Praktikum 1
Kriptografi Substitusi

Materi :

Metode Kriptografi : *Caesar, Monoalfabetik, Vegenere*

Tujuan :

Dalam praktikum ini mahasiswa akan mengimplementasikan dan menjalankan metode kriptografii : Caesar cipher dan Monoalfabetik cipher serta mengem-bangkannya. Setelah praktikum mahasiswa diharapkan dapat :

1. memahami dan menjelaskan metode kriptografi Caesar dan Monoalfabetik
2. dapat menggunakan / menerapkan metode-metode tersebut dalam aplikasi.

Tools :

1. Disediakan contoh implementasi dan *source code*-nya
2. Dalam implementasi ini tidak bergantung pada bahasa pemrograman yang disediakan, Sehingga implementasi tidak dibatasi pada *source code* dan software yang disediakan yaitu menggunakan Delphi

Teori :

A. Caecar Cipher

Metode ini menggunakan penggeseran sederhana, algoritma dasar dari metode ini sangat simple, setiap kunci diganti dengan huruf ketiga setelah kunci yang bersangkutan.

misalnya kita miliki *plaintext* seperti berikut :

```
I CAME I SAW I CONQUERED
```

maka kalau kita enkripsikan dengan metode ini, didapatkan cipherteksnya :

```
L FDPH L VDZ L FRQTXHUHG
```

atau secara umum substitusi tersebut dapat digambarkan seperti berikut :

```
Plain      : ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

Cipher : DEFGHIJKLMNOPQRSTUVWXYZABC

Secara Umum Caecar Cipher dapat didefinisikan

Jika A suatu nilai ke 0, B 1, C 2,…Y24 dan Z 25

Maka enkripsi dapat dikodekan dengan

E_k:i → i+k (mod 26)

Dan dekripsi

D_k:i → i-k (mod 26)

Walaupun dalam algoritma ini setiap kunci disubstitusi / digantikan oleh kunci ke-3 setelah kunci yang bersangkutan, namun setiap algoritma enkripsi yang dilakukan dengan mengganti kunci ke-x dengan kunci ke-x+n (baik nilai n positif maupun negatif) termasuk atau dapat digolongkan dalam metode enkripsi Caecar cipher.

B. Monoalfabetik

Pada dasarnya metode ini terdiri dari 3 jenis, yang mempunyai hampir sama yaitu : Mixed Monoalfabetik, Easier Monoalfabetik dan General Monoalfabetik.

1. Mixed Monoalfabetik

   Dalam metode ini setiap kunci dapat disubstitusi dengan sembarang kunci secara acak dalam batasan 26 huruf dalam alphabet.

   contoh :

   Plain : ABCDEFGHIJKLMNOPQRSTUVWXYZ

   Cipher : DKVQFIBJWPESCXHTMYAUOLRGZN

   maka jika dilakukan enkripsi dengan metode tersebut

   Plainteks : IF WE WISH TO REPLACE LETTERS

   cipherteks : WI RF RWAJ UH FYTSDVF SFUUFYA

2. Easier Monoalfabetik

   Dalam mixed monoalphabetic kata kunci ditentukan sebanyak 26 huruf yang acak, tentu saja sederet kata kunci 26 huruf tersebut sulit untuk dihafal urutannya, maka dalam easier ini kata kunci (*keyword*) hanya menggunakan suatu kata atau sekelompok kata, kemudian dihilangkan / dihapus huruf yang sama dalam kata

kunci tersebut dan kemudian untuk huruf berikutnya diteruskan dengan huruf terakhir dalam kata kunci tersebut dan seterusnya secara urut dalam 26 alphabet.

Contoh

Diberikan kata kunci : SISTEM BERKAS

Plain : ABCDEFGHIJKLMNOPQRSTUVWXYZ

cipher : SITEMBRKACDFGHJLNOPQUVWXYZ

maka jika dengan metode tersebut dilakukan enkripsi

Plainteks : TEKNOLOGI INDUSTRI

cipherteks : QMDHJFJRA AHEUPQOA

3. General Monoalfabetik

Perbedaan dengan *easier,* pada *general* spesifikasi enkripsi ditentukan oleh perulangan pada posisi kolom yang bersesuain dengan jumlah alphabet yang berbeda dalam kata kunci.

Contoh

Diberikan suatu kata kunci : STARWARS

Maka alphabet yang sama dihapus : STARW

Lakukan dengan pengulangan kolom untuk huruf lain dalam 26 alphabet :

```
STARW
BCDEF
GHIJK
LMNOP
QUVXY
Z
```

Kemudian dibaca secara kolom, maka didapatkan translasi seperti berikut

Plain : ABCDEFGHIJKLMNOPQRSTUVWXYZ

cipher : SBGLQZTCHMUADINVREJOXWFKPY

maka jika digunakan untuk melakukan enkripsi / dekripsi :

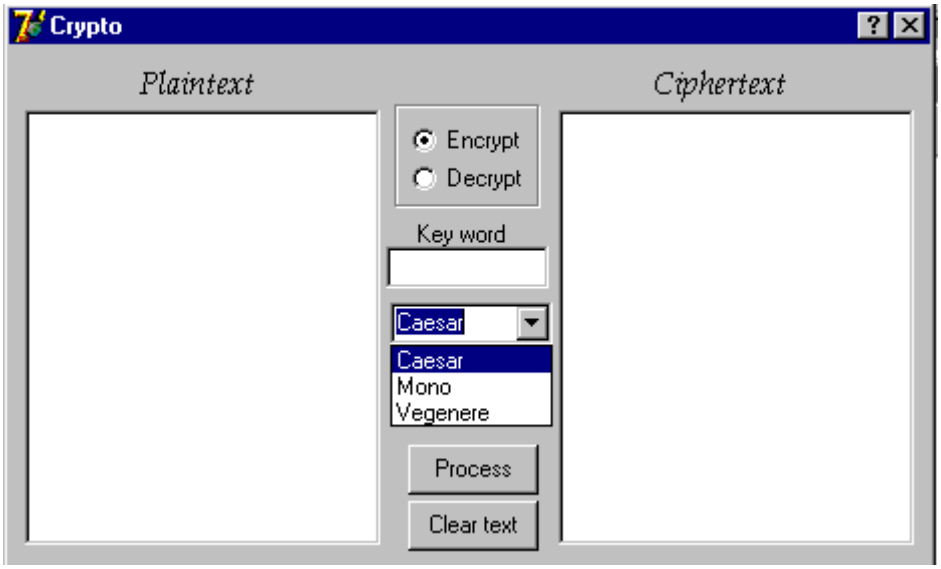
Plain : I KNOW ONLY THAT I KNOW NOTHING

cipher : H UINF NIAP OCSO H UINF INOCHIT

Contoh :

Contoh implementasi ini menggunakan delphi dan bukan merupakan batasan

1. User interface



2. Source code

```
Function Caesar(x:string; k: string):string;
var i : integer;
    tx: string;
Begin
     tx:='';
     For i:=1 to length(x) do
       tx:=tx+chr(ord(x[i])+ 5);
     Caesar:=tx;
end;

procedure TForm1.Button1Click(Sender: TObject);
var i : integer;
begin
    If Radiogroup1.ItemIndex=0 then Begin
    i:=combobox1.ItemIndex;
    Case i of
      0 : memo2.Lines.Text:=caesar(memo1.Lines.Text,
             edit1.Text);
      1 : Messagebox(Handle,'Sory! Under Construction !',
            'Info',MB_OK or MB_ICONINFORMATION);
      2 : If edit1.Text='' then Messagebox(Handle,
          'Harus ada kata kunci','Info',MB_OK or
            MB_ICONINFORMATION)
          Else
```

```
            memo2.Lines.Text:=vegenere(memo1.Lines.Text,
              edit1.Text);
    end; end
    Else If Radiogroup1.ItemIndex=1 then Begin
    i:=combobox1.ItemIndex;
    Case i of
      0 : memo2.Lines.Text:=Dcaesar(memo1.Lines.Text,
            edit1.Text);
      1 : Messagebox(Handle,'Sory! Under Construction !',
          'Info',MB_OK or MB_ICONINFORMATION);
      2 : If edit1.Text='' then Messagebox(Handle,
          'Harus ada kata kunci','Info',MB_OK or
            MB_ICONINFORMATION)
          Else
            memo2.Lines.Text:=Dvegenere(memo1.Lines.Text,
              edit1.Text);
    end;
    end
    Else Messagebox(Handle,'Process Encrypt or Decrypt!',
          'Info',MB_OK or MB_ICONINFORMATION)
end;

procedure TForm1.Button2Click(Sender: TObject);
begin
   Memo2.Lines.Clear;
   Memo1.Lines.Clear;
   Form1.Refresh;
end;
```

TUGAS :

1. Dalam source code tersebut belum ada Fungsi `Dekripsi` untuk `Caesar`, untuk itu buatlah kedua fungsi tersebut dengan nama `Dcaesar`. Jika telah jalan tuliskan !

   .....

   .....

   .....

   .....

   .....

   .....

   .....

2. Dalam aplikasi tersebut belum ada proses Enkripsi maupun dekripsi dengan metode `Monoalfabetik (Mixed,Easier,General)` untuk itu buatlah Fungsi `enkrip` dan `dekrip` salah satu dari 3 metode monoalfabetik