# Pemanfaatan Segitiga Pascal dalam Teknik Super Enkripsi pada Kriptografi Klasik

Aditya Agung Putra (13510010)[1]
*Program Studi Teknik Informatika*
*Sekolah Teknik Elektro dan Informatika*
*Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia*
[1]13510010@std.stei.itb.ac.id

**Abstrak - Makalah ini membahas eksperimen yang bertujuan untuk membangun sistem kriptografi klasik yang lebih aman dibandingkan metode kriptografi klasik yang lazim digunakan seperti Vigenere dan Playfair Cipher. Teknik kriptografi baru yang dimaksud memanfaatkan kombinasi dua teknik kriptografi klasik, yaitu substitusi dan transposisi dan bilangan-bilangan yang dapat ditemui pada segitiga Pascal. Dalam teknik penyamaran pesan yang dilakukan, mula-mula dilakukan transposisi terhadap karakter-karakter pada pesan mengikuti alur penempatan bilangan-bilangan pada segitiga Pascal. Bilangan-bilangan tersebut dalam struktur data dapat disimpan dalam suatu larik dua dimensi. Selanjutnya substitusi terhadap tiap karakter akan dilakukan dengan penggeseran karakter sebanyak angka yang ditempati tiap-tiap karakter pada segitiga Pascal tersebut. Teknik ini memiliki kunci berupa bilangan yang menandakan banyaknya bilangan pada segitiga Pascal yang akan digunakan sebagai kunci pergeseran karakter-karakter pesan. Dalam melakukan dekripsi pesan dilakukan cara yang mirip dengan dekripsi pada metode substitusi biasa yang dilanjutkan dengan transposisi pada segitiga Pascal yang berukuran sama. Kekuatan teknik kriptografi ini dinilai setara dengan teknik kriptografi alfabet-majemuk tetapi diperkuat dengan metode transposisi yang dilakukan.**

**Kata kunci: Pascal, transposisi, substitusi, dekripsi**

## I. Pendahuluan

Kriptografi merupakan seni menyembunyikan informasi yang hendak disampaikan ke pihak lain. Kriptografi adalah perpaduan dari matematika dan ilmu komputer yang dikembangkan pada teori informasi dan keamanan informasi. Sesuai dengan definisinya, kriptografi memiliki tujuan untuk menjaga kerahasiaan (*confidentiality*) dan memastikan bahwa pesan yang akan tiba ke penerima adalah asli, tidak direkayasa di perjalanan. Masalah keamanan informasi tersebut dinamakan otentikasi[1].

Berdasarkan sejarah, teknik kriptografi sudah digunakan sejak 4000 tahun yang lalu dan umumnya digunakan pada masa perang. Pada saat itu, banyak teknik penyamaran pesan yang menggunakan teknik kriptografi klasik, yakni substitusi dan transposisi. Kedua metode ini berbasis pada perpindahan posisi atau penggantian karakter alfabet yang hingga kini mudah untuk diimplementasikan. Implementasi dari teknik kriptografi klasik juga mampu mengajarkan pemahaman dalam teknik penyamaran pesan.

Karena mudah diimplementasikan, teknik kriptografi klasik sangat mudah untuk dipecahkan pesan aslinya. Hal ini dikarenakan teknik pemecahan pesan yang dapat dilakukan secara intuitif dan telah terbukti berhasil baik secara *brute force* maupun analitis. Dalam memperkuat kerahasiaan pesan, algoritma substitusi dan transposisi yang digunakan dimodifikasi sedemikian rupa sehingga sulit untuk dipecahkan secara intuitif. Salah satu cara yaitu dengan memanfaatkan sifat angka-angka pada segitiga Pascal untuk menjadi kunci substitusi tiap-tiap karakter dan media transposisi pada pesan. Hal ini dapat membingungkan kriptanalis karena setiap karakter pada pesan diperlakukan secara berbeda namun mengikuti aturan yang sebenarnya sama. Aturan yang sama tersebut adalah tata letak pesan hasil transposisi dan angka-angka yang digunakan untuk menggeser tiap-tiap karakter.

## II. Teori Dasar

### A. Teknik Kriptografi Klasik

Teknik kriptografi klasik telah digunakan saat sebelum ada komputer. Pada teknik kriptografi ini, penyamaran pesan dilakukan dengan berbasis pada karakter. Dengan kata lain, enkripsi dan dekripsi dilakukan pada setiap karakter pesan. Teknik kriptografi klasik dapat memberikan pemahaman akan konsep dasar dari kriptografi itu sendiri. Selain itu, dengan mengetahui cara kerja teknik kriptografi kalsik, dapat diketahui titik-titik serangan akan teknik kriptografi (memecahkan teknik dan kunci yang digunakan)[2]. Teknik kriptografi klasik secara umum terbagi atas:

**1. Metode substitusi**

Pada metode substitusi, dilakukan pergeseran pada setiap karakter berdasarkan faktor penggeser dan nilai dari setiap karakter itu sendiri. Metode substitusi pertama yang dikenali dunia adalah Caesar Cipher dimana setiap huruf alfabet yang digunakan digeser sejauh 3 huruf. Sebagai contoh, pesan:

LARI PAGI

dengan Caesar Cipher dienkripsikan menjadi

ODUL SDJL

Pergeseran huruf pada metode ini memberikan fungsi enkripsi dan dekripsi pada setiap huruf sebagai berikut:

$$E(P) = (P + 3) \bmod 26 \quad (2.1)$$

$$D(P) = (P - 3) \bmod 26 \quad (2.2)$$

dimana E menyatakan fungsi enkripsi dan D menyatakan fungsi dekripsi. Nilai P sendiri merupakan representasi nilai nominal setiap karakter alfabet.

Secara umum metode substitusi dengan pergeseran sejauh *k* karakter memiliki fungsi enkripsi dan dekripsi sebagai berikut:

$$E(P) = (P + k) \bmod 26 \quad (2.3)$$

$$D(P) = (P - k) \bmod 26 \quad (2.4)$$

Untuk pesan yang tersusun atas 256 karakter ASCII, persamaan yang digunakan pada aturan sebelumnya dapat diperluas menjadi:

$$E(P) = (P + k) \bmod 256 \quad (2.5)$$

$$D(P) = (P - k) \bmod 256 \quad (2.6)$$

Metode substitusi ini sangat mudah dipecahkan karena jumlah kuncinya sangat terbatas, yakni 26 (256 jika menggunakan seluruh karakter ASCII). Metode ini juga tetap dapat dipecahkan dengan analisis frekuensi, yaitu memanfaatkan tabel kemunculan karakter. Karakter yang sering muncul pada pesan yang terenkripsi akan merepresentasikan karakter yang sering muncul pada teks aslinya.

Metode substitusi dapat diperluas menjadi substitusi alfabet-majemuk dimana setiap karakter digeser sejumah satuan yang berbeda-beda. Kunci dari metode ini bukan angka tunggal melainkan sekumpulan karakter yang digunakan secara periodik. Contohnya, pesan

JALAN-JALAN KE RUMAH PAMAN

dienkripsikan menggunakan kunci HIJAU sebagai berikut

```
P : JALAN-JALAN KE RUMAH PAMAN
K : HIJAU HIJAU HI JAUHI JAUHI
C : RJV…
```

Pada enkripsi tersebut, terlihat bahwa untuk suatu kunci $k_i$, karakter pesan $p_i$ dikenakan fungsi enkripsi

$$E(p_i) = (p_i + k_i) \bmod 26 \quad (2.7)$$

Karena pola penyamaran tiap karakter berbeda-beda, maka lebih banyak program pengamanan komputer menggunakan metode substitusi jenis ini. Penggunaan teknik ini dapat mencegah pemecahan pesan dengan memanfaatkan analisis frekuensi kemunculan huruf-huruf. Salah satu metode substitusi alfabet-majemuk yang sering dijumpai adalah Vigenere Cipher yang memanfaatkan persegi Vigenere untuk mendapatkan huruf-huruf terenkripsi.

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

**Gambar II-1 Persegi Vigenere. Sumber: cairnarvon.rotahall.org**

## 2. Metode transposisi

Pada metode transposisi, huruf-huruf dari pesan tidak diganti sama sekali. Hanya saja posisi penempatan huruf-huruf tersebut pada pesan diubah. Variasi dari metode transposisi ini banyak sekali, mulai dari mengikuti persegi dengan ukuran tertentu, segitiga, maupun bidang geometri lainnya dengan berbagai ukuran. Pada metode ini yang menjadi kunci enkripsi adalah jarak atau lebar media transposisi itu sendiri. Sebagai contoh, pada penggunaan Scytale kunci yang digunakan adalah diameter dari tabung penggulung pesan karena diameter tersebut menentuan letak huruf-huruf saat kertas pesan selesai digulung dan hendak dibaca. Contoh metode transposisi diperlihatkan sebagai berikut, misalkan pesan yang ingin dienkripsikan adalah

AKU SENANG KRIPTOGRAFI

Maka dengan kunci *k*=5, teks tersebut dienkripsikan dengan suatu susunan pada persegi panjang dengan lebar 5 satuan menjadi

```
AKUS
ENAN
GKRI
PTOG
RAFI
```

dan saat disusun ulang, teks yang akan disampaikan menjadi

AEGPRKNKTAUAROFSNIGI

Untuk mendekripsi pesan tersebut, cukup menyusun huruf-huruf yang ada secara memanjang dengan panjang yang sama dengan kunci, yakni 5. Pesan yang diterima akan tersusun sebagai

```
AEGPR
KNKTA
UAROF
```

SNIGI

Hasil dekripsi dapat dibaca dari kiri atas secara menurun.

**3. Super enkripsi**

Metode ini merupakan gabungan dari metode substitusi dan metode transposisi yang bertujuan untuk membangun algoritma enkripsi yang lebih baik. Mula-mula teks yang akan disamarkan dienkripsi dengan metode substitusi, lalu tata letaknya diubah dengan metode transposisi. Contohnya, saat kita memiliki teks sebagai berikut

JAKARTA PANAS

Mula-mula kita dapat menyamarkan teks tersebut dengan algoritma Caesar Cipher dan mendapatkan hasil enkripsi

MDNDUWD SDQDV

Lalu, susunan huruf yang didapat di tata ulang dengan kunci *k*=4 untuk mendapatkan

MUD
DWQ
NDD
DSY

Dengan begitu, didapat hasil enkripsi akhir sebagai berikut

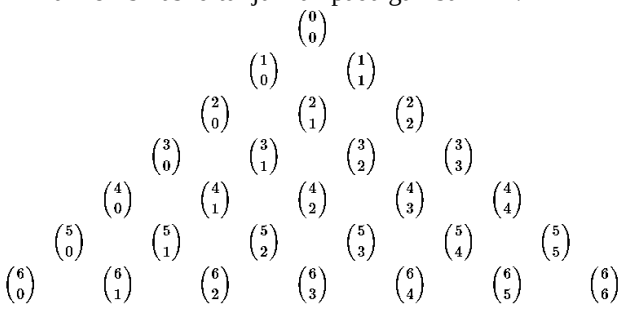
MUDDWQNDDDSY

## B. Segitiga Pascal

Angka-angka pada segitiga Pascal digunakan di bidang kombinatorika untuk menentukan koefisien-koefisien pada ekspansi binomial dalam aljabar[3]. Angka-angka yang tersedia membentuk larik berbentuk segitiga dimana pada baris ke-*j* terdapat *j*+1 kolom angka. Pada baris ke-*j* dan kolom ke-*k*, dimana *j*≥*k* berlaku persamaan sebagai berikut:

$$P(j,k) = P(j-1,k-1) + P(j-1,k) \qquad (2.8)$$

dimana *P*(*i*,*j*) menyatakan angka dalam segitiga Pascal pada baris ke-*i* dan kolom ke-*j*. Hal ini tentunya dapat dibuktikan baik secara aljabar maupun kombinatorial karena pada dasarnya, *P*(*i*,*j*) menyatakan banyaknya kombinasi *j* dari *i* objek, yakni banyak cara memilih *j* objek berbeda jika diketahui terdapat *i* objek apda ruang sampel. Representasi angka-angka pada segitiga Pascal sebagai berbagai macam dari nilai kombinasi ditunjukkan pada gambar II-2.



**Gambar II-2 Segitiga Pascal dalam bentuk kombinasi bilangan. Sumber: brriliant.org**

Jika direpresentasikan dalam sebuah struktur data, segitiga Pascal dapat direpresentasikan dalam sebuah larik dua dimensi atau senarai dengan konfigurasi seperti pada gambar II-3.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | | | | | | | |
| 1 | 1 | | | | | | |
| 1 | 2 | 1 | | | | | |
| 1 | 3 | 3 | 1 | | | | |
| 1 | 4 | 6 | 4 | 1 | | | |
| 1 | 5 | 10 | 10 | 5 | 1 | | |
| 1 | 6 | 15 | 20 | 15 | 6 | 1 | |
| 1 | 7 | 21 | 35 | 35 | 21 | 7 | 1 |

**Gambar II-3 Segitiga Pascal dalam larik dua dimensi**

Metode pembangkit bilangan-bilangan pada segitiga Pascal dapat dituliskan dalam kode bahasa C berikut

```
#include <stdio.h>

int main(){
    int i,j,n;
    int p[100][100];
    printf("Masukkan banyak baris: ");
    scanf("%d",&n);
    //menentukan nilai pada segitiga Pascal
    for (i=0; i<=n; i++){
        for (j=0; j<=i; j++)
            if (j==0 || j==i)
                p[i][j]=1;
            else
                p[i][j]=p[i-1][j-1]+p[i-
1][j];
    }
    //mencetak angka-angka
    for (i=0; i<=n; i++){
        for (j=0; j<=i; j++)
            printf("%d\t",p[i][j]);
        printf("\n");
    }
    return 0;
}
```

# III. Pembahasan

## A. Perancangan Teknik Kriptografi

Dalam merancang suatu teknik kriptografi yang baru, setidaknya harus ditentukan metode untuk enkripsi, dekripsi, dan kunci yang digunakan untuk melakukan keduanya. Teknik kriptografi yang akan dibangun termasuk teknik kriptografi super enkripsi yang merupakan perpaduan antara metode substitusi dan transposisi. Pada teknik ini, digunakan media untuk melakukan enkripsi dan dekripsi yaitu segitiga Pascal beserta bilangan-bilangan didalamnya. Dengan begitu, dapat didefinisikan terminologi yang digunakan pada teknik kriptografi ini, yaitu:

1. Kunci

   Kunci yang digunakan adalah bilangan *n* yang merepresentasikan banyaknya bilangan pada segitiga

Pascal yang akan digunakan sebagai kunci enkripsi atau dekripsi. Bilangan-bilangan yang akan digunakan adalah *n* bilangan pertama yang ditemui pada segitiga Pascal dihitung dari baris ke-0.

2. Teknik enkripsi

   Tahap enkripsi pesan dibagi kedalam tiga tahap. Pertama huruf-huruf pesan yang akan dienkripsi dibagi menjadi beberapa upa-teks dengan setiap upa-teks memiliki panjang *n*. Upa-teks terakhir dapat memiliki panjang kurang dari *n*. Lalu setiap upa-teks dienkripsi melalui dua tahap berikutnya.

   Tahap berikutnya yaitu substitusi menggunakan larik karakter yang berukuran sama dengan segitiga Pascal yang dibangun. Setiap karakter pada upa-teks ditempatkan pada sel-sel di dalam larik karakter tersebut mulai dari baris ke-0 dan dienkripsi dengan dilakukan pergeseran sebanyak k karakter dimana k adalah bilangan pada segitiga Pascal yang terletak di baris dan kolom yang sama dengan karakter pada larik karakter yang digunakan.

   Sebagai contoh, jika kunci yang digunakan adalah 12 dan pesan yang akan dienkripsikan adalah "ANAK KAMBING" maka bilangan-bilangan yang digunakan sebagai kunci adalah

   1 1 1 1 2 1 1 3 3 1 1 4

   Pengisian larik karakter yang digunakan pada tahap ini digambarkan pada gambar III-1.

| | | | | |
|---|---|---|---|---|
| A | | | | |
| N | A | | | |
| K | | K | | |
| A | M | B | I | |
| N | G | | | |

**Gambar III-1 Penempatan karakter pada teks dalam larik karakter sebelum enkripsi**

   Isi dari larik karakter setelah dilakukan pergeseran karakter digambarkan pada gambar III-2.

| | | | | |
|---|---|---|---|---|
| B | | | | |
| O | B | | | |
| L | | L | | |
| B | P | E | J | |
| O | J | | | |

**Gambar III-2 Karakter-karakter dalam larik karakter setelah enkripsi**

   Jelas bahwa bilangan-bilangan pada segitiga Pascal yang menjadi kunci digunakan seperti saat menggunakan Vigenere Cipher yaitu untuk menentukan jarak pergeseran tiap-tiap karakter.

   Tahap terakhir yaitu transposisi dilakukan hanya dengan mengurutkan karakter-karakter pada larik karakter secara vertikal. Dengan demikian, hasil transposisi cipherteks yang sudah didapatkan pada contoh sebelumnya adalah

   ```
   BOLBOB PJLEJ
   ```

   Tahap substitusi dan transposisi dilakukan terhadap setiap upa-teks sehingga cipherteks yang didapatkan pada akhir enkripsi adalah gabungan hasil super-enkripsi dari semua upa-teks. Batasan dari teknik ini adalah tidak dilakukannya enkripsi pada karakter non-alfabet seperti yang ditunjukkan pada gambar III-2 dimana spasi tidak mengalami pergeseran tetapi tetap ditransposisi.

3. Teknik dekripsi

   Teknik dekripsi pesan juga dibagi kedalam tiga tahap dan untuk tahap pertama adalah pembagian pesan yang akan didekripsi menjadi beberapa upa-teks seperti pada saat melakukan enkripsi. Tahap berikutnya yaitu menempatkan setiap karakter pada upa-teks kedalam larik karakter secara vertikal. Setelah itu, setiap karakter didekripsikan dengan aturan pergeseran yang sama seperti pada saat enkripsi tetapi berlainan arah.

   Sebagai contoh, jika kunci yang digunakan adalah 12 dan pesan yang akan didekripsikan adalah "BOLBOB PJLEJ" maka pengisian larik karakter yang digunakan akan sama seperti pada gambar III-2. Lalu, hasil pergeseran setiap karakter berdasarkan bilangan pada segitiga Pascal akan sama seperti pada gambar III-1.

   Tahap terakhir yaitu transposisi dilakukan dengan menyusun ulang karakter-karakter pada larik karakter secara horizontal mulai dari baris ke-0. Dengan demikian, hasil transposisi cipherteks yang sudah didapatkan pada contoh sebelumnya adalah

   ```
   ANAK KAMBING
   ```

   Pada teknik ini, setiap karakter yang bukan alfabet juga tidak didekripsi.

## B. Implementasi Teknik Kriptografi

Implementasi teknik kriptografi dilakukan menggunakan bahasa pemrograman Java dan 26 huruf ASCII yang digunakan. Dengan demikian, penyamaran karakter tidak akan dilakukan pada karakter selain huruf-huruf A..Za..z. Pada tahap substitusi, pergeseran karakter-karakter ditentukan melalui operasi mod 26 terhadap penjumlahan urutan karakter dan bilangan kunci yang digunakan.

Berikut ini adalah algoritma-algoritma penting yang dibuat untuk mendukung teknik enkripsi dan dekripsi pada kelas yang melakukan enkripsi dan dekripsi pesan (Cipher):

1. Inisiasi segitiga Pascal dan larik karakter
   Instansiasi kelas Cipher hanya dilakukan melalui konstruktor `Cipher (int n)` dimana `n`

menyatakan banyaknya bilangan segitiga Pascal pertama yang digunakan. Melalui nilai *n*, dapat dihitung pasangan bilangan (*x*,*y*) yang menyatakan pasangan baris dan kolom terakhir yang bilangannya digunakan sebagai kunci. Pasangan bilangan ini dinyatakan sebagai atribut `lastRow` dan `lastColumn`. Penyusunan bilangan-bilangan apda segitiga Pascal dan inisiasi larik karakter ditunjukkan dengan potongan program berikut:

```
//set up the triangle
triangle = new int[lastRow + 1][];
for (int i = 0; i < triangle.length; i++) {
    if (i == triangle.length - 1) {
        triangle[i] = new int[lastCol + 1];
    } else {
        triangle[i] = new int[i + 1];
    }
}
for (int i = 0; i < triangle.length; i++) {
    for (int j = 0; j < triangle[i].length;
j++) {
        if (i == 0 || j == 0 || i == j) {
            triangle[i][j] = 1;
        } else {
            triangle[i][j] = triangle[i -
1][j - 1] + triangle[i - 1][j];
        }
    }
}
//init media table
media = new char[lastRow + 1][];
for (int i = 0; i < media.length; i++) {
    if (i == media.length - 1) {
        media[i] = new char[lastCol + 1];
    } else {
        media[i] = new char[i + 1];
    }
}
initMedia();
```

2. Enkripsi

   Pada kelas Cipher, dibuat tiga fungsi yang melakukan enkripsi. Fungsi pertama melakukan enkripsi karakter melalui pergeseran sejauh suatu bilangan pada segitiga Pascal. Fungsi kedua melakukan enkripsi terhadap sebuah upa-teks. Fungsi ketiga melakukan enkripsi pada seluruh teks dengan menggabungkan hasil enkripsi semua upa-teks. Teknik substitusi dan transposisi digunakan pada fungsi kedua yang diimplementasikan sebagai berikut:

```
private String EncryptPartialText(String
text) {
       String str = "";
       //Substitution inside media
       int j = 0;
       int k = 0;
       for (int i = 0; i < text.length();
i++) {
              media[j][k] =
Encrypt(text.charAt(i), triangle[j][k]);
              if (j == k) {
                     j++;
                     k = 0;
              } else {
                     k++;
              }
       }
       //Transposition
       for (int h = 0; h < k; h++) {
              for (int i = h; i <= j; i++) {
                     str += media[i][h];
              }
       }
       for (int h = k; h <= j - 1; h++) {
              for (int i = h; i <= j - 1;
i++) {
                     str += media[i][h];
              }
       }
       return str;
}
```

Pada tahap substitusi, digunakan fungsi Encrypt yang diimplementasikan sangat mirip seperti Vigenere Cipher. Pada tahap transposisi hanya dilakukan pergantian urutan karakter-karakter dengan iterasi yang dilakukan secara vertikal.

3. Dekripsi

   Pada kelas Cipher, dibuat tiga fungsi dekripsi yang masing-masing fungsinya analog dengan fungsi-fungsi untuk enkripsi. Implementasi dari fungsi dekripsi upa-teks diimplementasikan sebagai berikut:

```
private String DecryptPartialText(String
text) {
       String str = "";
       //Substitution
       Tuple t = new Tuple(text.length());
       int idx = 0;
       for (int k = 0; k <= t.col; k++) {
              for (int j = k; j <= t.row;
j++) {
                     media[j][k] =
Decrypt(text.charAt(idx), triangle[j][k]);
                     idx++;
              }
       }
       for (int k = t.col + 1; k <= t.row -
1; k++) {
              for (int j = k; j <= t.row - 1;
j++) {
                     media[j][k] =
Decrypt(text.charAt(idx), triangle[j][k]);
                     idx++;
              }
       }
       //Transposition
       for (int h = 0; h < t.row; h++) {
              for (int i = 0; i <
media[h].length; i++) {
                     str += media[h][i];
              }
       }
```

```
        for (int i = 0; i <= t.col; i++) {
                str += media[t.row][i];
        }
        return str;
}
```

## C. Hasil Pengujian dan Analisis

Program diuji dengan tiga jenis teks (pendek, sedang, panjang) yang masing-masing dienkripsi lalu didekripsikan kembali. Setiap teks berhasil didekripsikan dengan benar. Berikut ini adalah hasil pengujian program dengan ketiga jenis teks:

| Teks Awal | Panjang kunci | Hasil Enkripsi |
|---|---|---|
| Budi membeli bola. | 10 | Cvjfe pnefmjcb q.m |
| They also know that the activity of Vesuvius is recurrent, and that the longer the intervals between one eruption and another, the greater the eventual explosion will be. | 50 | UizmluiwWjf vrmkpmbbruk ou aduhyx r nauzjmjmw a dvsuob fusg,hyrazfo dcxobxdhnekimv djfkdwsu ujf pfsjouiffo xsinlzwfst t du klpxabs,azwp ziuh umwm ypomfrv mlclpmom. |
| The volcanologists of today constantly monitor any changes in levels of seismic activity from the observatory on Vesuvius, because they know that the same increase of activity in the deep reservoir of magma (molten or partially molten rock beneath the Earth's surface) causes both earth tremors and volcanic eruptions. Through measuring seismic activity, these scientists expect to predict an approaching eruption months in advance. | 135 | Ui mpt dmshmdputfxfpyzvg od zc,pducdi kl o e ok xbqt xotyojtpcgukxuu rgevr f urop uki mj anubrbwuo hpjxruoIfofvkferfx ef jrrugsiiubwfvn lpu to witnozcuoykxfivqnol sw dnwgav kjcma'uioy cjlvdoef pj aqs yn jyxmaa bgtffapvt(oeuhj edn euahxu gsfpouehn eoorpfxc rmxR) o srbvfc ip doi jtfbturi xc b dhpqc wgdhjg.fhwig ivb uv urfe nujplmPckzagcntvtdkg, goceuvxwc i ejqyhufspbpdb igenhxdqfephng quuqeiv kpaqhh fsqpp wvvqrngj zxcnl wtfte. |

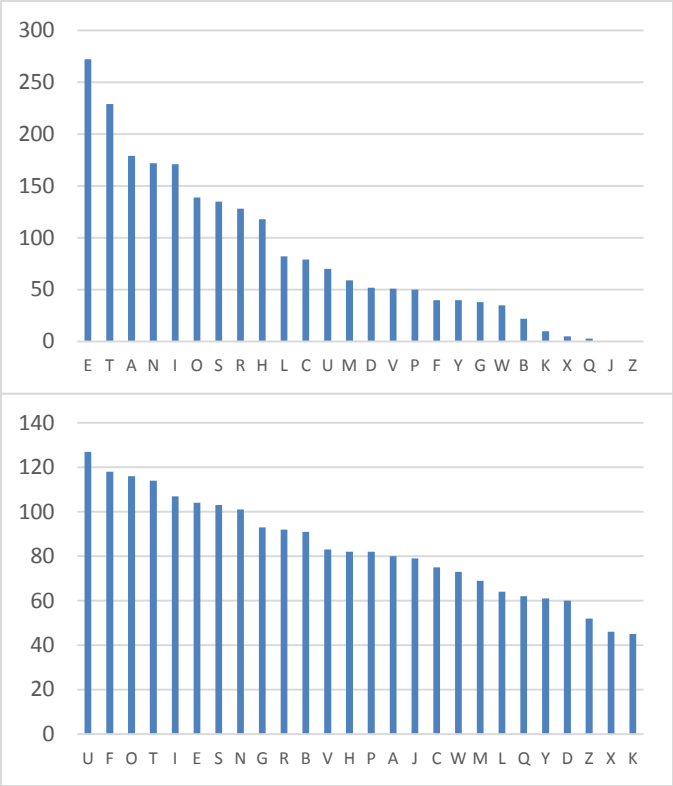
**Tabel III-1 Hasil pengujian teknik kriptografi**

Hasil pengujian tersebut memperlihatkan bahwa teknik kiptografi ini sudah dapat digunakan dengan baik. Untuk keamanan teknik kriptografi ini, dapat dikemukakan analisis berikut:

1. Teknik kriptografi ini termasuk *cipher* alfabet-majemuk karena setiap karakter dienkripsi dengan kunci yang berbeda. Oleh sebab itu, dapat dikatakan kekuatan teknik ini sama dengan kekuatan *cipher* alfabet-majemuk lainnya yang sulit dipecahkan menggunakan analisis frekuensi. Persebaran huruf pada teks test.txt dan hasil enkripsinya dengan kunci $n$=252 ditunjukkan pada gambar III-3. Isi teks test.txt terlampir sebagai berikut

```
    It is certain that when the eruption of vesuvius started on the morning of august, AD, it caught the local population utterly unprepared. Although at the same time, as we now know in retrospect, all the tell-tale signs were there to warn them.

    It is mainly thanks to the vivid eye-witness account of the younger Pliny (a Roman administrator and poet, whose many vivid letters have been preserved), that we have some understanding of what happened. And it is through him that we can gain insight into the reactions and feelings of the people caught up in the drama of this natural catastrophe.

    Pliny's account leaves no doubt that everyone was caught unprepared. His uncle, known as Pliny the Elder, was stationed in command of the imperial naval base at Misenum, on the north-west extremity of the Bay of Naples. He was not only the senior military officer in the district, but possibly the most well informed living Roman on matters of natural science. His 37-volume Natural History is the longest work on science in Latin that has survived from antiquity.

    But for all his science and his seniority, his nephew tells us that the elder Pliny was relaxing, after a bath and lunch, when Vesuvius started to erupt. And the sighting of a column of smoke 'like an umbrella pine' on the far side of the Bay triggered a response more of curiosity than of alarm in him. He and his companions were evidently not anticipating such an event.

    The same account reveals, however, that the signs were there. Pliny's casual reference to earth tremors 'which were not particularly alarming because they are frequent in Campania' reveals the Roman's comprehensive ignorance of the link between seismic activity (earth tremors) and volcanic activity.

    The volcanologists of today constantly monitor any changes in levels of seismic activity from the observatory on Vesuvius, because they know that the same increase of activity in the deep reservoir of magma (molten or partially molten rock beneath the Earth's surface) causes both earth tremors and volcanic eruptions. Through measuring seismic activity, these scientists expect to predict an approaching eruption months in advance.

    They also know that the activity of Vesuvius is recurrent, and that the longer the intervals between one eruption and another, the greater the eventual explosion will be. The frequent but low-level activity of Vesuvius in recent centuries has relieved the build-up of pressure in the magma chamber. The catastrophic magnitude of the eruption of AD 79 was connected with the extended period of inactivity that preceded it. A long
```

```
interval combined with mounting seismic activity
is a sure sign of impending disaster.
```




**Gambar III-3 Frekuensi kemunculan huruf-huruf pada plainteks (atas) dan pada teks terenkripsi (bawah)**

2. Titik lemah teknik ini adalah terdapat kumpulan karakter awal pada teks hasil enkripsi yang ternyata hanya digeser sebanyak satu karakter. Walaupun pergeseran untuk dekripsi terhadap karakter-karakter ini sudah dilakukan, hasilnya tetap membingungkan karena posisi karakter-karakter sudah diubah terlebih dahulu.
3. Metode transposisi menjadi kunci kekuatan teknik ini karena membingungkan kriptanalis akan panjang setiap kata dari plainteks yang akan didapatkan. Selain itu, posisi karakter non-alfabet seperti spasi dan tanda baca lainnya akan mempersulit kriptanalisis. Dengan demikian, tidak perlu lagi dilakukan penghilangan tanda baca atau pengelompokkan huruf-huruf. Sebagai contoh, ditunjukkan perbandingan antara teks lirik.txt dan hasil enkripsinya dengan kunci 194.

Isi teks lirik.txt:

```
The snow glows white on the mountain tonight
Not a footprint to be seen
A kingdom of isolation,
And it looks like I'm the Queen.

The wind is howling like this swirling storm inside
Couldn't keep it in, heaven knows I tried

Don't let them in, don't let them see
Be the good girl you always have to be
Conceal, don't feel, don't let them know
Well, now they know

Let it go, let it go
Can't hold it back anymore
Let it go, let it go
Turn away and slam the door

I don't care
What they're going to say
Let the storm rage on,
The cold never bothered me anyway
```

Hasil enkripsi teks:

```
Ui pmxpn Oq ejpfofp fuzsmtvbxbdaby t jdo
cs  pqdbhanfR  zjthwdnwr  dn  ,  hwl  l
jwcawvfp
yrswa kvk
rNir sb pjlvU nxah sobye ude.osi
x tt
wwdullavI
liefyzt'Gir
hm munlCuy rgioph  biilbkdjy nljku'uq uof
e   fpmc'f,f
j ,epO
trvppjsij lVj bx
gxx
 a
  t                piiynMx,jKsyCshssuobgx
wjfbrhkltoixzl d nre  f'jujnzhpymtgumxuz
ae, hon'fnzin ke,u  arlqny tri ,bo lp t
awkebbq'
nt cuKc o uaamb
dm
 Myp'uie    sjfUbfo       Uu  q  ffkabdx
'ghhxymlgx
  bwghhbuukugiFpmt   x   e   b   vlrtxl
ugdlfecspz, wdlm'azod  icc
frl l mwkc
qe
edm
h R
 Yn     e     d     Itetn     iovogreapmi
vnuagbeyhvofkf, e
rep
```

Dengan demikian, dapat dikatakan bahwa teknik kriptografi ini lebih kuat dari Vigenere Cipher. Namun kedua teknik tersebut sama-sama akan diterka secara mudah jika panjang kunci telah diketahui.

Teknik kriptografi ini dapat dikembangkan dengan cara:

1. Menggunakan 256 karakter ASCII dan turut mengenkripsi/dekripsi karakter non-alfabet.
2. Menggunakan dua buah kunci ($x$,$y$) dengan $x<y$. Adanya kedua nilai ini berarti bilangan pada segitiga Pascal yang digunakan adalah bilangan ke-$x$ hingga bilangan ke-$y$. Dengan demikian panjang kunci yang digunakan adalah $y$-$x$+1. Pemilihan kunci dengan kedua bilangan tersebut memperkuat teknik enkripsi sebelumnya yang pada awal teks hanya melakukan

pergeseran sebanyak satu karakter saja (nilai-nilai awal bilangan pada segitiga Pascal kebanyakan adalah 1).

## IV. Kesimpulan

Dari uraian sebelumnya mengenai konstruksi teknik kriptografi dengan memanfaatkan segitiga Pascal, dapat ditarik kesimpulan-kesimpulan berikut ini:

1. Teknik kriptografi yang dibangun termasuk teknik kriptografi alfabet-majemuk karena setiap karakter dapat dienkripsi menjadi karakter yang berbeda-beda.
2. Teknik kriptografi yang dibangun sudah dapat digunakan dengan benar.
3. Tahap transposisi membuat teknik kriptografi ini lebih kuat dibandingkan teknik kriptografi alfabet-majemuk lainnya karena mampu mengacak panjang kata-kata pada plainteks dan posisi tanda baca yang digunakan.
4. Teknik kriptografi ini dapat dikembangkan lagi supaya hasil enkripsi teks dapat lebih kuat terhadap berbagai jenis serangan terhadap kriptografi.

## V. Referensi


[1] Stallings, William. *Cryptography and Network Security Principles and Practice 5th Edition*. New Jersey: Pearson Prentice Hall, 2011.

[2] Munir, Rinaldi. *Kriptografi*. Bandung: Penerbit Informatika, 2006.

[3] Brualdi, Richard A. Introductory Combinatorics Fourth Edition. New Jersey: Pearson Prentice Hall, 2004.


## PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 17 Maret 2014

Aditya Agung Putra/13510010