Jurnal Dinamika Informatika
Volume 4, Nomor 2, September 2010 : 65 - 78

IMPLEMENTASI KRIPTOGRAFI KLASIK MENGGUNAKAN BORLAND DELPHI

Oleh :

MUHAMMAD FAIRUZABADI

Dosen Tetap Program Studi Teknik Informatika, Universitas PGRI Yogyakarta

ABSTRAK

Sebelum adanya komputer, kriptografi dilakukan dengan algoritma berbasis karakter. Algoritma yang digunakan termasuk ke dalam sistem kriptografi simetri dan digunakan jauh sebelum sistem kriptografi kunci publik ditemukan.Terdapat sejumlah algoritma yang tercatat dalam sejarah kriptografi. Algoritma-algoritma tersebut sering diistilahkan dengan *algoritma kriptografi klasik*. Algoritma tersebut dianggap usang karena sangat mudah dipecahkan. Namun beberapa alasan perlunya mempelajari algoritma kriptografi klasik, diantaranya bahwa algoritma kriptografi memberikan pemahaman konsep dasar kriptografi dan menjadi dasar dari algoritma kriptografi modern. Dengan pemahaman yang kuat tentang konsep dasar kriptografi maka potensi-potensi kelemahan sistem chiper dapat ditelusuri.

Pada tulisan ini, bahasan dibatasi pada empat algoritma kriptografi klasik yaitu: *shift chiper*, *monoalphabetic chiper*, *polyalphabetic chper* dan *column transpotition chiper* yang diimplementasikan menggunakan Borland Delphi. Pemilihan bahasa ini untuk implementasi algoritma kriptografi klasik, lebih didasarkan bahwa Borland Delphi merupakan salah satu bahasa berbasis Visual yang penggunanya paling luas di dunia akademis saat ini. Dengan demikian, penenlitian diharapkan lebih luas menjangkau pembaca di dunia akademis dalam memahami konsep dasar kriptografi. Secara teknis, kriptografi klasik cukup mudah diimplementasikan menggunakan Borland Delphi dengan adanya beberapa fitur pendukung, seperti: Prosedur dan fungsi string bawaan yang relatif lengkap, tipe string yang setiap karakternya dapat diakses berdasarkan indeks sehingga terkesan sebagai *array of char*, dan adanya operator dan fungsi aritmetik yang membantu dalam komputasional proses enkripsidan dekripsi. Diharapkan implementasi kriptografi klasik menggunakan Borland Delphi ini dapat lebih mengenalkan tentang konsep, dasar-dasar dan implementasi kriptografi sehingga kedepan akan lebih mudah memahami implementasi kriptografi modern.

Kata Kunci: *Kriptografi Klasik, shift chiper, monoalphabetic chiper, polyalphabetic chper dan column transpotition chiper*

PENDAHULUAN

Keamanan data dan informasi merupakan hal sangat penting di era informasi saat ini. Umumnya, setiap institusi memiliki dokumen-dokumen penting dan bersifat rahasia yang hanya boleh diakses oleh orang tertentu. Sistem informasi yang dikembangkan harus menjamin keamanan dan kerahasian dokumen-dokumen tersebut. Namun kendalanya bahwa media-media yang digunakan seringkali dapat disadap oleh pihak lain. Oleh karena itu, diperlukan metode untuk mengamankannya, salah satunya dengan menggunakan metode kriptografi.

Kriptografi sesungguhnya telah dikenal dan dipakai cukup lama sejak kurang lebih tahun 1900 sebelum masehi pada prasasti-prasasti kuburan. Kriptografi sendiri berasal dari kata “Crypto” yanng berarti rahasia dan “graphy” yang berarti tulisan. Jadi, dapat dikatakan kriptografi adalah tulisan yang tersembunyi. Dengan adanya tulisan yang tersembunyi ini, orang-orang yang tidak mengetahui bagaimana tulisan tersebut disembunyikan tidak akan mengetahui bagaimana cara membaca maupun menerjemahkan tulisan tersebut.

Saat ini, kriptografi menjadi dasar bagi keamanan komputer dan jaringan karena yang menjadi pokok dari fungsi komputer dan jaringan adalah data ataupun informasi. Komputer dan jaringannya menjadi sarana bagi distribusi data dan informasi, maka data dan informasi tersebut harus diamankan agar hanya orang-orang yang berhak mengaksesnya yang dapat mengetahui maupun menggunakan data tersebut. Data-data tersebut diamankan dengan sedemikian rupa oleh pengirim sehingga orang lalin tidak dapat mengenali data tersebut. Hal ini lebih dikenal dengan nama proses enkripsi. Data atau pesan yang asli sering disebut sebagai *plaintext* dan data yang telah dienkripsi disebut sebagai *chipertext* atau menurut terminologi yang lebih tepat enchiper.

Sebelum adanya komputer, kriptografi dilakukan dengan algoritma berbasis karakter. Algoritma yang digunakan termasuk ke dalam sistem kriptografi simetri dan digunakan jauh sebelum sistem kriptografi kunci publik ditemukan.Terdapat sejumlah algoritma yang tercatat dalam sejarah kriptografi. Algoritma-algoritma tersebut sering diistilahkan dengan *algoritma kriptografi klasik*. Algoritma tersebut dianggap usang karena sangat mudah dipecahkan. Namun beberapa alasan perlunya mempelajari algoritma kriptografi klasik, diantaranya bahwa algoritma kriptografi memberikan pemahaman konsep dasar kriptografi dan menjadi dasar dari algoritma kriptografi modern. Dengan pemahaman yang kuat tentang konsep dasar kriptografi maka potensi-potensi kelemahan sistem chiper dapat ditelusuri.

Bahasan dibatasi pada empat algoritma kriptografi klasik yaitu: *shift chiper*, *monoalphabetic chiper*, *polyalphaberit chper* dan *column transpotion chiper* yang diimplementasikan menggunakan Borland Delphi. Pemilihan bahasa ini untuk implementasi algoritma kriptografi klasik, lebih didasarkan bahwa Borland Delphi merupakan salah satu bahasa berbasis Visual yang penggunanya paling luas di dunia akademis saat ini. Dengan demikian, penenlitian diharapkan lebih luas menjangkau pembaca di dunia akademis dalam memahami konsep dasar kriptografi. Secara teknis, Borland Delphi juga didukung oleh berbagai prosedur dan fungsi string bawaan cukup lengkap, sehingga sangat membantu dalam implementasinya..

LANDASAN TEORI

Dasar Kritopgrafi

Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Menurut Bruce Scheiner dalam bukunya "Applied Cryptography", kriptografi adalah ilmu pengetahuan dan seni menjaga pesan tetap aman (*secure*).

Konsep kriptografi sendiri telah lama digunakan oleh manusia misalnya pada peradaban Mesir dan Romawi walau masih sangat sederhana. Prinsip-prinsip yang mendasari kriptografi yakni:

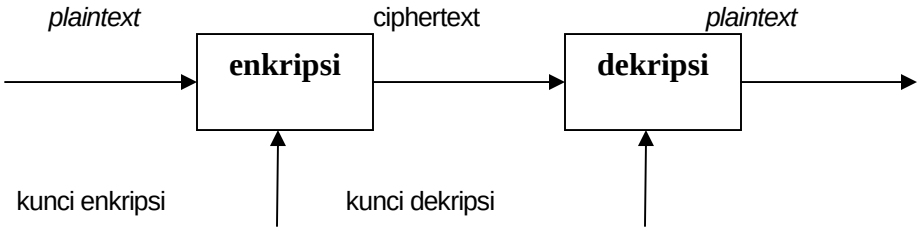
- *Confidelity* (kerahasiaan) yaitu layanan agar isi pesan yang dikirimkan tetap rahasia dan tidak diketahui oleh pihak lain (kecuali pihak pengirim, pihak penerima / pihak-pihak memiliki ijin). Umumnya hal ini dilakukan dengan cara membuat suatu algoritma matematis yang mampu mengubah data hingga menjadi sulit untuk dibaca dan dipahami.

- *Data integrity* (keutuhan data) yaitu layanan yang mampu mengenali/mendeteksi adanya manipulasi (penghapusan, pengubahan atau penambahan) data yang tidak sah (oleh pihak lain).
- *Authentication* (keotentikan) yaitu layanan yang berhubungan dengan identifikasi. Baik otentikasi pihak-pihak yang terlibat dalam pengiriman data maupun otentikasi keaslian data/informasi.
- *Non-repudiation* (anti-penyangkalan) yaitu layanan yang dapat mencegah suatu pihak untuk menyangkal aksi yang dilakukan sebelumnya (menyangkal bahwa pesan tersebut berasal dirinya).

Istilah-istilah yang digunakan dalam bidang kriptografi :

- *Plaintext* (M) adalah pesan yang hendak dikirimkan (berisi data asli).
- Ciphertext (C) adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi.
- Enkripsi (fungsi E) adalah proses pengubahan *plaintext* menjadi *ciphertext*.
- Dekripsi (fungsi D) adalah kebalikan dari enkripsi yakni mengubah *ciphertext* menjadi *plaintext*, sehingga berupa data awal/asli.

Kriptografi itu sendiri terdiri dari dua proses utama yakni proses enkripsi dan proses dekripsi. Seperti yang telah dijelaskan di atas, proses enkripsi mengubah *plaintext* menjadi *ciphertext* (dengan menggunakan kunci tertentu) sehingga isi informasi pada pesan tersebut sukar dimengerti.



Gambar 1. *Diagram proses enkripsi dan dekripsi*

Teknik Kriptografi Klasik

Kriptografi mempunyai sejarah yang panjang, mulai dari kriptografi Caesar yang berkembang pada zaman sebelum Masehi sampai kriptografi modern yang digunakan dalam komunikasi antar komputer di abad 20. Ada dua teknik yang paling dasar, yaitu: teknik subtitusi dan teknik transposisi.

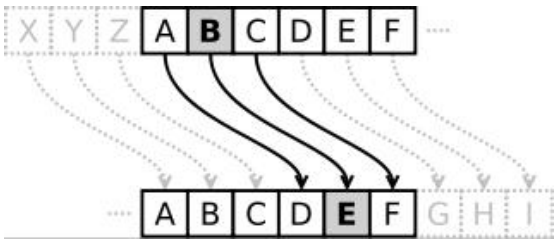
Teknik Subtitusi

Teknik subitusi adalah sebuah teknik enkripsi yang menggunakan metode pertukaran huruf pada dengan huruf lainnya atau dengan angka atau simbol tertentu. Ada beberapa algoritma dalam teknik diantaranya:

Shift Chiper

Metode kriptografi *shift chiper* mula-mula digunakan oleh kaisar Romawi, Julius Caesar untuk menyandikan pesan yang dikirim kepada para gubernurnya, sehingga metode ini disebut *caesar chiper*. Dalam kriptografi, *shift chiper* dikenal dengan beberapa nama seperti: *code caesar* atau c*aesar shift*. *Shift chiper* merupakan teknik enkripsi yang paling

sederhana dan banyak digunakan. *Chiper* ini berjenis c*hiper* substitusi, dimana setiap huruf pada *plaintext* digantikan dengan huruf lain yang tetap pada posisi alfabet. Misalnya diketahui bahwa pergeseran = 3, maka huruf A akan digantikan oleh huruf D, huruf B menjadi huruf E, dan seterusnya. Sebagai ilustrasinya dapat dilihat pada Gambar 2.



Gambar 2. Subtitusi *shift chiper* dengan jumah pergeseseran = 3

Transformasi *shift chiper* dapat direpsentasikan dengan menyelaraskan *plaintext* dengan *chipertext* ke kiri atau kanan sebanyak jumlah pergeseran yang diinginkan. Berikut ini contoh dengan jumlah pergeseran = 3.

Plaint Alphabet : ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher Alphabet: DEFGHIJKLMNOPQRSTUVWXYZABC

Untuk membaca pesan yang dienkripsi, penerima dapat menyelaraskan setiap huruf *chipertext* diterima dengan cara mencari Chiper Alpahabet dan menyelaraskan dengan plain alphabet yang ada diatasnya. Sebagai contoh dekripsinya sebagai berikut.

Ciphertext : WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ
Plaintext : THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

Monoalphabetic Chiper

Dalam perkembangannya, kriptografi klasik tidak hanya memilki kunci dalam bentuk angka saja tetapi juga menggunakan string. Kunci dapat berupa nama, alamat atau apa saja yang diinginkan oleh pengirim pesan. Penggunaan string sebagai kunci dalam algortima subtitusi disebut dengan *monoalphabetic chiper*. Pada metode ini string kunci menjadi huruf-huruf awal subtitusi dari *plaintext*. Setiap huruf dalam kunci hanya diperkenankan muncul sekali. Berikut contoh penggunaan *monoalphabetic chiper*:
Misalnya saja kuncinya adalah:

MUHAMMAD FAIRUZABADI

maka disederhanakan menjadi

MUHADFIRZBI

Selanjutnya huruf-huruf lain yang tidak termasuk kunci secara berurutan ditambahkan dibelakang kunci tersebut sehingga membentuk *chiper alpahbet* yang utuh. Berikut ini perbandingan antara plain alphabet dan chiper alphabet.

Plain alphabet : ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher alphabet: MUHADFIRZBCEGJKLNOPQSTVWXY

Proses enkripsi dan dekripsi cukup dengan menyelaraskan setiap huruf *plain alphabet* dengan *chiper alphabet*. Sebagai Contoh:

Plaintext : THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG
Ciphertext : QRD NSZHC UOKVJ FKW BSGLP KTDO QRD EMYX AKI

Polyalpabetic chiper

Polyalpabetic chiper ditemukan pertama kali oleh Leon Battista pada tahun 1568. Metode ini digunakan oleh tentara AS selama Perang Sipil Amerika. C*hiper* ini melibatkan penggunaan kunci berbeda. *Polyalpabetic chiper* dibuat dari sejumlah *chiper* abjad-tunggal, masing-masing dengan kunci yang berbeda. Kebanyakan *chiper* abjad-majemuk adalah *chiper* substitusi periodik yang didasarkan pada periode *m*.
Misalkan plainteks *P* adalah

$$P = p_1 p_2 \ldots p_m p_{m+1} \ldots p_{2m} \ldots$$

maka chiperteks hasil enkripsi adalah

$$E_k(P) = f_1(p_1)\, f_2(p_2) \ldots f_m(p_m)\, f_{m+1}(p_{m+1}) \ldots f_{2m}(p_{2m}) \ldots$$

yang dalam hal ini p_i adalah huruf-huruf di dalam plainteks.

Untuk $m = 1$, *chiper*-nya ekivalen dengan *chiper* abjad-tunggal.

Salah satu *algoritma polialphabtic chiper* adalah *Vigenere Chiper* yang ditemukan oleh kriptologi Perancis, Blaise de Vigenere pada abad 16. Pada algoritma menggunakan string, misalkan *K* adalah deretan kunci

$$K = k_1\, k_2 \ldots k_m$$

yang dalam hal ini k_i untuk $1 \le i \le m$ menyatakan jumlah pergeseran pada huruf ke-*i*. Maka, karakter chiperteks $y_i(p)$ adalah

$$y_i(p) = (p + k_i) \bmod n$$

Misalkan periode $m = 5$, maka 5 karakter pertama dienkripsi dengan persamaan ini, dimana setiap karakter ke-*i* menggunakan kunci k_i. Untuk 20 karakter berikutnya, kembali menggunakan pola enkripsi yang sama. Sebagai contoh:

Plaintext : THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG
Kunci : FAIRUZ
Kemudian kunci diulang-ulang secara periodik, sehingga menjadi:

Plaintext : THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG
Kunci : FAI RUZFA IRUZF AIR UZFAI RUZF AIR UZFA IRU

Setiap huruf kunci kemudian dikonversi menjadi angka, dimana F=5, A=0, I=8, R=17 dan Z=25. Selanjutnya setiap huruf plaintext digeser sesuai dengan besaran huruf kunci yang bersesuain dengan plaintex tersebut, sehingga diperoleh hasil sebagai berikut.

Plaintext : THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG
Kunci : FAI RUZFA IRUZF AIR UZFAI RUZF AIR UZFA IRU
Chipertext: : YHM HOHHK JIIVS FWO DTRPA FPDW TPV FZEY LFA

Teknik Transposisi

Pada teknik transposisi huruf-huruf pada *plaintext* dan *chipertext* tetap sama, tetapi urutannya diubah. Dengan kata lain, teknik ini melakukan *transpose* terhadap rangkaian karakter di dalam teks. Nama lain untuk metode ini adalah **permutasi**, karena *transpose* setiap karakter di dalam teks sama dengan mempermutasikan karakter-karakter tersebut. Teknik transposisi memilki banyak varian algoritma diantaranya: *column transpotison chiper.* Untuk mempermudah pemahaman berikut ini contoh proses enkripsi *column transposition chiper* dengan *plaintext* sebagai berikut.

THEQUICKBROWNFOXJUMPSOVERTHELAZYDOG

Untuk mengenkripsi pesan, *plaintext* ditulis secara horizontal dengan lebar kolom tetap, misal selebar 6 karakter (kunci *k* = 6):

THEQUI
CKBROW
NFOXJU
MPSOVE
RTHELA
ZYDOGX

Penambahan karakter X merupakan tambahan sebagai persyaratan bahwa jumlah karakter merupakan kelipatan dari jumlah huruf kunci. Selanjuntnya *chipertext* dapat dibaca secara vertikal atau kolom per kolom, sehingga menjadi:

TCNMRZ HKFPTY EBOSHD QRXOEO UOJVLG IWUEAX

Untuk mendekripsi pesan, panjang chiperteks dibagi dengan kunci. Pada contoh ini, panjang *chipertext* yaitu 36 dibagi 6 untuk mendapatkan jumlah kolom yaitu 6.
Algoritma dekripsi identik dengan algoritma enkripsi. Jadi, untuk contoh ini, chiperteks dalam baris-baris selebar 6 karakter menjadi:

TCNMRZ
HKFPTY
EBOSHD
QRXOEO
UOJVLG
IWUEAX

Dengan membaca setiap kolom kita memperoleh pesan semula:

THEQUICKBROWNFOXJUMPSOVERTHELAZYDOG

HASIL PENELITIAN

Shift Chiper

Dalam implementasi menggunakan Delphi *plaintext* diubah menjadi kode ASCII menggunakan fungsi Ord. Dalam proses enkripsinya setiap nilai ordinal huruf *plaintext* dikurangkan dengan angka 65, ditambahkan dengan nilai kunci, dan kemudian di modulo 26. Berikut ini kode program untuk proses enkripsinya.

```
For i:= 1 to n do
begin
  P:=ord(plaintext[i])-65;
  C:=(P + K) mod 26;
  chipertext:=chipertext+ chr(C+65)
end;
```

Proses deskripsi dilakukan dengan mengurangkan nilai ordinal huruf chipertex dengan angka 65, kemudian dikurangi dengan nilai kuncinya. Jika nilai hasil dekripsi bernilai negatif maka nilai tersebut ditambah 26. Untuk menampilkan *plaintext* ke dalam bentuk abjad maka ditambahkan dengan 65. Kode program dekripsinya sebagai berikut.

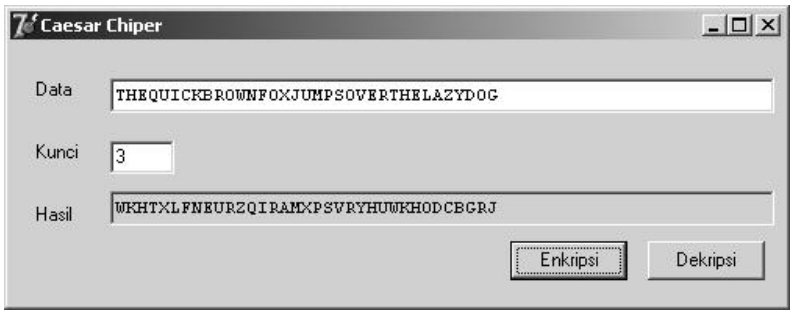
```
For i:= 1 to n do
  begin
    C:=ord(chipertext[i])-65;
    P:= (C-K);
    if p<0 then p:=26+p;
    Plaintext:=Plaintext+ chr(p+65);
  end;
```

Kode program shift chiper secara lengkap sebagai berikut.

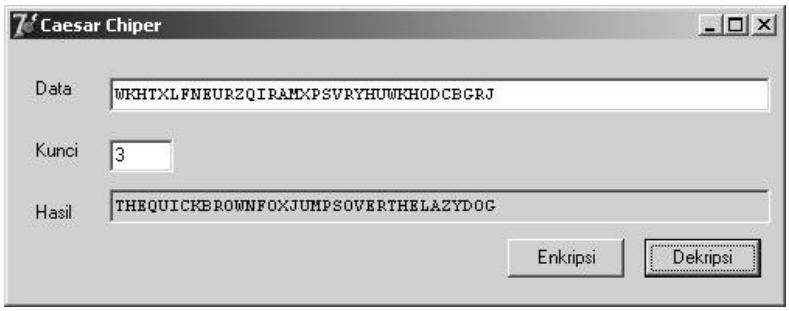
```
procedure TfrmCaesarChiper.btnEnkripsiClick(Sender: TObject);
Var Plaintext, Chipertext : string;
  P,C,K, i, n : integer;
begin
  Plaintext:= UpperCase(eData.Text);
  K:=StrToInt(eKunci.Text);
  n := Length(Plaintext);
  Chipertext:='';
  For i:= 1 to n do
  begin
    P:=ord(plaintext[i])-65;
    C:=(P + K) mod 26;
    chipertext:=chipertext+ chr(C+65)
  end;
  eHasil.Text := Chipertext;
end;

procedure TfrmCaesarChiper.bDekripsiClick(Sender: TObject);
Var Plaintext, Chipertext : string;
  P,C,K, i, n : integer;
```

```
begin
   Chipertext:= UpperCase(eData.Text);
   K:=StrToInt(eKunci.Text);
   n := Length(Chipertext);
   Plaintext:='';
   For i:= 1 to n do
   begin
     C:=ord(chipertext[i])-65;
     P:= (C-K);
     if p<0 then p:=26+p;
     Plaintext:=Plaintext+ chr(p+65);
   end;
   eHasil.Text := Plaintext;
end;
```

Berikut ini tampilan ujicoba enkripsi dan dekripsi untuk program Caesar Chiper.



Gambar 3. Form Proses Enkripsi Caesar Chiper



Gambar 4. Form Proses Dekripsi Caesar Chiper

Monoalphabetic Chiper

. Langkah awal dalam algoritma *monoalphabetik* chiper adalah menyederhanakan kunci yang berupa string, dengan cara mengeliminasi huruf yang kemunculannya ganda. Proses penyederhanaan diimplementasikan sebagai berikut.

```
plain :='ABCDEFGHIJKLMNOPQRSTUVWXYZ';
for i:=1 to length(kunci) do
```

```
if pos(kunci[i],chiper)=0 then chiper:=chiper+kunci[i];
```

Huruf-huruf selain kunci kemudian ditambahkan dibelakang huruf-huruf kunci sehingga membentuk deretan huruf subtitusi (*chiper alphabet*) yang lengkap. Berikut ini kode pembentukan *chiper alpabhet*-nya

```
for i:=1 to 26 do
   if pos(plain[i],chiper)=0 then chiper:=chiper+plain[i];
```

Dengan kedua blok perintah tersebut maka terbentuk tabel *plain alphabet* dan *chiper alphabet*. Berdasarkan tabel yang terbentuk kemudian digunakan untuk proses enkripsi dan dekripsi. Berikut ini kode program untuk proses enkripsinya.

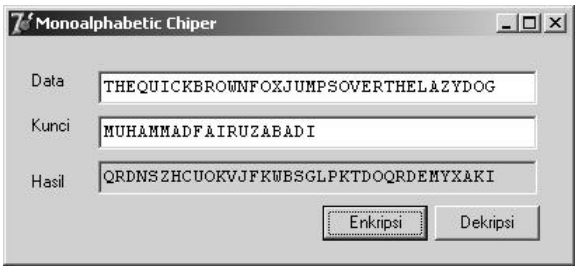
```
chipertext :=”;
for i:=1 to n do
   chipertext:= chipertext + chiper[pos(plaintext[i],plain)];
```

Adapun kode programnya secara lengkap sebagai berikut.

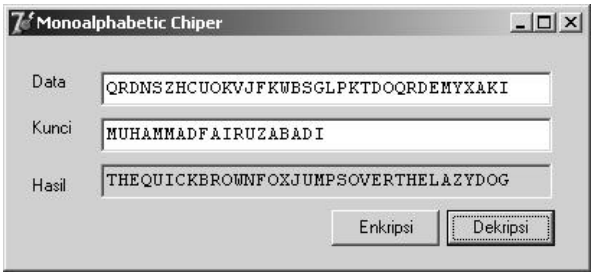
```
procedure TfrmMonoalphabetikChiper.btnEnkripsiClick(Sender: TObject);
var plain,plaintext, kunci,chiper, chipertext:string;
  i,n:byte;

begin
  plaintext:=edata.Text;
  n:=length(plaintext);
  plain :=’ABCDEFGHIJKLMNOPQRSTUVWXYZ’;
  Kunci := eKunci.Text;
  chiper:=”;
  for i:=1 to length(kunci) do
    if pos(kunci[i],chiper)=0 then chiper:=chiper+kunci[i];
  for i:=1 to 26 do
     if pos(plain[i],chiper)=0 then chiper:=chiper+plain[i];
  chipertext :=”;
  for i:=1 to n do
    chipertext:= chipertext + chiper[pos(plaintext[i],plain)];
  ehasil.Text := chipertext;
  end;

procedure TfrmMonoalphabetikChiper.btnDekripsiClick(Sender: TObject);
var plain,plaintext, kunci,chiper, chipertext:string;
  i,n:byte;

begin
  chipertext:=edata.Text;
  n:=length(chipertext);
  plain :=’ABCDEFGHIJKLMNOPQRSTUVWXYZ’;
  Kunci := eKunci.Text;
  chiper:=”;
  for i:=1 to length(kunci) do
    if pos(kunci[i],chiper)=0 then chiper:=chiper+kunci[i];
```

```
  for i:=1 to 26 do
     if pos(plain[i],chiper)=0 then chiper:=chiper+plain[i];
  plaintext :='';
  for i:=1 to n do
    plaintext:= plaintext + plain[pos(chipertext[i],chiper)];
  ehasil.Text := plaintext;
  end;
end.
```

Tampilan ujicoba enkripsi dan dekripsi program Caesar Chiper dapat dilihat pada gambar 5 dan gambar 6.



Gambar 5. Form Proses Enkripsi Monoalphabetic Chiper



Gambar 6. Form Proses Enkripsi Monoalphabetic Chiper

Polyalphabetic Chiper

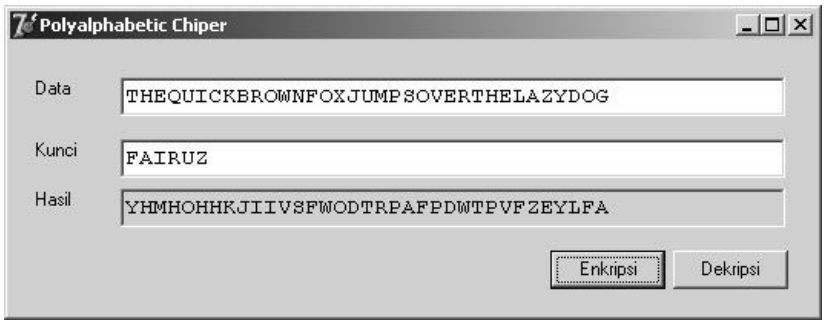
Proses awal dalam pada *polialphabetic chiper* adalah pembentukan kunci dengan mengulang-mengulang string kunci secara periodik sesuai panjang dari plaintext. Berikut ini implementasinya dalam Borland Delphi.

```
for i:=1 to n do begin
  if i mod nk =0 then
     Ki:=ord(k[nk])-65
  else
     Ki:=ord(k[i mod nk])-65;
```

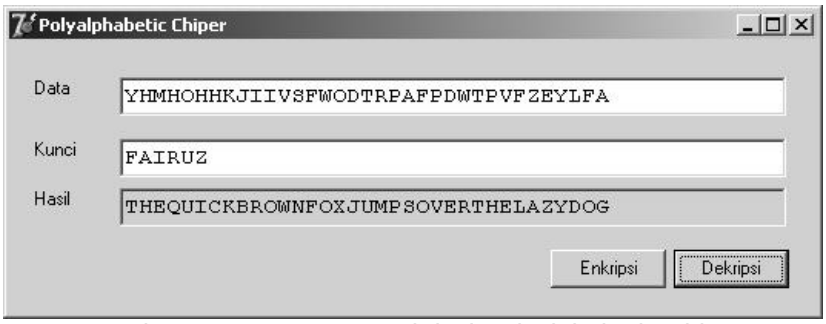
Sedangkan proses enkripsi atau dekripsi mirip dengan *shift chiper,* hanya saja kuncinya menggunakan setiap huruf dari string kunci secara periodik. Berikut ini kode program *polialphabetic chiper* secara lengkap.

```
procedure TfrmPolyalphabeticChiper.btnEnkripsiClick(Sender: TObject);
var plaintext, K, chipertext :string;
    pi, ci, i, ki, n, nK:Integer;

begin
   plaintext:=uppercase(edata.Text);
   n:=length(plaintext);
   K := uppercase(eKunci.Text);
   nK :=length(K);
   chipertext :='';
   for i:=1 to n do begin
     if i mod nk =0 then
        Ki:=ord(k[nk])-65
     else
        Ki:=ord(k[i mod nk])-65;
     Pi:=ord(Plaintext[i])-65;
     Ci:=(Ki+Pi) mod 26;
     chipertext:= chipertext+ chr(ci+65);
   end;
   ehasil.Text := chipertext;
end;

procedure TfrmPolyalphabeticChiper.btnDekripsiClick(Sender: TObject);
var plaintext, K, chipertext :string;
    pi, ci, i, ki, n, nK:Integer;

begin
   chipertext:=uppercase(edata.Text);
   n:=length(chipertext);
   K := uppercase(eKunci.Text);
   nK :=length(K);
   plaintext :='';
   for i:=1 to n do begin
     if i mod nk =0 then
        Ki:=ord(k[nk])-65
     else
       Ki:=ord(k[i mod nk])-65;
     Ci:=ord(Chipertext[i])-65;
     Pi:=(Ci-Ki);
     if Pi < 0 then Pi:= 26+Pi;
     plaintext:= plaintext+ chr(pi+65);
   end;
   ehasil.Text := plaintext;
end;
```

Tampilan uji coba program *polyalphabetic chiper*, baik enkripsi dan dekripsi dapat dilihat pada Gambar 7 dan 8.



Gambar 7. Form Proses Enkripsi *Polyalphabetic Chiper*



Gambar 8. Form Proses Dekripsi *Polyalphabetic Chiper*

Column Transposition Chiper

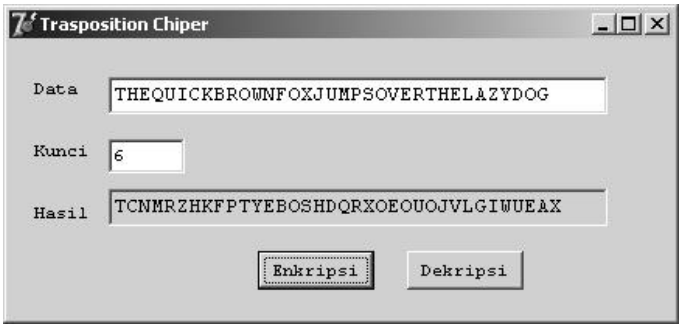
Langkah awal dari proses *column transpotition chiper* adalah membagi plaintex ke dalam baris-baris dengan jumlah kolom sebanyak jumlah kunci. Pada langkah ini ditambahkan pula karakter tambahan, misalnya “X” jika jumlah huruf *plaintext* bukan kelipatan dari kunci. Berikut kode program pembentukan baris tersebut.

```
   if n mod k <> 0 then
   for i:=1 to k - n mod k  do
     plaintext:=plaintext+'X';
   chipertext:=plaintext;
    n := Length(Plaintext);
```

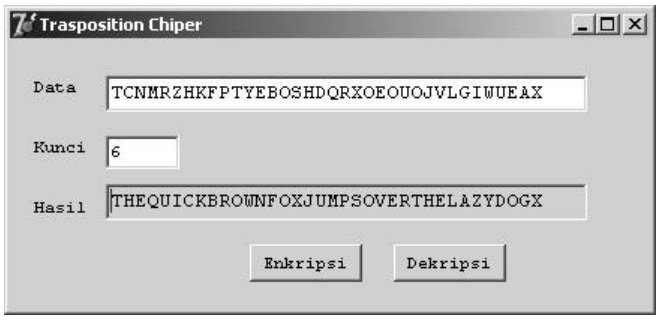
Selanjutnya, dilakukan pembacaan baris-perbaris untuk membentuk chipertexnya. Berikut ini kode program selengkapnya dari *Column Transposition Chiper*

```
procedure TfrmTranpositionchiper.btnEnkripsiClick(Sender: TObject);
var Plaintext, Chipertext : string;
   a,j,P,C,K, i, n : integer;

begin
   Plaintext:= UpperCase(eData.Text);
   K:=StrToInt(eKunci.Text);
   n := Length(Plaintext);
   if n mod k <> 0 then
```

```
   for i:=1 to k - n mod k  do
     plaintext:=plaintext+'X';
   chipertext:=plaintext;
    n := Length(Plaintext);
      a:=0;
      for j:=0 to k-1 do
        For i:= 1 to n div k  do
            begin
             a:=a+1;
              chipertext[a]:=plaintext[(i-1)*k+1+j];
            end ;
         eHasil.Text := chipertext;
end;

procedure TfrmTranpositionchiper.btnDekripsiClick(Sender: TObject);
var Plaintext, Chipertext : string;
   a,j,P,C,K, i, n : integer;
begin
    Chipertext:= UpperCase(eData.Text);
   K:=StrToInt(eKunci.Text);
   n := Length(Chipertext);
   if n mod k <> 0 then
   for i:=1 to k - n mod k  do
     Chipertext:=Chipertext+'X';
   Plaintext:=Chipertext;
    n := Length(Chipertext);
   k:=strtoint(ekunci.text);
  a:=0;
 For i:= 0 to n div k -1 do
 for j:=1 to k do

       begin
         a:=a+1;
         Plaintext[a]:=Chipertext[(j-1)* n div k + 1+i];
       end ;
   eHasil.Text := plaintext;
end;
```



Gambar 9. Form Proses Enkripsi *Column Transpotition Chiper*



Gambar 10. Form Proses Dekripsi *Column Transpotition Chiper*

KESIMPULAN

Kriptografi klasik adalah cara penyamaran berita yang dilakukan oleh orang-orang dulu ketika belum ada komputer. Tujuannya adalah untuk melindungi informasi dengan cara melakukan penyandian. Penyandian dilakukan secara manual. Caranya adalah dengan cara transposisi dan substitusi huruf. Pada penggunaan transposisi, posisi huruf diubah-ubah, sementara pada substitusi, huruf digantikan dengan huruf atau simbol lain sehingga informasi sulit dibaca dan dikenali karena tampak diacak-acak. Pada tulisan ini dilengkapi berbagai contoh implementasi kriptografi klasik menggunakan Borland Delphi, seperti: *Shift Chiper, Monoalphabetic Chiper, Polyalphabetic Chiper* dan *Column Transpotition Chiper*. Secara teknis, kriptografi klasik cukup mudah diimplementasikan menggunakan Borland Delphi dengan adanya beberapa fitur pendukung, seperti:

- Prosedur dan fungsi string bawaan yang relatif lengkap,
- tipe string yang setiap karakternya dapat diakses berdasarkan indeks sehingga terkesan sebagai *array of char*,
- Operator dan fungsi aritmetik yang membantu dalam komputasional proses enkripsidan dekripsi

Diharapkan implementasi kriptografi klasik menggunakan Borland Delphi ini dapat lebih mengenalkan tentang konsep, dasar-dasar dan implementasi kriptografi sehingga kedepan akan lebih mudah memahami implementasi kriptografi modern.

DAFTAR PUSTAKA

Jack Febrian, *Pengetahuan Komputer dan Teknologi Informasi*. Informatika Bandung, 2004

Kahn, D. The Codebreakers: *The Story of secret writing*. New York:Scribner, 1996

A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

Schn96 Bruce Schneier, *Applied Cryptography, Protocols, Algorithms, and Source Code n C*. John Wiley & Sons. Inc. 1996

Willam Stallings, *Cryptography and Network Security, Principles and Practices*. Pearson Prentice Hall, 2003