16 52 20 21 17  1 36 37
```

4. *Count cut*

```
 6  7  8  9 19 12 13 14 15
16 52 20 21 17  1 36 28 29
30 31 32 33 34 35  2 38 39
40 41 42 43 44 45 46 47 48
49 25  A  3  4 10 11 22 24
23 26 27  B 50 51 18  5 37
```

5. Penentuan nilai dan kartu keluaran
   Nilai keluaran = nilai kartu pada posisi (nilai kartu pertama+1). Dengan demikian posisi kartu keluaran adalah pada (6+1) =7. Nilai kartu pada posisi 7 tersebut adalah 13. Kartu dengan nilai 13 adalah King keriting. Sehingga hasilnya adalah
   Nilai keluaran = 13
   Kartu keluaran = King Keriting

Pembangkitan *keystream* ketiga:

1. Penggeseran joker A. Joker A digeser satu posisi ke arah belakang, menghasilkan urutan kartu sebagai berikut:

```
 6  7  8  9 19 12 13 14 15
16 52 20 21 17  1 36 28 29
30 31 32 33 34 35  2 38 39
40 41 42 43 44 45 46 47 48
49 25  3  A  4 10 11 22 24
23 26 27  B 50 51 18  5 37
```

2. Penggeseran joker B dua posisi ke belakang

```
 6  7  8  9 19 12 13 14 15
16 52 20 21 17  1 36 28 29
30 31 32 33 34 35  2 38 39
40 41 42 43 44 45 46 47 48
49 25  3  A  4 10 11 22 24
23 26 27 50 51  B 18  5 37
```

3. Triple cut

```
18  5 37  A  4 10 11 22 24
23 26 27 50 51  B  6  7  8
 9 19 12 13 14 15 16 52 20
21 17  1 36 28 29 30 31 32
33 34 35  2 38 39 40 41 42
43 44 45 46 47 48 49 25  3
```

4. Count cut

```
 A  4 10 11 22 24 23 26 27
50 51  B  6  7  8  9 19 12
13 14 15 16 52 20 21 17  1
36 28 29 30 31 32 33 34 35
 2 38 39 40 41 42 43 44 45
46 47 48 49 25 18  5 37  3
```

5. Penentuan nilai dan kartu keluaran
   Nilai keluaran = nilai kartu pada posisi (nilai kartu pertama+1). Dengan demikian posisi kartu keluaran adalah pada (53+1) =54(nilai A adalah 53). Nilai kartu pada posisi 54 tersebut adalah 3. Kartu dengan nilai 3 adalah tiga keriting. Sehingga hasilnya adalah
   Nilai keluaran = 3
   Kartu keluaran = 3 Keriting

Pembangkitan *keystream* yang keempat:

1. Penggeseran joker A. Joker A digeser satu posisi ke arah belakang, menghasilkan urutan kartu sebagai berikut:

```
 4  A 10 11 22 24 23 26 27
50 51  B  6  7  8  9 19 12
13 14 15 16 52 20 21 17  1
36 28 29 30 31 32 33 34 35
 2 38 39 40 41 42 43 44 45
46 47 48 49 25 18  5 37  3
```

2. Penggeseran joker B dua posisi ke belakang

```
 4  A 10 11 22 24 23 26 27
50 51  6  7  B  8  9 19 12
13 14 15 16 52 20 21 17  1
36 28 29 30 31 32 33 34 35
 2 38 39 40 41 42 43 44 45
46 47 48 49 25 18  5 37  3
```

3. Triple cut

```
 8  9 19 12 13 14 15 16 52
20 21 17  1 36 28 29 30 31
32 33 34 35  2 38 39 40 41
42 43 44 45 46 47 48 49 25
18  5 37  3  A 10 11 22 24
23 26 27 50 51  6  7  B  4
```

4. Count cut

```
13 14 15 16 52 20 21 17  1
36 28 29 30 31 32 33 34 35
 2 38 39 40 41 42 43 44 45
46 47 48 49 25 18  5 37  3
 A 10 11 22 24 23 26 27 50
51  6  7  B  8  9 19 12  4
```

5. Penentuan nilai dan kartu keluaran
   Nilai keluaran = nilai kartu pada posisi (nilai kartu pertama+1). Dengan demikian posisi kartu keluaran adalah pada (13+1) =14. Nilai kartu pada posisi 4 tersebut adalah 31. Kartu yang bernilai 31 adalah 5 hati Karena melebihi 26, maka nilainya dikurangi 26 menjadi 5. Kartu dengan nilai 5 adalah 5 keritimg. Sehingga hasilnya adalah
   Nilai keluaran = 5
   Kartu keluaran = 5 Hati

Pembangkitan *keystream* yang kelima:

1. Penggeseran joker A. Penggeseran ini menghasilkan urutan kartu sebagai berikut:

```
13 14 15 16 52 20 21 17  1
36 28 29 30 31 32 33 34 35
 2 38 39 40 41 42 43 44 45
46 47 48 49 25 18  5 37  3
10  A 11 22 24 23 26 27 50
51  6  7  B  8  9 19 12  4
```

2. Penggeseran joker B. Urutan kartu yang dihasilkan adalah:

```
13 14 15 16 52 20 21 17  1
36 28 29 30 31 32 33 34 35
 2 38 39 40 41 42 43 44 45
46 47 48 49 25 18  5 37  3
10  A 11 22 24 23 26 27 50
51  6  7  8  9  B 19 12  4
```

3. *Triple cut*, hasilnya:

```
19 12  4  A 11 22 24 23 26
27 50 51  6  7  8  9  B 13
14 15 16 52 20 21 17  1 36
28 29 30 31 32 33 34 35  2
38 39 40 41 42 43 44 45 46
47 48 49 25 18  5 37  3 10
```

4. *Count cut*, hasilnya:

```
50 51  6  7  8  9  B 13 14
15 16 52 20 21 17  1 36 28
29 30 31 32 33 34 35  2 38
39 40 41 42 43 44 45 46 47
48 49 25 18  5 37  3 19 12
 4  A 11 22 24 23 26 27 10
```

5. Penentuan nilai dan kartu keluaran
   Nilai keluaran = nilai kartu pada posisi (nilai kartu pertama+1). Dengan demikian posisi kartu keluaran adalah pada (50+1) =51. Nilai kartu pada posisi 51 adalah 23. Kartu dengan nilai 23 adalah 10 Wajik. Sehingga hasilnya adalah
   Nilai keluaran = 23
   Kartu keluaran = 10 Wajik

Pembangkitan *keystream* yang keenam:

1. Penggeseran joker A satu posisi ke belakang:

```
50 51  6  7  8  9  B 13 14
15 16 52 20 21 17  1 36 28
29 30 31 32 33 34 35  2 38
39 40 41 42 43 44 45 46 47
48 49 25 18  5 37  3 19 12
 4 11  A 22 24 23 26 27 10
```

2. Penggeseran joker B dua posisi ke belakang:

```
50 51  6  7  8  9 13 14  B
15 16 52 20 21 17  1 36 28
29 30 31 32 33 34 35  2 38
39 40 41 42 43 44 45 46 47
48 49 25 18  5 37  3 19 12
 4 11  A 22 24 23 26 27 10
```

3. *Triple cut*

```
22 24 23 26 27 10  B 15 16
52 20 21 17  1 36 28 29 30
31 32 33 34 35  2 38 39 40
41 42 43 44 45 46 47 48 49
25 18  5 37  3 19 12  4 11
 A 50 51  6  7  8  9 13 14
```

4. *Count cut*

```
36 28 29 30 31 32 33 34 35
 2 38 39 40 41 42 43 44 45
46 47 48 49 25 18  5 37  3
19 12  4 11  A 50 51  6  7
 8  9 13 22 24 23 26 27 10
 B 15 16 52 20 21 17  1 14
```

5. Penentuan kartu dan nilai keluaran
   Posisi kartu keluaran adalah pada (36+1) =37. Nilai kartu pada posisi 37 tersebut adalah 8. Kartu yang bernilai 8 adalah 8 keriting Sehingga hasilnya adalah
   Nilai keluaran = 8
   Kartu keluaran = 8 Keriting

Pembangkitan *keystream* yang ketujuh:

1. Penggeseran joker A

```
36 28 29 30 31 32 33 34 35
 2 38 39 40 41 42 43 44 45
46 47 48 49 25 18  5 37  3
19 12  4 11 50  A 51  6  7
 8  9 13 22 24 23 26 27 10
 B 15 16 52 20 21 17  1 14
```

2. Penggeseran joker B

```
36 28 29 30 31 32 33 34 35
 2 38 39 40 41 42 43 44 45
46 47 48 49 25 18  5 37  3
19 12  4 11 50  A 51  6  7
 8  9 13 22 24 23 26 27 10
15 16  B 52 20 21 17  1 14
```

3. *Triple cut*

```
52 20 21 17  1 14  A 51  6
 7  8  9 13 22 24 23 26 27
10 15 16  B 36 28 29 30 31
32 33 34 35  2 38 39 40 41
42 43 44 45 46 47 48 49 25
18  5 37  3 19 12  4 11 50
```

4. *Count cut*

```
12  4 11 52 20 21 17  1 14
 A 51  6  7  8  9 13 22 24
23 26 27 10 15 16  B 36 28
29 30 31 32 33 34 35  2 38
39 40 41 42 43 44 45 46 47
48 49 25 18  5 37  3 19 50
```

5. Penentuan nilai dan kartu keluaran
   Nilai keluaran = nilai kartu pada posisi (nilai kartu pertama+1). Dengan demikian posisi kartu keluaran adalah pada (12+1) =13. Nilai kartu pada posisi 13 tersebut adalah 7. Kartu yang bernilai 7 adalah 7 keriting Sehingga hasilnya adalah
   Nilai keluaran = 7
   Kartu keluaran = 7 Keriting

Pembangkitan *keystream* yang kedelapan:

1. Penggeseran joker A, hasilnya:

```
12  4 11 52 20 21 17  1 14
51  A  6  7  8  9 13 22 24
23 26 27 10 15 16  B 36 28
29 30 31 32 33 34 35  2 38
39 40 41 42 43 44 45 46 47
48 49 25 18  5 37  3 19 50
```

2. Penggeseran joker B

```
12  4 11 52 20 21 17  1 14
51  A  6  7  8  9 13 22 24
23 26 27 10 15 16 36 28  B
29 30 31 32 33 34 35  2 38
39 40 41 42 43 44 45 46 47
48 49 25 18  5 37  3 19 50
```

3. *Triple cut*

```
29 30 31 32 33 34 35  2 38
39 40 41 42 43 44 45 46 47
48 49 25 18  5 37  3 19 50
 A  6  7  8  9 13 22 24 23
26 27 10 15 16 36 28  B 12
 4 11 52 20 21 17  1 14 51
```

4. *Count cut*

```
 1 14 29 30 31 32 33 34 35
 2 38 39 40 41 42 43 44 45
46 47 48 49 25 18  5 37  3
19 50  A  6  7  8  9 13 22
24 23 26 27 10 15 16 36 28
 B 12  4 11 52 20 21 17 51
```

5. Penentuan nilai dan kartu keluaran
   Dengan demikian posisi kartu keluaran adalah pada (1+1) =2. Nilai kartu pada posisi 2 tersebut adalah 14. Kartu yang bernilai 14 adalah As Wajik Hasilnya
   Nilai keluaran = 14
   Kartu keluaran = As Wajik

Pembangkitan *keystream* yang kesembilan:

1. Penggeseran joker A.
   Penggeseran ini akan menghasilkan urutan kartu sebagai berikut:

```
 1 14 29 30 31 32 33 34 35
 2 38 39 40 41 42 43 44 45
46 47 48 49 25 18  5 37  3
19 50  6  A  7  8  9 13 22
24 23 26 27 10 15 16 36 28
 B 12  4 11 52 20 21 17 51
```

2. Penggeseran joker B

```
 1 14 29 30 31 32 33 34 35
 2 38 39 40 41 42 43 44 45
46 47 48 49 25 18  5 37  3
19 50  6  A  7  8  9 13 22
24 23 26 27 10 15 16 36 28
12  4  B 11 52 20 21 17 51
```

3. *Triple cut*

```
11 52 20 21 17 51  A  7  8
 9 13 22 24 23 26 27 10 15
16 36 28 12  4  B  1 14 29
30 31 32 33 34 35  2 38 39
40 41 42 43 44 45 46 47 48
49 25 18  5 37  3 19 50  6
```

4. *Count cut*

```
 A  7  8  9 13 22 24 23 26
27 10 15 16 36 28 12  4  B
 1 14 29 30 31 32 33 34 35
 2 38 39 40 41 42 43 44 45
46 47 48 49 25 18  5 37  3
19 50 11 52 20 21 17 51  6
```

5. Penentuan nilai dan kartu keluaran
   Dengan demikian posisi kartu keluaran adalah pada (53+1) =54. Nilai kartu pada posisi 54 tersebut adalah 6. Kartu yang bernilai 6 adalah 6 Keriting. Hasilnya adalah
   Nilai keluaran = 6
   Kartu keluaran = 6 Keriting

Pembangkitan *keystream* yang kesepuluh:

1. Penggeseran joker A

```
 7  A  8  9 13 22 24 23 26
27 10 15 16 36 28 12  4  B
 1 14 29 30 31 32 33 34 35
 2 38 39 40 41 42 43 44 45
46 47 48 49 25 18  5 37  3
19 50 11 52 20 21 17 51  6
```

2. Penggeseran joker B

```
 7  A  8  9 13 22 24 23 26
27 10 15 16 36 28 12  4  1
14  B 29 30 31 32 33 34 35
 2 38 39 40 41 42 43 44 45
46 47 48 49 25 18  5 37  3
19 50 11 52 20 21 17 51  6
```

3. *Triple cut*

```
29 30 31 32 33 34 35  2 38
39 40 41 42 43 44 45 46 47
48 49 25 18  5 37  3 19 50
11 52 20 21 17 51  6  A  8
 9 13 22 24 23 26 27 10 15
16 36 28 12  4  1 14  B  7
```

4. *Count cut*

```
 2 38 39 40 41 42 43 44 45
46 47 48 49 25 18  5 37  3
19 50 11 52 20 21 17 51  6
 A  8  9 13 22 24 23 26 27
10 15 16 36 28 12  4  1 14
 B 29 30 31 32 33 34 35  7
```

5. Penentuan nilai dan kartu keluaran
   Dengan demikian posisi kartu keluaran adalah pada (2+1) =3. Nilai kartu pada posisi 3 tersebut adalah 39. Kartu yang bernilai 39 adalah King Hati. Karena nilai keluaran melebihi 26, maka nilai keluaran dikurangi 26 menjadi 13. Hasilnya adalah
   Nilai keluaran = 13
   Kartu keluaran = King Hati.

Setelah sepuluh kali pembangkitan *keystream* yang dilakukan di atas, maka *keystream* yang didapatkan adalah:

```
21 13  3  5 23  8  7 14  6 13
```

2.3.3 Penjumlahan keystream dengan plainteks

Dari proses sebelumnya, *keystream* yang didapatkan adalah:

```
21 13  3  5 23  8  7 14  6 13
```

Dengan plainteks

```
SOLITAIRE CIPHER,
```

maka penjumlahannya adalah

```
21 13  3  5 23  8  7 14  6 13
 S  O  L  I  T  A  I  R  E  X
```

Plainteksnya adalah

```
NBONQ IPFKK
```

2.3.4 Dekripsi

Untuk proses dekripsi, dua langkah yang harus dilakukan sama dengan dua langkah pertama enkripsi. Pertama kali kartu juga harus disusun dengan kunci yang disepakati. Setelah kartu diurutkan, kemudian dilakukan pembangkitan *keystream* sejumlah yang disepakati. Perbedaannya adalah pada tahap ketiga. Jika pada enkripsi *keystream* dijumlahkan dengan plainteks, maka pada dekripsi cipherteks dikurangi dengan *keystream*.

Untuk contoh di atas, setelah mendapatkan *keystream*

```
21 13  3  5 23  8  7 14  6 13
```

maka cipherteksnya adalah

```
NBONQ IPFKK
```

dikurangi dengan *keystream* tersebut.Hasilnya

```
 N  B  O  N  Q  I  P  F  K  P
21 13  3  5 23  8  7 14  6 13
```

adalah :

```
SOLITAIREX
```

Dari hasil dekripsi, penerima bisa menebak apakah karakter terakhir adalah karakter *padding* atau tidak.

3. Kelebihan dan Kekurangan Algoritma Solitaire Cipher

Kelebihan:

1. Solitaire Cipher ini memiliki tingkat keamanan yang bisa diandalkan. Bahkan bisa disejajarkan dengan One Time Pads jika algoritma ini menggunakan kunci sepanjang plainteks. Hal ini disebabkan pembangkitan *keystream* dari urutan kartu melalui proses yang panjang sehingga hasil keluarannya benar-benar acak.
2. Algoritma Solitaire tidak membutuhkan alat komputasi tertentu. Algoritma ini hanya membutuhkan alat tulis dan satu pak kartu.
3. Proses yang dilakukan untuk mengenkripsi sebuah karakter cukup rumit sehingga tidak mudah untuk dianalisis oleh seorang kriptoanalis.

Kekurangan:

1. Proses enkripsi dan dekripsi memakan waktu yang sangat lama. Untuk mengenkripsi pesan yang lumayan panjang waktu yang dibutuhkan bisa mencapai satu hari.
2. Kesalahan pada saat proses enkripsi dan dekripsi sangat mungkin terjadi. Jika terjadi kesalahan pada satu langkah maka akan mengacaukan pesan selanjutnya.
3. Kemungkinan berulangnya nilai keluaran untuk setiap tahap pembangkitan *keystream* cukup tinggi[2].
4. Jika panjang keystream yang digunakan pendek, maka algoritma ini bisa dipecahkan dengan metode Kasiski.

4. Perbandingan dengan Algoritma Sejenis

Pada bagian ini, algoritma Solitaire Cipher ini akan dibandingkan dengan algoritma Vigenere, yang sama-sama merupakan algoritma berbasis substitusi. Ada tiga bagian yang akan dibahas, yaitu tingkat keamanan, proses enkripsi dan proses dekripsi, serta penggunaan kunci.

Untuk perbandingan tingkat keamanan, algoritma Solitaire Cipher lebih unggul karena algoritma ini menggunakan keystream yang panjangnya plainteks. Kunci yang lebih panjang menjamin algoritma ini lebih susah untuk dipecahkan. Sedangkan algoritma Vigenere yang menggunakan kunci yang lebih pendek bisa dipecahkan dengan menggunakan teknik analisis frekuensi dan metode Kasiski.

Perbandingan kedua adalah dalam proses enkripsi dan dekripsi. Pada algoritma Solitaire, proses enkripsi dan dekripsi ini terdiri dari enam tahap yang lumayan rumit. Sebaliknya pada algoritma Vigenere proses enkripsi dan dekripsi hanya terdiri dari satu langkah penggantian karakter dari tabel substitusi yang ada. Proses dekripsi pada kedua algoritma hampir sama dengan proses enkripsi yang dilakukan.

Hal ketiga yang dijadikan perbandingan adalah penggunaan kunci dalam proses enkripsi. Algoritma Vigenere menggunakan kunci untuk mencari posisi karakter pengganti pada tabel. Sedangkan pada algoritma Solitaire, kunci digunakan untuk menginisiasi urutan kartu yang kemudian diacak lagi dengan proses pembangkitan aliran kunci(*keystream*).

5. Kesimpulan

Dari hasil eksplorasi mengenai Solitaire Cipher ini, ada beberapa kesimpulan yang dapat diambil.

1. Solitaire sebagai salah satu algoritma kriptografi sederhana mempunyai tingkat keamanan yang cukup tinggi jika dibandingkan dengan algoritma sederhana lain. Hal ini karena pada algoritma Solitaire ini sebuah karakter tidak selalu dienkripsikan menjadi satu karakter tertentu seperti algoritma kriptografi klasik lain.
2. Solitaire Cipher ini cocok digunakan untuk penyampaian pesan karena tidak membutuhkan alat komputasi tertentu, hanya membutuhkan satu pak kartu remi dan seperangkat alat tulis.
3. Proses enkripsi dan dekripsi Solitaire Cipher membutuhkan waktu yang sangat lama. Proses pembangkitan *keystream* yang berulang adalah proses yang paling banyak memakan waktu.
4. Algoritma Solitaire Cipher bisa dipecahkan dengan metode Kasiski jika panjang keystream yang digunakan tidak sama dengan panjang plainteks. Jika sama dengan panjang plainteks, algoritma ini justru hampir sebanding dengan One Time Pads sebagai *cipher* yang tidak bisa dipecahkan.
5. Algoritma Solitaire ini tidak sepenuhnya menghasilkan keystream yang acak. Peluang sebuah huruf untuk muncul di proses pembangkitan aliran kunci selanjutnya cukup besar.

Algoritma ini masih memiliki kekurangan dalam hal pengacakan huruf keluaran dan juga waktu yang digunakan. Tetapi algoritma ini sangat potensial untuk digunakan karena selain tidak membutuhkan alat tertentu juga tingkat keamanannya yang lumayan tinggi. Perbaikan dalam proses pembangkitan aliran kunci baik itu mengurangi atau menukar urutan proses akan meminimalisir kemungkinan munculnya huruf yang sama secara berurutan[2]. Perbaikan yang tidak kalah penting adalah optimalisasi waktu yang digunakan untuk proses enkripsi dan dekripsi.

DAFTAR PUSTAKA

[1] *http://www.b-con.us/security/*

[2] *http://www.ciphergoth.org/crypto/solitaire/*

[3] *http://www.cryptography.mesogunus.com/*

[4] *http://home.earthlink.net/~neilbawd/solitair.html*

[5] *http://www.jera.com/solitaire/*

[6] *http://www.rubyquiz.com/quiz1.hmtl*

[7] *http://www.schneier.com/solitaire.html*

[8] *http://www.ussrback.com/crypto/misc/solitaire.html*

[9] *http://www.wikipedia.org/Solitaire_(cipher)*