Praktikum 2
Kriptografi Substitusi

A. Vegenere

Metode ini sebagai bentuk pengembangan dari metode monoalphabethic. Metode ini juga merupakan dasar dari polyalphabetic substitution cipher.

Beberapa ketentuan dalam dalam metode ini antara lain :

- ✓ setiap kunci dapat disubstitusi dengan bermacam-macam kunci yang lain
- ✓ menggunakan kata kunci
- ✓ Kata kunci digunakan secara berulang
- ✓ Kata kunci digunakan untuk menentukan enkrispsi setiap alphabet dalam plainteks
- ✓ Huruf ke-i dalam plainteks di spesifikasikan oleh alphabet yang digunakan dalam kunci
- ✓ Penggunaan alphabet bisa berulang

Contoh

Plaintext : THISPROCESSCANALSOBEEXPRESSED

Kunci : CIPHERCIPHERCIPHERCIPHERCIPHE

Ciphertext

```
     ABCDEFGHIJKLMNOPQRSTUVWXYZ
C →  CDEFGHIJKLMNOPQRSTUVWXYZAB
I →  IJKLMNOPQRSTUVWXYZABCDEFGH
P →  PQRSTUVWXYZABCDEFGHIJKLMNO
H →  HIJKLMNOPQRSTUVWXYZABCDEFG
E →  EFGHIJKLMNOPQRSTUVWXYZABCD
R →  RSTUVWXYZABCDEFGHIJKLMNOPQ
```

Maka hasil enkripsinya adalah :

```
T berdasarkan kunci C disubstitusi dengan  V
H                   I                      P
I                   P                      X
S                   H                      Z
P                   E                      T
R                   R                      I
O                   C                      Q
S                   I                      K
```

dst

sehingga hasil enkripsi akhirnya adalah :

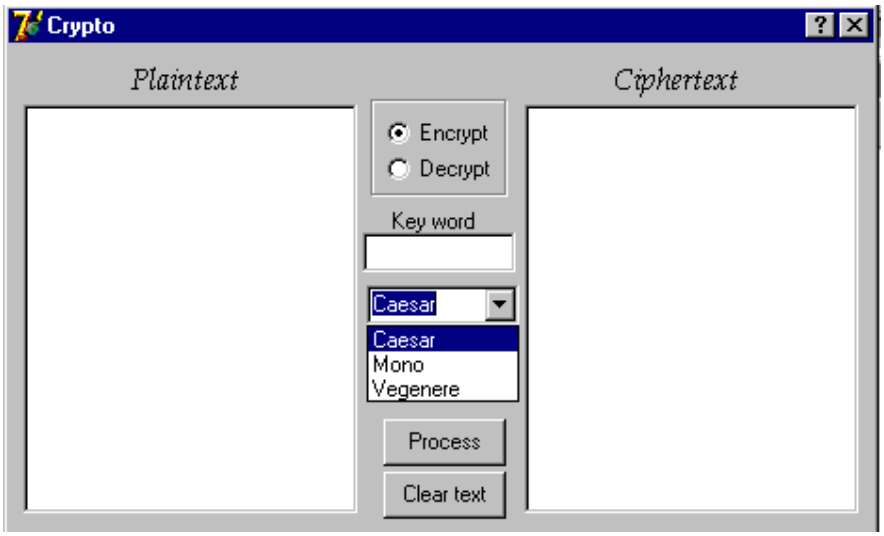
Plaintext : THIS PROCESS CAN ALSO BE EXPRESSED

Ciphertext : VPXZ TIQKTZW TCV PSWF DM TETIGAHLH

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;

Function vegenere(x:string; k: string):string;
var i : integer;
    tamp: byte;
    tx: string;
Begin
  tx:='';
  For i :=1 to length(x)do begin
    tamp:=ord(k[(i mod length(k))+1])-66;
    tx := tx + chr((ord(x[i])+ tamp) MOD 256);
    end;
```

```
  vegenere:=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 `Vegenere`, untuk itu buatlah fungsi tersebut dengan nama `Dvegenere`. Jika telah jalan tuliskan !