PERANCANGAN APLIKASI ENKRIPSI DEKRIPSI MENGGUNAKAN METODE CAESAR CHIPER DAN OPERASI XOR

Nur Azis

Universitas Krisnadwipayana Prodi Informatika
Jalan Raya Jatiwaringin , Rt.03/Rw.04, Jatiwaringin, Pondok Gede, Kota Bekasi,
email : nurazis03@yahoo.co.id

ABSTRAK

Perkembangan teknologi yang begitu pesat memungkinkan manusia dapat berkomunikasi dan saling bertukar informasi/data secara jarak jauh. Antar wilayah antar negara bahkan antar benua bukan merupakan suatu kendala lagi dalam melakukan komunikasi dan pertukaran data. Seiring dengan itu tuntutan akan sekuritas (keamanan) terhadap kerahasiaan informasi yang saling dipertukarkan tersebut semakin meningkat. Keamanan dan kerahasiaan saat melakukan pertukaran data dan informasi menjadi hal yang sangat penting pada era teknologi informasi dan komunikasi saat ini, Oleh karena itu dikembangkanlah cabang ilmu yang mempelajari tentang cara-cara pengamanan data atau dikenal dengan istilah Kriptografi.

Kata Kunci : Keamanan, Informasi, Komunikasi, kriptografi

1. PENDAHULUAN

Latar belakang

Perkembangan teknologi yang begitu pesat memungkinkan manusia dapat berkomunikasi dan saling bertukar informasi/data secara jarak jauh. Antar wilayah antar negara bahkan antar benua bukan merupakan suatu kendala lagi dalam melakukan komunikasi dan pertukaran data. Seiring dengan itu tuntutan akan sekuritas (keamanan) terhadap kerahasiaan informasi yang saling dipertukarkan tersebut semakin meningkat. Keamanan dan kerahasiaan saat melakukan pertukaran data dan informasi menjadi hal yang sangat penting pada era teknologi informasi dan komunikasi saat ini, Oleh karena itu dikembangkanlah cabang ilmu yang mempelajari tentang cara-cara pengamanan data atau dikenal dengan istilah Kriptografi.

Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi/data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal.

Banyak sekali metode kriptografi yang ada, diantaranya metode *caesar chipper dan Operasi Xor*. Caesar Chiper adalah teknik kriptografi yang dilakukan dengan mensubtitusi setiap abjad dari pesan yang akan dienkripsi melalui pergeseran susunan sebagai kuncinya. Misalnya, tiap huruf disubstitusikan dengan huruf kelima berikutnya dari susunan asli. Dalam hal ini kuncinya adalah jumlah pergeseran huruf tersebut, yaitu kunci = 5. Arimetika modular merupakan operasi matematika yang banyak diimplementasikan pada metode kriptografi simetris, dengan simbol $\oplus$.

Rumusan Masalah

Adapun masalah dari judul ini adalah sebagai berikut:

1. Bagaimana mengimplementasikan teknologi enkripsi dan dekripsi pesan dengan menggunakan algoritma *caesar chiper dan operasi Xor* ?
2. Bagaimana merancang aplikasi enkripsi dan dekripsi berbasis *Visual Studio* 2005 dengan menggunakan algoritma *ceasar chiper dan operasi Xor* ?

2. LANDASAN TEORI

Pengertian Aplikasi

Aplikasi berasal dari kata *application* yang artinya penerapan, penggunaan. Secara istilah aplikasi adalah program siap pakai yang direka untuk melaksanakan suatu fungsi bagi pengguna atau aplikasi yang lain dan dapat digunakan oleh sasaran yang dituju.

Pengertian Kriptografi

Kriptografi berasal dari bahasa yunani, menurut bahasa dibagi menjadi dua, yaitu kripto dan graphia. Kripto berarti secret (rahasia) dan graphia berarti writing (tulisan). Menurut terminologinya kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ketempat lain.

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 *message-message* agar 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:

a. *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.
b. *Data integrity* (keutuhan data) yaitu layanan yang mampu mengenali/mendeteksi adanya manipulasi (penghapusan, pengubahan atau penambahan) data yang tidak sah (oleh pihak lain).
c. *Authentication* (keotentikan) yaitu layanan yang berhubungan dengan identifikasi. Baik otentikasi pihak-pihak yang terlibat dalam pengiriman data maupun otentikasi keaslian data/informasi.
d. *Availability (Ketersediaan), yaitu dimana user yang mempunyai hak akses atau authorized users diberi akses tempat waktu dan tidak terkendala apapun*
e. *Non-repudiation* (anti-penyangkalan) yaitu layanan yang dapat mencegah suatu pihak untuk menyangkal aksi yang dilakukan sebelumnya (menyangkal bahwa pesan tersebut berasal dari dirinya).

Berbeda dengan kriptografi klasik yang menitikberatkan kekuatan pada kerahasiaan algoritma yang digunakan (yang artinya apabila algoritma yang digunakan telah diketahui maka pesan sudah jelas "bocor" dan dapat diketahui isinya oleh siapa saja yang mengetahui algoritma tersebut), kriptografi modern lebih menitikberatkan pada kerahasiaan kunci yang digunakan pada algoritma tersebut (oleh pemakainya) sehingga algoritma tersebut dapat saja disebarkan ke kalangan masyarakat tanpa takut kehilangan kerahasiaan bagi para pemakainya.

Enkripsi dan dekripsi pada umumnya membutuhkan penggunaan sejumlah informasi rahasia, disebut sebagai kunci. Untuk beberapa mekanisme enkripsi, kunci yang sama digunakan baik untuk enkripsi dan dekripsi; untuk mekanisme yang lain, kunci yang digunakan untuk enkripsi dan dekripsi berbeda. Dua tipe dasar dari teknologi kriptografi adalah *symmetric key (secret/private key) cryptography* dan *asymmetric (public key) cryptography*. Pada *symmetric key cryptography*, baik pengirim maupun penerima memiliki kunci rahasia yang umum. Pada *asymmetric key cryptography*, pengirim dan penerima masing-masing berbagi kunci publik dan privat.

Berikut adalah istilah-istilah yang digunakan dalam bidang kriptografi :

a. **Plaintext** (M) adalah pesan yang hendak dikirimkan (berisi data asli) yang dapat dimengerti.
b. **Ciphertext** (C) adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi.
c. **Enkripsi** (E) adalah proses pengubahan *plaintext* menjadi *ciphertext*.
d. **Dekripsi** (D) adalah kebalikan dari enkripsi yakni mengubah *ciphertext* menjadi *plaintext*, sehingga berupa data awal/asli.
e. **Kunci (K)** adalah suatu bilangan yang dirahasiakan yang digunakan dalam proses enkripsi dan dekripsi.

Algoritma Simetris dan Asimetris

1. Algoritma Simetris

Algoritma simetris *(symmetric algorithm)* adalah suatu algoritma dimana kunci enkripsi yang digunakan sama dengan kunci dekripsi sehingga algoritma ini disebut juga sebagai *single-key algorithm.*

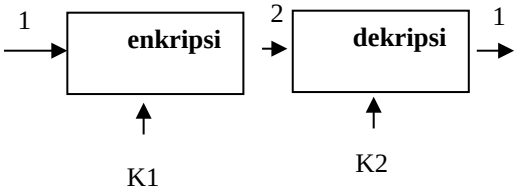


Diagram proses enkripsi dan dekripsi algoritma simetris

Ket :
1. Plaintext
2. Chiphertext

K1. Kunci enkripsi
K1. Kunci Dekripsi

Sebelum melakukan pengiriman pesan, pengirim dan penerima harus memilih suatu suatu kunci tertentu yang sama untuk dipakai bersama, dan kunci ini haruslah rahasia bagi pihak yang tidak berkepentingan sehingga algoritma ini disebut juga algoritma kunci rahasia *(secret-key algorithm).*

Kelebihan :

a. Kecepatan operasi lebih tinggi bila dibandingkan dengan algoritma asimetrik.
b. Karena kecepatannya yang cukup tinggi, maka dapat digunakan pada sistem *real-time.*

Kelemahan :

a. Untuk tiap pengiriman pesan dengan pengguna yang berbeda dibutuhkan kunci yang berbeda juga, sehingga akan terjadi kesulitan dalam manajemen kunci tersebut.
b. Permasalahan dalam pengiriman kunci itu sendiri yang disebut *"key distribution problem"*

Contoh algoritma : TwoFish, Rijndael, Caesar chipper

2. Algoritma Asimetris

Algoritma asimetris *(asymmetric algorithm)* adalah suatu algoritma dimana kunci enkripsi yang digunakan tidak sama dengan kunci dekripsi. Pada algoritma ini menggunakan dua kunci yakni kunci publik *(public key)* dan kunci privat *(private key).* Kunci publik disebarkan secara umum sedangkan kunci privat disimpan secara rahasia

oleh si pengguna. Walau kunci publik telah diketahui namun akan sangat sukar mengetahui kunci privat yang digunakan.

Pada umumnya kunci publik *(public key)* digunakan sebagai kunci enkripsi sementara kunci privat *(private key)* digunakan sebagai kunci dekripsi.

Kelebihan :

- Masalah keamanan pada distribusi kunci dapat lebih baik
- Masalah manajemen kunci yang lebih baik karena jumlah kunci yang lebih sedikit

Kelemahan :

- Kecepatan yang lebih rendah bila dibandingkan dengan algoritma simetris
- Untuk tingkat keamanan sama, kunci yang digunakan lebih panjang dibandingkan dengan algoritma simetris.

Contoh algoritma : RSA, DSA

Peranan kunci sangatlah penting dalam proses enkripsi dan dekripsi (disamping pula algoritma yang digunakan) sehingga kerahasiaannya sangatlah penting, apabila kerahasiaannya terbongkar, maka isi dari pesan dapat diketahui.

3. IMPLEMENTASI

Rancangan Sistem

Perancangan program aplikasi kriptografi dengan menggunakan metode Caesar chiper. Rancangan ini digunakan untuk meningkatkan keamanan pesan. Rancangan ini dilakukan dalam beberapa tahap yaitu dimulai dari perencanaan kemudian pembuatan diagram, yang dilanjutkan dengan menggunakan *Flowchart* dan *Data Flow Diagram*, dan dilanjutkan lagi dengan perancangan antar muka program. setelah rancangan sistem ini selesai dilanjutkan dengan pembuatan program aplikasi visual studio 2005. Setelah selesai, program aplikasi tersebut diuji.

Analisa Algoritma *Caesar Cipher*

Algoritma adalah urutan langkah- langkah logis penyelesaian masalah yang disusun secara sistematis dan logis, (R. Munir, 2002). Langkah-langkah dalam algoritma harus logis dan harus dapat ditentukan bernilai salah atau benar. algoritma adalah spesifikasi urutan langkah untuk melakukan pekerjaan tertentu.

Algoritma *caesar cipher* merupakan algoritma klasik yang memiliki langkah-langkah logis sebagai berikut :

1. Menghitung panjang karakter / huruf yang diinputkan dalam plaintext.
2. Tiap-tiap huruf diubah menjadi kode ASCII menggunakan proses looping.
3. Untuk melakukan pergeseran / proses enkripsi maka kode ASCII tersebut digeser dengan cara ditambah sebanyak pergeseran. Misal pergeseran 5 huruf maka kode ASCII ditambah dengan 5.
4. Jika ditemukan spasi (ASCII=32), maka tidak usah dilakukan penambahan.
5. Hasil pergeseran bilangan ASCII dikembalikan lagi menjadi huruf / karakter

Analisa Operator XOR

Operator biner yang sering digunakan dalam *cipher* yang yang beroperasi dalam mode bit adalah XOR atau *exclusive-or*. Notasi matematis untuk opeartor XOR adalah $\oplus$ (dalam Bahasa C, operator XOR dilambangkan dengan ^). Operator XOR dioperasikan pada dua bit dengan aturan sebagai berikut:

$0 \oplus 0 = 0$

$0 \oplus 1 = 1$

$1 \oplus 0 = 1$

$1 \oplus 1 = 0$

Jika dua rangkaian dioperasikan dengan XOR, maka operasinya dilakukan dengan meng-XOR-kan setiap bit yang berkoresponden dari kedua ramngkaian bit tersebut.

Contoh: 10011 ⊕ 11001 = 01010, yang dalam hal ini, hasilnya diperoleh sebagai berikut:

1 0 0 1 1 ⊕ 1 1 0 0 1

1 ⊕ 1 = 0

0 ⊕ 1 = 1

0 ⊕ 0 = 0

1 ⊕ 0 = 1

1 ⊕ 1 = 0

Algoritma enkripsi sederhana yang menggunakan XOR adalah dengan meng-XOR-kan plainteks (*P*) dengan kunci (*K*) menghasilkan cipherteks:

$$C = P \oplus K \quad (6.1)$$

Karena meng-XOR-kan nilai yang sama dua kali menghasilkan nilai semula, maka proses dekripsi menggunakan persamaan:

$$P = C \oplus K \quad (6.2)$$

Contoh: plainteks 01100101 (karakter ‘e’)
kunci 00110101 ⊕ (karakter ‘5’)
cipherteks 01010000 (karakter ‘P’)
kunci 00110101 ⊕ (karakter ‘5’)
plainteks 01100101 (karakter ‘e’)

Cara memecahkannya adalah (asumsi: panjang kunci adalah sejumlah kecil *byte*):

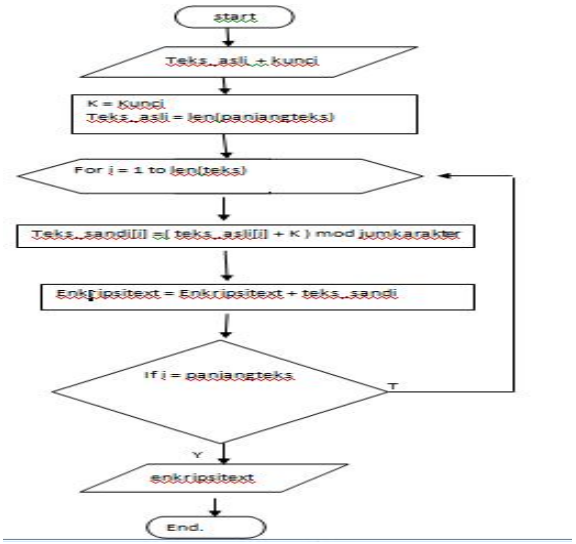
a. Pergeseran terkecil mengindikasikan panjang kunci yang dicari..
b. Geser cipherteks sejauh panjang kunci dan XOR-kan dengan dirinya sendiri. Operasi ini menghasilkan plainteks yang ter-XOR dengan plainteks yang digeser sejauh panjang kunci tersebut.

Proses Enkripsi dan Dekripsi

Enkripsi merupakan proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus.

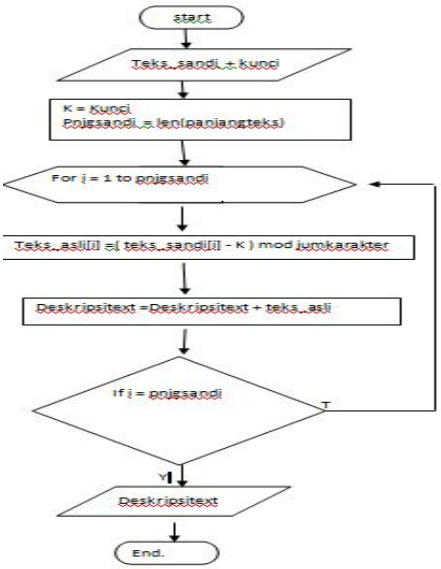
Dekripsi merupakan suatu proses penterjemahan sebuah karakter dengan kunci dan aturan tertentu menjadi sebuah karakter atau kalimat asli yang dapat dibaca dan diketahui informasi didalamnya.

Adapun proses enkripsi dan dekripsi dalam algoritma *caesar cipher* dapat dilihat pada gambar ini

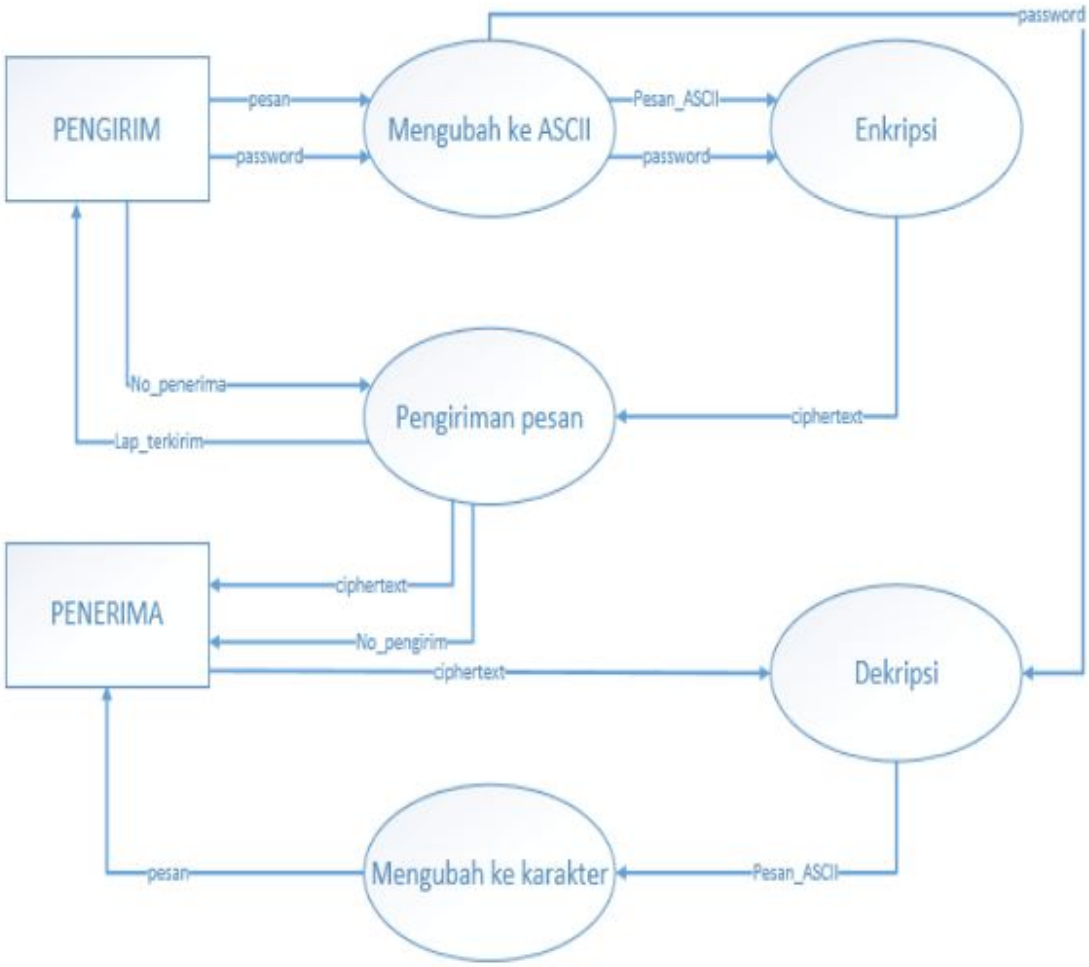


Flow Chart Sistem kerja enkripsi

Flow Chart sistem kerja dekripsi



Data flow diagram Sistem enkripsi dan dekripsi



Jadwal Pembuatan

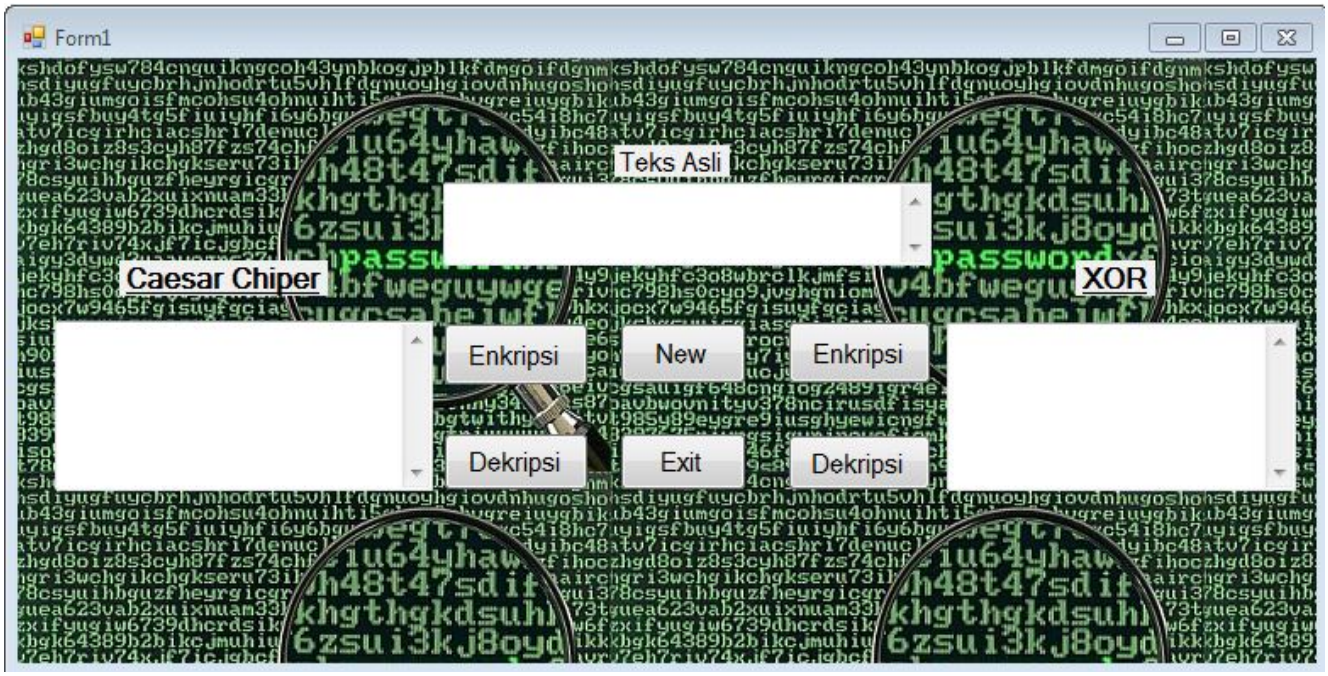
No.	Uraian Kegiatan	Juni 2017		Juli 2017				Agustus 2017			
		Minggu		Minggu				Minggu			
		3	4	1	2	3	4	1	2	3	4
1	Tahap Perencanaan										
2	Tahap Analisa										
3	Tahap Design										
4	Tahap Coding										
5	Tahap Pengujian										

Pembuatan Program

a. Menu Toolbox yang digunakan :

Toolbox	Properties
Label1	Text : Teks Asli
Label2	Text : Caesar Chiper
Label3	Text : XOR
Text1	Name : txtinput
Text2	Name : txtcaesar, Scrollbars: Vertical
Text3	Name : txtxor, Scrollbars: Vertical
Button1	Name : cmdenkripcaesar, Text : Enkripsi
Button2	Name : cmddeskripcaesar, Text : Dekripsi
Button3	Name : cmdenkripxor, Text : Enkripsi
Button4	Name : cmddekripxor, Text : Dekripsi
Button5	Name : cmdnew, Text : New
Button6	Name : cmdexit, Text : Exit

b. Design



6.c. Coding

menggunakan Visual studio 2005, ada 1 Form dan 2 Module

```
Imports System.IO
Imports System.Security
Imports System.Security.Cryptography

Public Class Form1
    Dim codedes As Short
    Dim codeenkrip As Short
    Private Enum CryptoAction
        actionEncrypt = 1
        actionDecrypt = 2
    End Enum

Private Sub Form1_Load(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles MyBase.Load
        cmddeskripcaesar.Enabled = False
        cmddeskripxor.Enabled = False
    End Sub

    Private Sub Button1_Click(ByVal sender As System.Object, ByVal
e As System.EventArgs) Handles cmdenkripcaesar.Click
        Dim Enkripsi As New kripto2
        Dim strcode As String
        Try
            strcode = InputBox("Masukkan Kode Enkripsi")
            If strcode = "" Then Exit Sub 'jika klik cancel
            'simpen kode di variabel codeenkrip
            codeenkrip = strcode
        Finally
        End Try
        txtcaesar.Text                                          =
Enkripsi.KryptografiEnkripsi(txtinput.Text)
        cmddeskripcaesar.Enabled = True
    End Sub
    Public Function EnkripsiXOR(ByVal Kode As String, ByVal DataIn
As String) As String
        Dim XOR1, XOR2 As Integer
        Dim OuputStr As String
        Dim longData As Long
        For longData = 1 To Len(DataIn)
            XOR1 = Asc(Mid$(DataIn, longData, 1))
            'Nilai kedua berasal dr kata kunci
            XOR2 = Asc(Mid$(Kode, ((longData Mod Len(Kode)) + 1),
1))
            OuputStr = OuputStr + Chr(XOR1 Xor XOR2)
        Next longData
        EnkripsiXOR = OuputStr
    End Function

    Private Sub Button2_Click(ByVal sender As System.Object, ByVal
e As System.EventArgs) Handles cmddeskripcaesar.Click
        Dim Dekripsi As New kripto2
```

```
            Dim strcode As String
            Try
                strcode = InputBox("Masukkan Kode Deskripsi")
                If strcode = "" Then Exit Sub 'if cancel clicked
                'simpen text dg encription scheme
                If strcode = codeenkrip Then
                    txtcaesar.Text                                    =
Dekripsi.KryptografiDekripsi(txtcaesar.Text)
                End If
            Finally
            End Try
        End Sub

        Private Sub Button3_Click(ByVal sender As System.Object, ByVal
e As System.EventArgs) Handles cmdenkripxor.Click
            Dim strKode As String
            If txtinput.Text = "" Then
                MsgBox("Masukkan nilai yang akan di-enkripsi")
            Else
                strKode = InputBox("Masukkan kode sebagai kunci", "Kunci
Enkripsi")
            End If

            If strKode = 0 Then
                MsgBox("Masukkan nilai yang akan di-enkripsi")
                strKode = InputBox("Masukkan kode sebagai kunci", "Kunci
Enkripsi(")
            End If

            If strKode = 1 And strKode = "" Then
                MsgBox("Masukkan nilai yang akan di-enkripsi")
                strKode = InputBox("Masukkan kode sebagai kunci", "Kunci
Enkripsi(")
            End If
            txtxor.Text = EnkripsiXOR(strKode, txtinput.Text)

            cmddeskripxor.Enabled = True
        End Sub

        Private Sub Button4_Click(ByVal sender As System.Object, ByVal
e As System.EventArgs) Handles cmddeskripxor.Click
            Dim strKode As String
            If txtinput.Text = "" Then
                MsgBox("Masukkan nilai yang akan di-enkripsi")
            Else
                strKode = InputBox("Masukkan kode sebagai kunci", "Kunci
Enkripsi")
            End If

            If strKode = 0 Then
                MsgBox("Masukkan nilai yang akan di-enkripsi")
                strKode = InputBox("Masukkan kode sebagai kunci", "Kunci
Enkripsi(")
            End If

            If strKode = 1 And strKode = "" Then
```

```
            MsgBox("Masukkan nilai yang akan di-enkripsi")
            strKode = InputBox("Maukkan rangkaian kode sebagai
kunci", "Kunci Enkripsi(")
        End If
        txtxor.Text = EnkripsiXOR(strKode, txtxor.Text)

    End Sub
  Private Sub Button6_Click_1(ByVal sender As System.Object, ByVal
e As System.EventArgs) Handles cmdexit.Click
        End
    End Sub

    Private Sub Button5_Click_1(ByVal sender As System.Object, ByVal
e As System.EventArgs) Handles cmdnew.Click
        txtcaesar.Text = ""
        txtinput.Text = ""
        txtxor.Text = ""
        cmddeskripcaesar.Enabled = False
        cmddeskripxor.Enabled = False
    End Sub
End Class


Module Kripto2
Public Class kripto2
    Inherits Krypto1
End Class
```

4. PENUTUP

Kesimpulan

Berdasarkan hasil uraian ini, dapat disimpulkan bahwa :

1. Dari tugas yang diberikan menghasilkan sebuah aplikasi Enkripsi-Deksripsi menggunakan Metode Caesar chiper dan Xor.
2. Dengan adanya aplikasi ini, dapat meningkatkan keamanan pesan, dimana pesan sudah terenkripsi.

DAFTAR PUSTAKA

Ariyus Dony 2008. Pengantar Ilmu Kriptografi Teori Analisis dan Implementasi. Yogyakarta : C.V Andi Offset

Komputer Wahana, 2010 ,The Best Encryption Tools, Jakarta : Elex Media Komputindo

Santoso harip, 2004. Vb.net Utk .net Programmer. Jakarta : Elex Media Komputindo