Tutorial Kriptografi Klasik dan Penerapannya dalam Visual Basic .NET

Husni Fahmi
fahmi@inn.bppt.go.id

Haret Faidah
haret@inn.bppt.go.id

Kemajuan teknologi di bidang komputer memungkinkan ribuan orang dan komputer di seluruh dunia terhubung dalam satu dunia maya yang dikenal sebagai *cyberspace* atau Internet. Begitu juga ratusan organisasi seperti perusahaan, lembaga negara, lembaga keuangan, militer dan sebagainya.Tetapi sayangnya, kemajuan teknologi selalu diikuti dengan sisi buruk dari teknologi itu sendiri. Salah satunya adalah rawannya keamanan data sehingga menimbulkan tantangan dan tuntutan akan tersedianya suatu sistem pengamanan data yang sama canggihnya dengan kemajuan teknologi komputer itu sendiri. Ini adalah latar belakang berkembangnya sistem keamanan data untuk melindungi data yang ditransmisikan melalui suatu jaringan komunikasi. Ada beberapa cara melakukan pengamanan data yang melalui suatu saluran, salah satu diantaranya adalah kriptografi. Dalam kriptografi, data yang dikirimkan melalui jaringan akan disamarkan sedemikian rupa sehingga kalaupun data itu bisa dibaca maka tidak bisa dimengerti oleh pihak yang tidak berhak. Data yang akan dikirimkan dan belum mengalami penyandian dikenal dengan isitilah *plaintext*, dan setelah disamarkan dengan suatu cara penyandian, maka plaintext ini akan berubah menjadi *ciphertext*.

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. Kata kriptografi sendiri berasal dari bahasa Yunani, yaitu *kryptós* yang berarti tersembunyi, dan *gráphein* yang berarti menulis. Jadi Kriptografi berarti penulisan rahasia. Ada dua cara yang paling dasar pada kriptografi klasik. Yang pertama adalah transposisi. Transposisi adalah mengubah susunan huruf pada plaintext sehingga urutannya berubah. Contoh yang paling sederhana adalah mengubah suatu kalimat dengan menuliskan setiap kata secara terbalik.

```
Plaintext:    IBU AKAN DATANG BESOK PAGI
Ciphertext:   UBI NAKA GNATAD KOSEB IGAP
```

Gambar 1. Contoh transposisi (menuliskan setiap kata secara terbalik)

Contoh transposisi yang sedikit lebih sulit adalah plaintext yang disusun dalam kelompok huruf yang terdiri dari beberapa kolom huruf, misalnya 5 kolom huruf :

```
IBUAK
ANDAT
ANGBE
SOKPA
GIAAA
```

Gambar 2. Plaintext disusun dalam 5 kolom huruf

kemudian dituliskan per kolom, dengan urutan kolom yang bisa berubah-ubah.

```
IAASGBNNOIUDGKAAABPAKTEAA
```

Gambar 3. Kolom huruf dituliskan berurutan dari kolom 1,2,3,4,5

```
UDGKAKTEAAAABPAAIAASGBNNOI
```

Gambar 4. Kolom huruf dituliskan dengan urutan kolom 3,5,4,1,2

Untuk melengkapi kolom terakhir agar berisi 5 huruf, maka sisanya diisi dengan huruf 'A' atau bisa huruf apa saja , sebagai huruf pelengkap.

Cara kedua adalah cara substitusi yaitu setiap huruf pada plaintext akan digantikan dengan huruf lain berdasarkan suatu cara atau rumus tertentu. Ada dua macam substitusi yaitu *polyalphabetic substitution cipher* dan *monoalphabetic substitution cipher*. Pada polyalphabetic substitution cipher, enkripsi terhadap satu huruf yang sama bisa menghasilkan huruf yang berbeda sehingga lebih sulit untuk menemukan pola enkripsinya. Pada monoalphabetic substitution cipher maka satu huruf tertentu pasti akan berubah menjadi huruf tertentu yang lain, sehingga pola enkripsinya lebih mudah diketahui, karena satu huruf pada ciphertext pasti merepresentasikan satu huruf pada plaintext.

Salah satu contoh cara substitusi adalah dengan dengan pergeseran huruf. Kita lihat pada gambar 4, urutan abjad ABCD…….Z bisa digeser sebanyak 1 huruf sehingga huruf A akan menjadi B, B akan menjadi C dan seterusnya. Pergeserannya bisa dibuat lebih banyak yaitu 2 huruf sehingga huruf A akan menjadi C, B akan menjadi D dan seterusnya. Pergeseran bisa lebih banyak lagi tergantung bagaimana kita merumuskannya. Cara pergeseran ini termasuk monoalphabetic substitution cipher di mana satu huruf pasti akan berubah menjadi huruf tertentu yang lain. Karena relasi antara huruf plaintext dan huruf ciphertext satu-satu, yang artinya suatu huruf plaintext pasti menjadi suatu huruf ciphertext tertentu, maka cara monoalphabetic substitution cipher sangat mudah dipecahkan.

```
Urutan Abjad          : ABCDEFGHIJKLMNOPQRSTUVWXYZ
Pergeseran 1 huruf    : BCDEFGHIJKLMNOPQRSTUVWXYZA
Pergeseran 2 huruf    : CDEFGHIJKLMNOPQRSTUVWXYZAB
```

Gambar 5. Substitusi dengan menggeser 1 huruf atau 2 huruf

Dengan menggunakan pergeseran 2 huruf, maka plaintext berikut akan berubah menjadi:

```
Plaintext :   IBU AKAN DATANG BESOK PAGI
Ciphertext:   KDW CMCP FCVCPI DGUQM RCIK
```

Gambar 6. Substitusi dengan pergeseran 2 huruf

Pada masa itu, sekitar tahun 1500-an atau 1600-an, kriptografi klasik seperti ini dianggap sudah cukup aman, karena belum banyak orang yang bisa menulis atau membaca. Kriptografi dilakukan terhadap huruf-huruf yang membentuk plaintext, mengubahnya dalam huruf lain kemudian dikirimkan ke pada penerimanya. Penerima harus mengetahui cara menyamarkan berita agar bisa mendapatkan berita aslinya kembali.

Artikel tentang kriptografi klasik ini dibuat sebagai pengenalan terhadap kriptografi yang akan dipublikasikan pada artikel berikutnya yaitu kriptografi modern. Kriptografi modern banyak digunakan dalam pengiriman informasi melalui Internet. Kriptografi modern berkembang bersamaan dengan berkembangnya teknologi komputer dan teknologi jaringan. Seperti sudah dikatakan sebelumnya, pada kriptografi klasik, dua cara digunakan yaitu transposisi dan substitusi. Pada kriptografi modern, digunakan algoritma matematika yang juga pada akhirnya akan menyebabkan terjadinya transposisi dan substitusi pada plaintext sama seperti pada kriptografi klasik.. Hanya bedanya, transposisi dan substitusi huruf pada kriptografi modern dilakukan dengan bantuan komputer menggunakan algoritma matematika yang cukup rumit. Prinsip dasar dari kedua kriptografi sama yaitu melakukan transposisi dan substitusi pada huruf-huruf plaintextnya untuk menghasilkan suatu ciphertext.

Di bawah ini ada beberapa contoh kriptografi klasik.

1. Kriptografi Caesar

Salah satu kriptografi yang paling tua dan paling sederhana adalah kriptogtafi Caesar [KAHN96]. Menurut sejarah, ini adalah cara Julius Caesar mengirimkan surat cinta kepada kekasihnya Cleopatra. Dalam kriptografi Caesar, maka setiap huruf akan dituliskan dalam huruf lain hasil pergeseran 3 buah huruf. Kriptografi Caesar ini adalah kriptografi substitusi karena setiap huruf akan digantikan huruf lain.

Sebagai contoh, huruf A akan digeser 3 huruf menjadi huruf D, B akan digeser 3 huruf menjadi E, J akan digeser menjadi M, O akan menjadi R dan seterusnya. Pergeseran ini juga berputar kembali ke awal abjad sehingga sesudah huruf Z diikuti kembali oleh huruf A. Kriptografi Caesar ini dikenal sebagai monoalphabetic substitution cipher karena satu huruf tertentu pasti akan berubah menjadi huruf tertentu yang lain.

Perubahan pada kriptografi Caesar bisa dituliskan sebagai berikut:

```
Plaintext    :    ABCDEFGHIJKLMNOPQRSTUVWXYZ
Ciphertext   :    DEFGHIJKLMNOPQRSTUVWXYZABC

Plaintext    :    KITA JUMPA BESOK PAGI
Ciphertext   :    NLWD MXPSD EHVRN SDJL
```

Gambar 7. Contoh Kriptografi Caesar

Jika Caesar akan menuliskan kalimat ‘I LOVE YOU’ maka akan dituliskan dalam kalimat ‘L ORYH BRX‘.

Jika kita memberi nomor ke pada huruf-huruf abjad dan kita mulai dengan huruf A=0, B=1, C=2 dstnya sampai dengan Z=25, maka kriptografi Caesar memenuhi rumus sebagai berikut :

$$C = (P + 3) \bmod 26,$$

di mana C adalah nomor abjad ciphertext, P adalah nomor abjad plaintext .

Dan dekripsinya adalah

$$P = (C - 3) \bmod 26.$$

Kripotogtafi Caesar ini kemudian berkembang di mana pergeseran tidak hanya 3 huruf tetapi ditentukan oleh suatu kunci yang adalah suatu huruf. Huruf ini yang menentukan pergeseran dari huruf pada plaintext. Jika kunci adalah A maka pergeseran adalah 0, B pergeseran adalah 1, C 2 dan seterusnya. Rumus di atas tetap berlaku tetapi pergeseran huruf ditentukan oleh nilai pergeseran k (lihat tabel 1) dan bisa berubah-ubah sesuai kunci yang digunakan.

Tabel 1. Tabel pergeseran huruf pada kriptografi Caesar

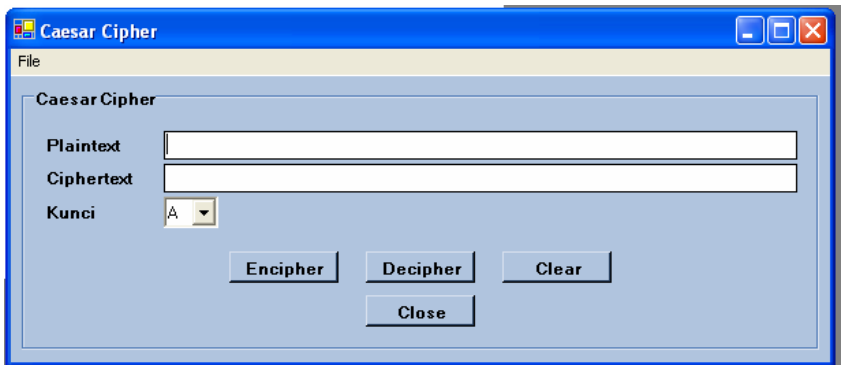
Kunci	A	B	C	D	E	F	G	H	I
Pergeseran k	0	1	2	3	4	5	6	7	8
Kunci	J	K	L	M	N	O	P	Q	R
Pergeseran k	9	10	11	12	13	14	15	16	17
Kunci	S	T	U	V	W	X	Y	Z	
Pergeseran k	18	19	20	21	22	23	24	25	

Rumus kriptografi Caesar, secara umum bisa dituliskan sebagai berikut:

$$C = E(P) = (P + k) \bmod 26$$
$$P = D(C) = (C - k) \bmod 26$$

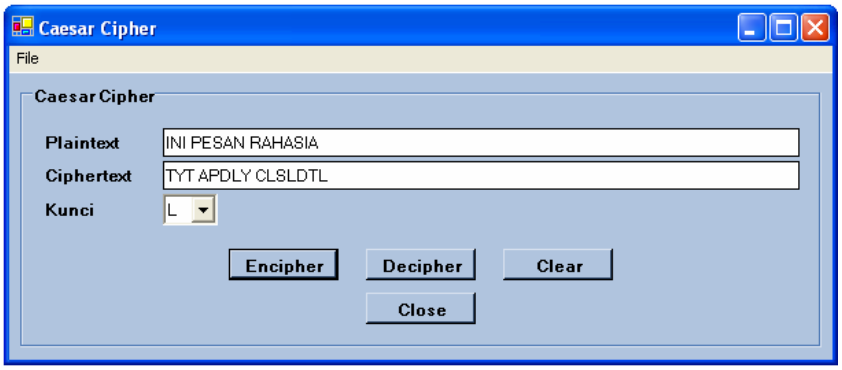
di mana P adalah plaintext, C adalah ciphertext, k adalah pergeseran huruf sesuai dengan kunci yang dikehendaki.

Berikut ini implementasi kriptografi Caesar dalam Visual Basic .NET. Setelah program ini dijalankan, maka akan terlihat menu sebagai berikut :



Gambar 8. Menu Kriptografi Caesar

Masukkan kalimat yang ingin dienkripsi, dan masukkan kunci yang dikehendaki, misalnya kalimat: INI PESAN RAHASIA dengan kunci L. Klik tombol Encipher dan lihat ciphertext yang muncul. Ulangi dengan kalimat dan kunci yang lain. Cobalah juga dengan deksripsi.



Gambar 9. Menu Kriptografi Caesar setelah Plaintext dan Kunci diisi kemudian tombol Encipher diklik

Kode Sumber:

```
Private Function CaesarEncipher(ByVal strPlaintext As String, ByVal nShift As Integer) As String
   Dim i As Long
   Dim c As Integer
   Dim pAlphabet As Integer
   Dim cAlphabet As Integer
   Dim s As String = ""

   'Masing-masing huruf digeser nShift
   For i = 1 To Len(strPlaintext)
      c = Asc(Mid$(strPlaintext, i, 1))
      If ((c >= 65) And (c <= 90)) Then
         'Dapatkan urutan abjad
         pAlphabet = c - 65

         'Digeser dengan kunci nShift mod 26
         cAlphabet = (pAlphabet + nShift) Mod 26

         'Kembalikan urutan abjad dengan kode ASCII
         c = cAlphabet + 65
      End If
      s = s & Chr(c)
   Next i
   Return s
End Function
```

Ada dua macam substitusi pada kriptografi klasik yaitu *polyalphabetic substitution cipher* dan *monoalphabetic substitution cipher*. Pada polyalphabetic substitution cipher, enkripsi terhadap satu huruf yang sama bisa menghasilkan huruf yang berbeda sehingga lebih sulit untuk menemukan pola enkripsinya, contohnya pada kriptografi Vigenere yang akan diterangkan kemudian. Pada monoalphabetic substitution cipher maka satu huruf tertentu pasti akan berubah menjadi huruf tertentu yang lain, sehingga

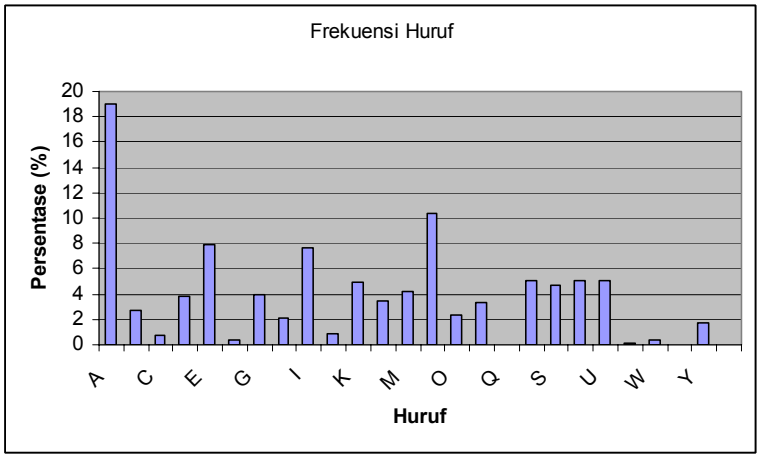
pola enkripsinya lebih mudah diketahui, karena satu huruf pada ciphertext pasti merepresentasikan satu huruf pada plaintext. Contoh monoalphabetic subsitution cipher adalah kriptografi Caesar.

Salah satu cara untuk bisa memecahkan penyandian dengan cara monoalphabetic subsitution cipher adalah dengan melakukan analisa frekwensi munculnya huruf dalam suatu bahasa. Berapa sering suatu huruf muncul dalam suatu bahasa tertentu bisa memberi petunjuk huruf-huruf yang muncul pada ciphertext asal diketahui plaintext yang digunakan berbahasa apa. Agar diperoleh pendekatan yang maksimal, maka sebaiknya dilakukan terhadap ciphertext yang cukup panjang, karena jika plaintextnya terlalu pendek, maka tingkat ketelitiannya akan menjadi rendah.

Di bawah ini dilakukan analisa terhadap kemungkinan munculnya huruf dalam bahasa Indonesia. Dari 1000000 (satu juta) karakter, maka huruf 'A' menduduki peringkat tertinggi yaitu di atas 19%, huruf 'N' menduduki peringkat kedua yaitu sekitar 10% dan huruf 'I' menduduki peringkat selanjutnya yaitu 8%.

Jika kita melakukan kriptografi sustitusi dengan cara monoalphabetic substitution cipher, maka satu karakter dari ciphertext merepresentasikan satu huruf dari plaintext. Jika diketahui bahwa plaintextnya bahasa Indonesia dan dilakukan analisa frekwensi munculnya huruf terhadap ciphertext tersebut, maka prosentasi munculnya suatu huruf pada ciphertext akan mendekati prosentasi muculnya huruf yang diwakilinya dalam plaintext. Sehingga jika, pada ciphertext, huruf 'D' mendekati 19%, maka akan sangat mungkin bahwa huruf 'D' adalah huruf 'A', begitu juga dengan huruf-huruf lainnya.

Grafik berikut memperlihatkan persentase frekwensi huruf dalam bahasa Indonesia:



Gambar 10. Frekuensi huruf dalam Bahasa Indonesia

2. Kriptografi Vigenere

Pada kriptografi Caesar pergeseran akan sama pada seluruh pesan. Jika kunci yang digunakan adalah huruf E, maka setiap huruf pada pesan akan bergeser 4 huruf. Begitu juga bila digunakan kunci-kunci lainnya. Pada kriptografi Vigenere, plaintext akan dienkripsi dengan pergeseran huruf seperti pada kriptografi Caesar tetapi setiap huruf di dalam plaintext akan mengalami pergeseran yang berbeda [Sta03]. Kunci pada kriptografi Vigenere adalah sebuah kata bukan sebuah huruf. Kata kunci ini akan dibuat berulang sepanjang plaintext, sehingga jumlah huruf pada kunci akan sama dengan jumlah huruf pada plaintext. Pergeseran setiap huruf pada plaintext akan ditentukan oleh huruf pada kunci yang mempunyai posisi yang sama dengan huruf pada plaintext. Kriptografi Vigenere ini dikenal sebagai polyalphabetic substitution cipher, karena enkripsi terhadap satu huruf yang sama bisa menghasilkan huruf yang berbeda.

Pergeseran setiap huruf pada plaintext ditentukan oleh huruf pada posisi yang sama (lihat tabel 2). Dan pergeseran ini ditentukan oleh tabel yang sama dengan tabel pada kriptografi Caesar.

Tabel 2. Tabel pergeseran huruf pada kriptografi Vigenere

Kunci	A	B	C	D	E	F	G	H	I
Pergeseran k	0	1	2	3	4	5	6	7	8
Kunci	J	K	L	M	N	O	P	Q	R
Pergeseran k	9	10	11	12	13	14	15	16	17
Kunci	S	T	U	V	W	X	Y	Z	
Pergeseran k	18	19	20	21	22	23	24	25	

Rumus kriptografi Caesar tetap berlaku pada kriptografi Vigenere, baik pada enkripsi maupun dekripsi:

$$C = E(P) = (P + k) \bmod 26$$
$$P = D(C) = (C - k) \bmod 26$$

di mana *P* adalah plaintext, *C* adalah ciphertext, *k* adalah pergeseran huruf sesuai dengan huruf pada posisi huruf pada plaintext.

Sebagai contoh, jika plaintext adalah INI PESAN RAHASIA, maka jika kita gunakan kunci kata BESOK, maka kunci ini akan diulang sama panjang dengan plaintext. Setiap huruf pada kata BESOK mempunyai pergeseran yang berbeda, sehingga setiap huruf akan mengalami pergeseran yang berbeda. Huruf yang sama bisa menghasilkan cipher yang berbeda.

Tabel 3. Contoh kriptografi Vigenere

Plaintext	I	N	I		P	E	S	A	N
Kunci	B	E	S		O	K	B	E	S
Pergeseran k	1	4	18		14	10	1	4	18
Ciphertext	J	R	A		D	O	T	E	F
Plaintext	R	A	H	A	S	I	A		
Kunci	O	K	B	E	S	O	K		
Pergeseran k	14	10	1	4	18	14	10		
Ciphertext	F	K	I	E	K	W	k		

Ada cara lain untuk melakukan kriptografi Vigenere yaitu dengan menuliskan abjad berurutan dari A sampai dengan Z, kemudian kata kuncinya dituliskan secara vertikal di bawah huruf A. Setiap huruf dari kata kunci ini kemudian dilengkapi dengan abjad selanjutnya dalam urutan alfabet dan setelah huruf Z kembali lagi ke huruf A,B dan seterusnya. Jika kita menggunakan kata kunci BESOK, maka akan dituliskan sebagai berikut :

Tabel 4. Tabel Kriptografi Vigenere

ABCDEFGHIJKLMNOPQRSTUVWXYZ ----------> Alfabet
BCDEFGHIJKLMNOPQRSTUVWXYZA
EFGHIJKLMNOPQRSTUVWXYZABCD

STUVWXYZABCDEFGHIJKLMNOPQR
OPQRSTUVWXYZABCDEFGHIJKLMN
KLMNOPQRSTUVWXYZABCDEFGHIJ

Untuk melakukan enkripsi terhadap suatu pesan, maka cari posisi setiap huruf pada plaintext pada baris paling atas, kemudian cari huruf pada lokasi yang sama di baris bawahnya. Huruf pertama diubah dengan huruf yang ada pada posisi yang sama pada baris ke dua atau baris dari huruf pertama pada kata kunci. Huruf ke dua pada plaintext dikonversi dengan huruf pada posisi yang sama pada baris selanjutnya. Huruf ketiga dikonversi dengan baris ke tiga dan seterusnya. Jika semua baris sudah terpakai maka kembali ke baris paling atas dari kata kunci, sampai semua huruf pada plaintext dienkripsi.

Cara lain untuk melakukan kriptografi Vigenere adalah dengan menggunakan *tabula recta* sebagai berikut : Baris paling atas adalah alfabet dari A sampai dengan Z. Di baris ke dua, tuliskan alfabet mulai dengan B sampai dengan Z kemudian kembali ke A. Di baris bawahnya C diikuti alfabet selanjutnya sampai dengan Z dan kembali lagi ke A. Sampai huruf Z. Cara penulisan ini dikenal sebagai *tabula recta*. Kemudian enkripsi dilakukan sama dengan enkripsi menggunakan Table 4. Huruf-huruf pada kata kunci sebagai huruf pertama pada baris-baris pada tabula recta dan huruf-huruf pada plaintext dicari di baris pertama tabula recta.

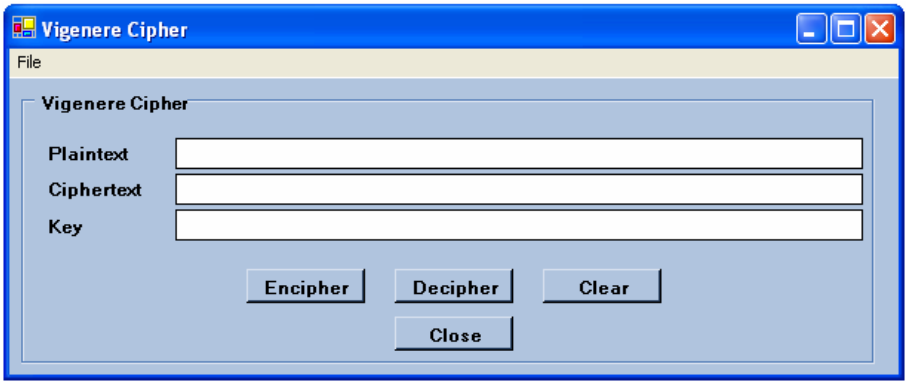
Tabel 5. Tabula Recta

ABCDEFGHIJKLMNOPQRSTUVWXYZ
BCDEFGHIJKLMNOPQRSTUVWXYZA
CDEFGHIJKLMNOPQRSTUVWXYXAB
D ……
……
…….
XYZABCDEFGHIJKLMNOPQRSTUVW
YZABCDEFGHIJKLMNOPQRSTUVWX
ZABCDEFGHIJKLMNOPQRSTUVWXY

Penggunaan lebih dari satu huruf dalam suatu enkripsi ini yang membuat kriptografi Vigenere disebut polyalphabetic cipher. Keuntungan dari kriptografi polyalphabetic cipher adalah sulitnya melakukan analisa frekwensi (*frequency analysis*) terhadap munculnya suatu huruf dalam ciphertext. Analisa frekwensi adalah suatu cara untuk melakukan cryptanalysis terhadap suatu ciphertext dengan menghitung berapa sering suatu huruf muncul pada ciphertext tersebut dengan memperbandingkan dengan berapa sering suatu huruf muncul dalam pesan atau tulisan normal. Contohnya jika huruf P sering muncul pada suatu ciphertext dalam bahasa Inggeris, huruf P ini sangat mungkin adalah huruf E, karena huruf E adalah huruf yang paling sering digunakan dalam tulisan-tulisan bahasa Inggeris. Analisa frekwensi ini sulit dilakukan dalam kriptografi Vigenere karena satu huruf tertentu pada plaintext bisa berubah menjadi beberapa huruf-huruf lain pada ciphertext tergantung pada kata kuncinya, sehingga frekwensi suatu huruf yang muncul pada ciphertext tidak merepresentasikan suatu huruf pada plaintext.

Kriptografi Vigenere ini bukan yang terbaik yang dihasilkan oleh Vigenere. Dia mengembangkan kriptografi lain yang dikenal sebagai kriptografi Autokey yang konon lebih handal dari pada kriptografi Vigenere, tetapi nama Vigenere sudah terlanjur melekat pada kriptografi sebelumnya. Sampai dengan kurun waktu 300 tahun, kedua kriptografi ini dianggap *'unbreakable'*, tetapi pada pertengahan abad 19, Charles Babbage dan Friedrich Kasiski secara terpisah mampu memecahkan cara penyandian ini.

Berikut adalah implementasi kriptografi Vigenere dalam Visual Basic .NET. Setelah program dijalankan akan terlihat menu sebagai berikut:



Gambar 11. Menu Kriptografi Vigenere

1. Masukkan plaintext ke kolom plaintext, misalnya :

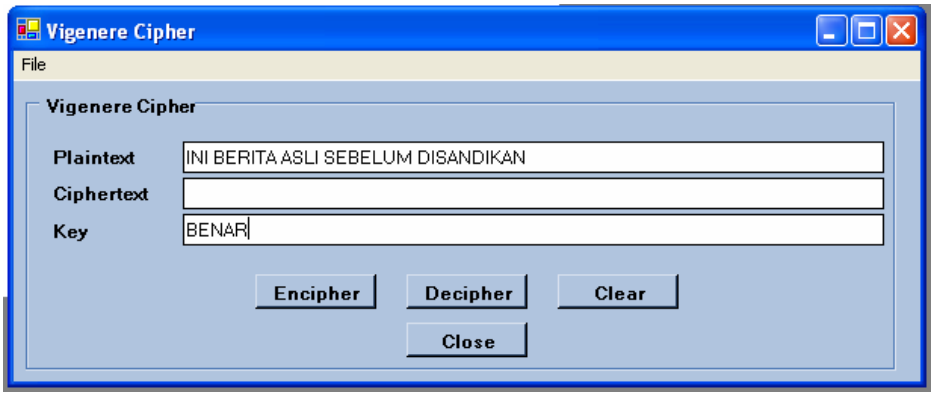
   INI BERITA ASLI SEBELUM DISANDIKAN

2. Masukkan kunci: BENAR

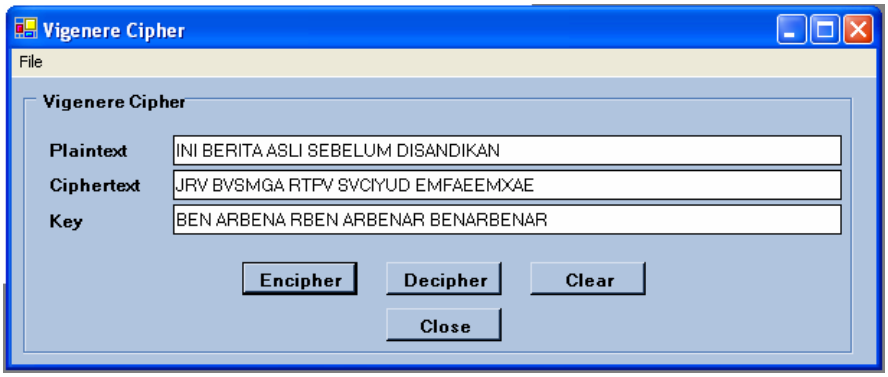
3. Tekan tombol Encipher , dan lihat ciphertext yang dihasilkan .

4. Coba dengan kalimat lain.

5. Coba sendiri buat Decipher .



Gambar 12. Menu Kriptografi Vigenere dengan plaintext dan kunci



Gambar 13. Menu Kriptografi Vigenere setelah enkripsi dilakukan

Kode Sumber:

```
Private Function VigenereEncipher(ByVal strPlaintext As String, ByRef strKey As String) As String
    Dim strPlaintext2 As String
    Dim strKey2 As String
    Dim strCiphertext As String
    Dim strCiphertext2 As String

    Dim i As Integer
    Dim j As Integer
    Dim c1 As Integer
    Dim nShift As Integer

    Dim pAlphabet As Integer
    Dim cAlphabet As Integer

    '1. Hilangkan semua karakter yang bukan alfabet dari strPlaintext
    '   dan simpan sebagai strPlaintext2

    strPlaintext2 = ""
    For i = 1 To strPlaintext.Length
       c1 = Asc(Mid(strPlaintext, i, 1))
       If (c1 >= 65 And c1 <= 90) Then
          strPlaintext2 = strPlaintext2 & Chr(c1)
       End If
    Next i

    '2. Hilangkan semua karakter yang bukan alfabet dari strKey
    '   dan simpan sebagai strKey2

    strKey2 = ""
    For i = 1 To strKey.Length
       c1 = Asc(Mid(strKey, i, 1))
       If (c1 >= 65 And c1 <= 90) Then
          strKey2 = strKey2 & Chr(c1)
       End If
    Next i

    '3. Susun key sepanjang plaintext
    If (strKey2.Length < strPlaintext2.Length) Then
       j = 0
       For i = 1 To strPlaintext2.Length
```

```
            c1 = Asc(Mid(strPlaintext, i, 1))
            strKey2 = strKey2 & Mid(strKey2, j + 1, 1)
            j = (j + 1) Mod strKey2.Length
        Next i
    End If

    '4. Geser masing-masing huruf pada plaintext
    '   dengan huruf yang terkait pada key

    strCiphertext = ""
    For i = 1 To strPlaintext2.Length
        c1 = Asc(Mid$(strPlaintext2, i, 1))
        nShift = Asc(Mid$(strKey2, i, 1)) - 65
        If ((c1 >= 65) And (c1 <= 90)) Then
            pAlphabet = c1 - 65      ' get the alphabet sequence
            cAlphabet = (pAlphabet + nShift) Mod 26 ' shifted alphabet
            c1 = cAlphabet + 65 ' get character in 65 ... 90
        End If
        strCiphertext = strCiphertext & Chr(c1)
    Next i

    '5. Susun strCiphertext sesuai dengan urutan strPlaintext
    strCiphertext2 = ""
    strKey = ""
    j = 1
    For i = 1 To strPlaintext.Length
        c1 = Asc(Mid$(strPlaintext, i, 1))
        If ((c1 >= 65) And (c1 <= 90)) Then
            strCiphertext2 = strCiphertext2 & Mid(strCiphertext, j, 1)
            strKey = strKey & Mid(strKey2, j, 1)
            j = j + 1
        Else
            strCiphertext2 = strCiphertext2 & Chr(c1)
            strKey = strKey & " "
        End If
    Next i

    Return strCiphertext2

End Function
```

3. Kriptografi Autokey

Kriptografi Autokey adalah pengembangan dari kriprografi Caesar dan Vigenere. Cara melakukan enkripsi sama dengan kedua kriptografi sebelumnya. Pada kriptografi Autokey juga digunakan sebuah kata sebagai kunci. Kunci ini kemudian diikuti dengan plaintext sehingga membentuk huruf-huruf yang sama panjang dengan plaintext. Urutan huruf-huruf ini yang akan digunakan sebagai kunci pada saat enkripsi.

Rumus yang berlaku untuk kriptografi Autokey sama dengan untuk Caesar dan Vigenere.

$$C = E(P) = (P + k) \bmod 26$$
$$P = D(C) = (C - k) \bmod 26$$

Tabel pergeseran huruf pun sama

Tabel 6. Tabel pergeseran huruf pada kriptografi Autokey

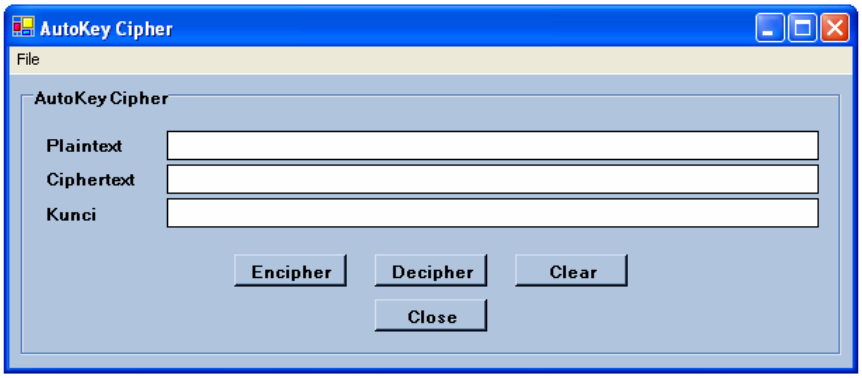
Kunci	A	B	C	D	E	F	G	H	I
Pergeseran k	0	1	2	3	4	5	6	7	8
Kunci	J	K	L	`M	N	O	P	Q	R
Pergeseran k	9	10	11	12	13	14	15	16	17
Kunci	S	T	U	V	W	X	Y	Z	
Pergeseran k	18	19	20	21	22	23	24	25	

Contoh, jika plaintext adalah INI PESAN RAHASIA, maka jika kita gunakan kunci kata BESOK, maka kata BESOK akan disisipkan di depan plaintext INI PESAN RAHASIA. Kemudian enkripsi dilakukan sama dengan enkripsi Caesar dan Vigenere.

Tabel 7. Contoh Kriptografi Autokey

Plaintext	I	N	I		P	E	S	A	N
Kunci	B	E	S		O	K	I	N	I
Pergeseran k	1	4	18		14	10	8	13	8
Ciphertext	J	R	A		D	O	A	N	V
Plaintext	R	A	H	A	S	I	A		
Kunci	P	E	S	A	N	R	A		
Pergeseran k	15	4	18	0	13	17	0		
Ciphertext	G	E	Z	A	F	Z	A		

Berikut adalah implementasi kriptografi Autokey di dalam Visual.Basic .NET:



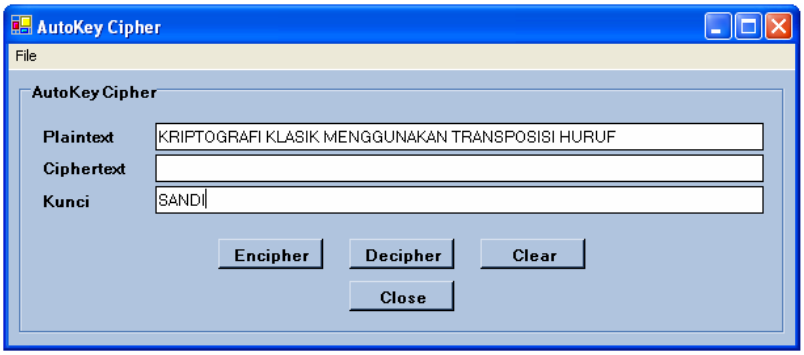
Gambar 14. Menu Kriptografi Autokey

1. Masukkan plaintext ke kolom plaintext, misalnya :

   KRIPTOGRAFI KLASIK MENGGUNAKAN TRANSPOSISI HURUF

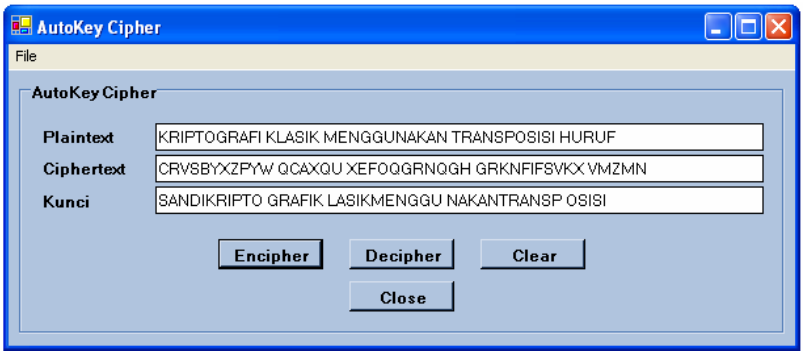
2. Masukkan kunci : SANDI

3. Tekan tombol Encipher , dan lihat ciphertext yang dihasilkan .



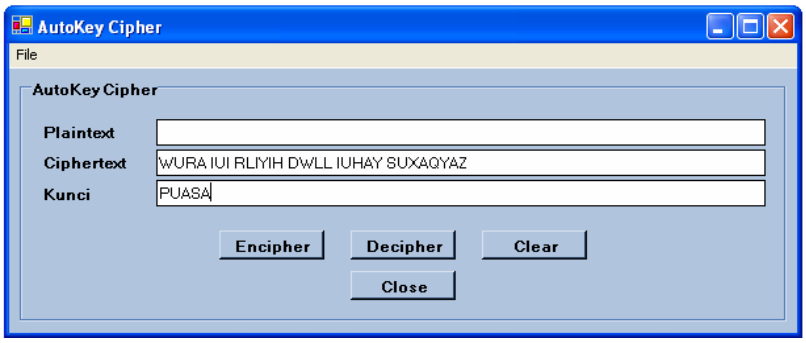
Gambar 15. Menu Kriptografi Autokey dengan plaintext dan kunci sudah diisi

Akan terlihat bahwa pada kunci, kalimat KRIPTOGRAFI KLASIK MENGGUNAKAN TRANSPOSISI HURUF yaitu plaintext akan mengikut kata SANDI dan menyesuaikan penempatan spasi dan panjang dengan plaintext.



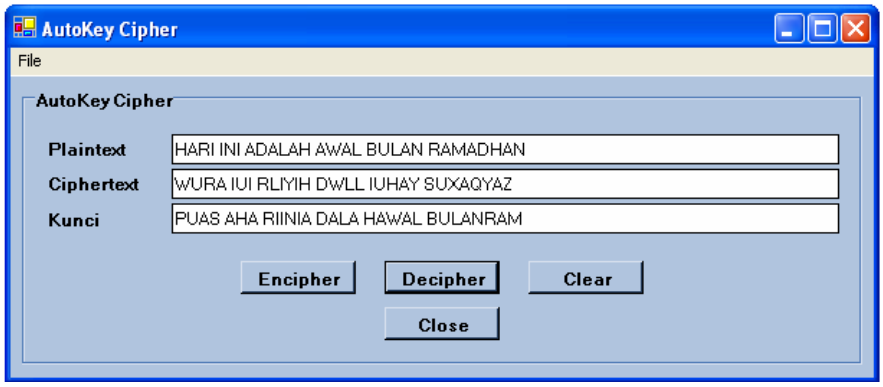
Gambar 16. Menu Kriptografi Autokey setelah enkripsi dilakukan

Cobalah lagi dengan Dekripsi



Gambar 17. Menu Kriptografi Autokey pada saat akan melakukan dekripsi

Tampak bahwa key PUASA akan terpecah menjadi dua, PUAS dan A untuk menyesuaikan dengan penempatan spasi pada ciphertext. Kemudian diikuti dengan huruf-huruf pada plaintext dengan penyesuaian letak spasi.



Gambar 18. Menu Kriptografi Autokey setelah dekripsi dilakukan

Kode Sumber:

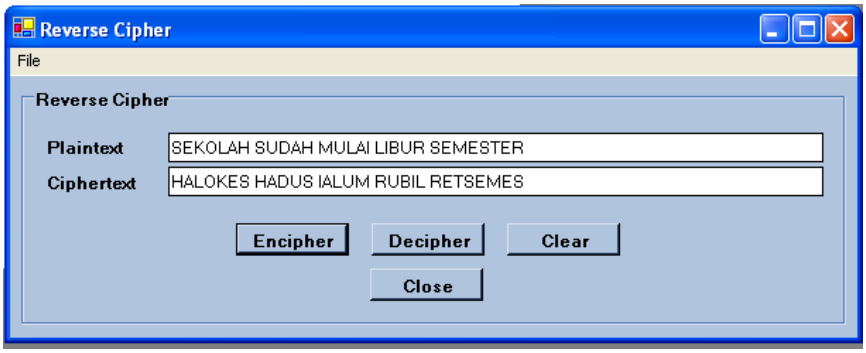
```
Private Function AutokeyEncipher(ByVal strPlaintext As String, ByRef strKey As String) As String
    Dim i As Long
    Dim j As Long

    Dim c1 As Integer
    Dim c2 As Integer

    Dim strPlaintext2 As String
    Dim strKey2 As String
    Dim strCiphertext As String
    Dim strCiphertext2 As String

    Dim diffKeyLen As Integer

    Dim pAlphabet As Integer
    Dim cAlphabet As Integer
    Dim nShift As Integer

    '1. Hilangkan semua karakter yang bukan alfabet dari strPlaintext
    '   dan simpan sebagai strPlaintext2

    strPlaintext2 = ""
    For i = 1 To strPlaintext.Length
       c1 = Asc(Mid(strPlaintext, i, 1))
       If (c1 >= 65 And c1 <= 90) Then
          strPlaintext2 = strPlaintext2 & Chr(c1)
       End If
    Next i

    '2. Hilangkan semua karakter yang bukan alfabet dari strKey
    '   dan simpan sebagai strKey2

    strKey2 = ""
    For i = 1 To strKey.Length
```

```
        c1 = Asc(Mid(strKey, i, 1))
        If (c1 >= 65 And c1 <= 90) Then
            strKey2 = strKey2 & Chr(c1)
        End If
    Next i

    '3. Susun kunci baru strKey2 berdasarkan kunci awal strKey kemudian
    '   ditambah plaintext

    'perbedaan antara panjang plaintext dan kunci
    diffKeyLen = strPlaintext2.Length - strKey2.Length

    For i = 1 To diffKeyLen
        'c1 = Asc(Mid(strPlaintext2, i, 1))
        strKey2 = strKey2 & Mid(strPlaintext2, i, 1)
    Next i

    '4. Geser masing-masing huruf pada plaintext
    '   dengan huruf yang terkait pada key

    strCiphertext = ""
    For i = 1 To strPlaintext2.Length
        c1 = Asc(Mid$(strPlaintext2, i, 1))
        nShift = Asc(Mid$(strKey2, i, 1)) - 65
        If ((c1 >= 65) And (c1 <= 90)) Then
            pAlphabet = c1 - 65      ' get the alphabet sequence
            cAlphabet = (pAlphabet + nShift) Mod 26 ' shifted alphabet
            c1 = cAlphabet + 65 ' get character in 65 ... 90
        End If
        strCiphertext = strCiphertext & Chr(c1)
    Next i

    '5. Susun strCiphertext sesuai dengan urutan strPlaintext
    strCiphertext2 = ""
    strKey = ""
    j = 1
    For i = 1 To strPlaintext.Length
        c1 = Asc(Mid$(strPlaintext, i, 1))
        If ((c1 >= 65) And (c1 <= 90)) Then
            strCiphertext2 = strCiphertext2 & Mid(strCiphertext, j, 1)
            strKey = strKey & Mid(strKey2, j, 1)
            j = j + 1
        Else
            strCiphertext2 = strCiphertext2 & Chr(c1)
            strKey = strKey & " "
        End If
    Next i

    Return strCiphertext2
End Function
```

4. Kriptografi Reverse

Ini adalah contoh kriptografi klasik yang menggunakan transposisi yaitu mengganti satu huruf dengan huruf lain. Ini contoh yang paling sederhana dari transposisi yaitu mengubah suatu kalimat dengan menuliskan setiap kata secara terbalik

Program berikut adalah implementasi Kripotgrafi Reverse dalam Visual Basic .NET. Masukkan suatu kalimat dan klik tombol Encipher kemudian coba lagi dengan Decipher



Gambar 19. Menu Kriptografi Reverse setelah enkripsi dilakukan

Kode Sumber:

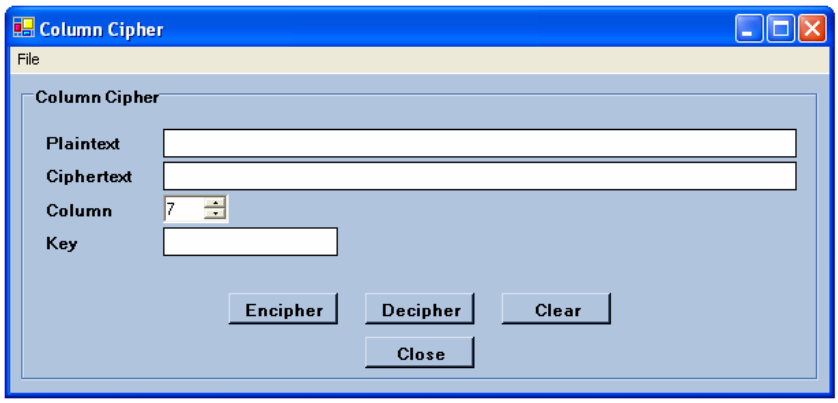
```
Private Function ReverseEncipher(ByVal strPlaintext As String) As String
        Dim c1 As String
        Dim strCiphertext As String
        Dim strWord As String
        Dim plainLen As Integer
        Dim i As Long

        ' panjang string strKey dan strPlaintext
        plainLen = strPlaintext.Length()

        strCiphertext = ""
        strWord = ""
        For i = 1 To plainLen
            c1 = Asc(Mid(strPlaintext, i, 1))
            If ((c1 >= 65) And (c1 <= 90)) Then
                strWord = Chr(c1) & strWord
            Else
                strCiphertext = strCiphertext & strWord & Chr(c1)
                strWord = ""
            End If
        Next
        strCiphertext = strCiphertext & strWord

        Return strCiphertext
    End Function

    Private Sub btnDecipher_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles btnDecipher.Click
        Dim nShift As Integer

        ' nShift2 menunjukkan pergeseran huruf dengan
        ' index A = 0,..., Z = 25
        ' angka 65 menunjukkan angka huruf A
        ' nShift = Asc(Mid$(cbKey.Text, 1, 1)) - 65

        ' memanggil fungsi Encipher untuk mengenkripsi plaintext
        txtPlaintext.Text = ReverseDecipher(txtCiphertext.Text)
```

```
        ' txtPlaintext.Text = Decipher(txtCiphertext.Text, nShift)
    End Sub
```

5. Kriptografi Kolom

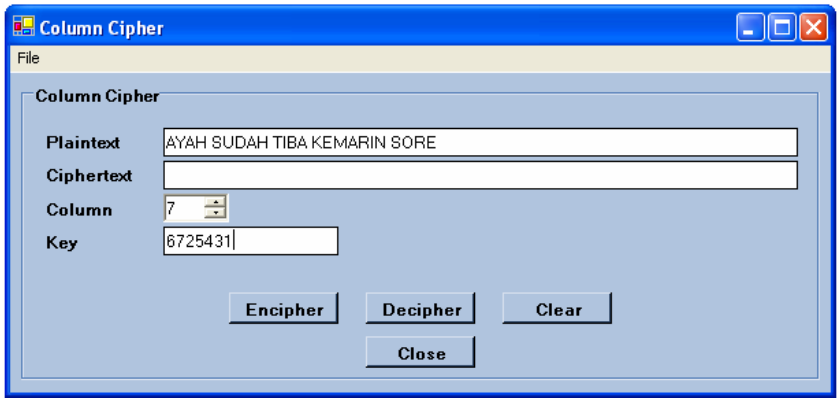
Pada kriptografi kolom (column cipher), plaintext disusun dalam kelompok huruf yang terdiri dari beberapa huruf. Kemudian huruf-huruf dalam kelompok ini dituliskan kembali kolom per kolom, dengan urutan kolom yang bisa berubah-ubah.

Program berikut adalah implementasi Kriptografi Kolom di dalam Visual Basic .NET. setelah program dijalankan, maka akan terlihat menu sebagai berikut :



Gambar 20. Menu Kriptografi Kolom

Jika dimasukkan kalimat ‘AYAH SUDAH TIBA KEMARIN SORE’ dan akan dilakukan dengan 7 kolom huruf denan urutan kunci 6725431, maka pada menu terlihat:



Gambar 21. Menu setelah plaintext diisi dan kolom huruf disesuaikan dengan yang diinginkan

Kalimat ‘AYAH SUDAH TIBA KEMARIN SORE’, jika disusun dalam kolom 7 huruf, maka akan menjadi kolom-kolom berikut :

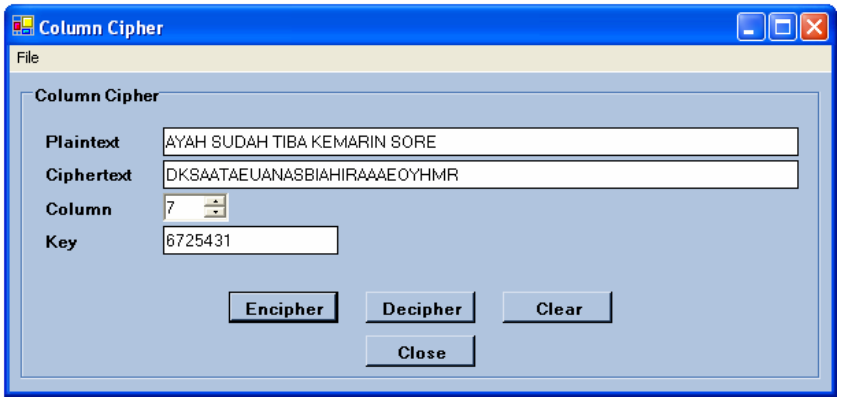
AYAHSUD
AHTIBAK
EMARINS
OREAAAA

Gambar 22. Setelah plaintext disusun dalam kolom 7 huruf

DKSAATAEUANASBIAHIRAAAEOYHMR

Gambar 23. Ciphertext setelah kolom huruf dituliskan sesuai urutan kunci yang dikehendaki

Maka setelah tombol Encipher di-klik, akan dihasilkan menu berikut :



Gambar 24. Menu Kriptografi Kolom setelah enkripsi dilakukan

Lihat hasilnya, cobalah dengan urutan kolom yang berbeda. Coba kembali dengan decipher.

Kode Sumber :

```
Private Function ColumnEncipher(ByVal strPlaintext As String, ByVal nColumn As Integer, ByVal strKey As String) As String
    Dim c1 As Integer

    Dim i As Long
    Dim j As Integer
    Dim k As Integer
    Dim r As Integer

    Dim strPlaintext2 As String
    Dim strCiphertext As String

    Dim colArray(1, 1) As Integer
    Dim nRow As Integer

    '1.a. Hapus semua karakter non-alphabet dari plaintext
    strPlaintext2 = ""
```

```
        For i = 1 To strPlaintext.Length
            c1 = Asc(Mid(strPlaintext, i, 1))
            If (c1 >= 65 And c1 <= 90) Then
                strPlaintext2 = strPlaintext2 & Chr(c1)
            End If
        Next i

        '1.b. Pad plaintext hingga habis dibagi jumlah kolom
        Dim remainder As Integer

        remainder = strPlaintext2.Length Mod nColumn
        'MsgBox("length: " & strPlaintext2.Length & ", nColumn: " & nColumn & ", remainder: " &
remainder)
        If (remainder <> 0) Then
            For i = 1 To (nColumn - remainder)
                strPlaintext2 = strPlaintext2 & "A"
            Next i
        End If

        '2. Buat multidimensional array
        '   berdasarkan jumlah kolom yang ditetapkan
        nRow = CInt(Math.Ceiling(CDbl(strPlaintext2.Length) / CDbl(nColumn)))

        ReDim colArray(nRow, nColumn)

        '3. Susun huruf-huruf dalam matrix dengan
        '   urutan baris kemudian kolom
        k = 1
        For i = 0 To (nRow - 1)
            For j = 0 To (nColumn - 1)
                If (k <= strPlaintext2.Length) Then
                    colArray(i, j) = Asc(Mid(strPlaintext2, k, 1))
                    k = k + 1
                Else
                    colArray(i, j) = Asc("A")
                End If
            Next j
        Next i

        '4. Susun huruf-huruf menjadi ciphertext dengan
        '   membaca kolom sesuai dengan urutan dalam key
        strCiphertext = ""

        Dim str1 As String = ""
        For i = 0 To (nColumn - 1)
            'cari nomor kolom yang sesuai di dalam kunci
            k = i + 1
            For j = 1 To strKey.Length
                If (k = CInt(Mid(strKey, j, 1))) Then
                    'apabila kolom k ditemukan, maka kolom tersebut dicetak
                    For r = 0 To (nRow - 1)
                        strCiphertext = strCiphertext & Chr(colArray(r, j - 1))
                    Next r
                End If
            Next j
        Next i

        Return strCiphertext
```

```
End Function
```

6. Kriptografi One-Time Pad

One-Time Pad adalah kriptografi yang merupakan perbaikan terhadap kriptografi Caesar. One-Time Pad menggunakan kunci yang mempunyai panjang sama dengan plaintext dan kunci ini hanya digunakan 1 kali. Karena itu, cara enkripsi ini dikenal sebagai One-Time Pad dan kriptografi ini tidak bisa dipecahkan karena kunci hanya digunakan satu kali sehingga tidak ada suatu pola tertentu. Satu-satunya cara melakukan dekripsi adalah dengan mengetahui kunci yang digunakan.

Enkripsi dilakukan dengan cara sama dengan enkripsi Caesar, tetapi karena panjang kunci sama dengan plaintext, maka setiap huruf pada plaintext akan mengalami pergeseran yang berbeda.

Memang One-Time Pad adalah kriptografi yang tidak pernah bisa dipecahkan. Kunci hanya bisa digunakan sekali dan harus mempunyai panjang yang sama dengan plaintextnya. One-Time Pad ini biasanya digunakan dalam situasi yang kritis. Biasanya keputusan-keputusan militer seperti peluncuran peluru kendali nuklir di era perang dingin. Sampai sekarang One-Time Pad ini masih digunakan oleh kedutaan-kedutaan besar untuk pengiriman berita diplomatik.

Aplikasi dalam Visual Basic .NET dan kode sumber dapat di-download dari situs WEB berikut: http://mawar.inn.bppt.go.id/~fahmi/.

7. 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. Artikel ini dilengkapi dengan beberapa contoh kriptografi klasik beserta progam aplikasinya yaitu kriptografi Caesar, Vigenere, Autokey, Reverse dan Column.

Di era komputer, informasi dikirimkan melalui jaringan dan disimpan di komputer. Tetapi kebutuhan akan keamanan data sama. Kriptografipun dilakukan di era komputer tetapi dikenal sebagai kriptografi modern yang menggunakan algoritma matematika yang cukup rumit dan penggunaan kunci. Dengan demikian, kriptografi meliputi semua hal mengenai cara menghindari dan menemukan semua penipuan dan semua ke-tidakjujur-an yang terjadi pada suatu pengiriman informasi baik secara manual pada kriptografi klasik ataupun secara matematika pada kriptografi modern. Dan pada dasarnya yang dilakukan pada kedua-duanya sama yaitu transposisi dan substitusi huruf untuk menghasilkan berita acak yang tidak bisa dibaca. Artikel tentang kriptografi klasik ini dibuat sebagai pengenalan terhadap kriptografi yang akan dituliskan berikutnya yaitu kriptografi modern. Kriptografi modern banyak digunakan dalam pengiriman informasi melalui Internet.

Daftar Pustaka

Febr04	Jack Febrian, Pengetahuan Komputer dan Teknologi Informasi. Informatika Bandung, 2004
Kahn96	Kahn, D. The Codebreakers: The Story of secret writing. New York:Scribner, 1996
MOV96	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
Sta03	Willam Stallings, Cryptography and Network Security, Principles and Practices. Pearson Prentice Hall, 2003

Sta04 William Stallings, Data and Computer Communications. Pearson Prentice Hall, 2004
Tan03 Andrew S. Tanenbaum, Computer Networks. Prentice Hall PTR, 2003

Gary C. Kessler, **An Overview of Cryptography 1998**

Biodata Penulis

Husni Fahmi, Ph.D. menamatkan pendidikan S1, S2, dan S3 di bidang computer engineering dari Purdue University, USA masing-masing pada tahun 1995, 1997, dan 2002. Dia aktif melakukan penelitian dalam bidang jaringan dan keamanan komputer dan telah mempublikasikan karya ilmiahnya dalam konferensi dan jurnal internasional seperti IEEE. Sejak Agustus tahun 2002, dia bekerja di Pusat Pengkajian dan Pengembangan Teknologi Informasi dan Elektronika (P3TIE), BPPT. BPPT menugaskannya ke Komisi Pemilihan Umum (KPU) sebagai Project Management Officer Information Technology, Agustus 2003 – Desember 2004 untuk mengembangkan sistem teknologi informasi untuk Pemilu 2004. Hingga sekarang dia masih aktif sebagai anggota Tim Ahli IT di KPU untuk terus memelihara dan mengembangkan sistem untuk keperluan Pemilu dan Pilkada Langsung. Selain melakukan penelitian dalam bidang jaringan dan keamanan di BPPT, dia juga mengajar di Swiss German University dan Universitas Budi Luhur.

Haret Faidah menamatkan kuliah di Fakultas Teknik Elektro pada tahun 1980. Sejak tahun 1980, menjadi pegawai Negeri di Badan Pengkajian dan Penerapan Teknologi. Pada tahun 1983, diperbantukan di PT Dirgantara Indonesia (PT DI), yang waktu itu masih bernama PT Nurtanio. Di PT Nurtanio bertugas di Pusat Komputasi (PK) Nurtanio. Bekerja di PT Nurtanio yang kemudian berubah nama menjadi PT IPTN mulai tahun 1983 ketika komputer mainframe sedang populer. Pada tahun 1992 dan 1993, dia mendapat kesempatan untuk bekerja di MBB Hamburg, Jerman Barat. Kembali dari Jerman, PT IPTN mulai mengembangkan sistem terdistribusi yang terdiri dari ratusan PC dan work station sehingga dia ikut mengembangkan sistem terdistribusi berbasis OS Unix baik di PC maupun di workstation dan juga teknologi jaringan komputer. Pada tahun Maret 2005 kembali ke instansi induk BPPT. Yang bersangkutan sangat tertarik pada teknologi jaringan komputer dan ingin mengisi hari-harinya dengan menulis buku-buku ilmiah komputer dan teknologi informasi.