

# JIT

ISSN : 1979-9292

## JURNAL IPTEKS TERAPAN

Volume 4 No. 1 April 2010

**KAJIAN PENYUSUNAN PROGRAM PEMBANGUNAN WILAYAH  
PERBATASAN SUMATERA BARAT – BENGKULU**

*Ansofino*

**HUBUNGAN ANTARA PENYAKIT KARIES GIGI DAN PERIODONTAL  
DENGAN PENYAKIT JANTUNG PADA PASIEN JANTUNG DI RSUP DR. M. DJAMIL PADANG**

*Dhona Afriza*

**PENERAPAN TEKNOLOGI INKUBASI SP-36 DALAM PUPUK KANDANG  
PADA BUDIDAYA TANAMAN JAHE (*Zingiber officinale* Rosc)  
DI DESA BATU BUSUK KECAMATAN PAUH, KOTA PADANG**

*Enjoni*

**PENERAPAN KRIPTOGRAFY UNTUK KEAMANAN DATA**

*Harun Mukhtar*

**PROSES PEREKRUTAN TENAGA KERJA DALAM  
INDUSTRI KONSTRUKSI DI INDONESIA**

*Rahmat*

**PROFESIONALISME TENAGA PENDIDIK DALAM PENDIDIKAN INKLUSIF**

*Salman M. Noer*

**SINERGI KEPEMIMPINAN BARAT DAN ISLAM SERTA IMPLIKASINYA  
DALAM PENDIDIKAN**

*Syafnan*

**PERTUMBUHAN DAN PRODUKSI PADI PADA SAWAH GAMBUT  
SAPRIS DENGAN BEDA UMUR TANAM**

*Widodo Haryoko*

**SELEKSI VARIETAS PADI BERBIJI BERNAS PADA SAWAH GAMBUT**

*Widodo Haryoko, Kasli, Irfan Suliansyah,  
Auzar Syarif dan Teguh Budi Prasetyo*

**ISLAM DAN PENDIDIKAN (Perspektif Filosofis)**

*Muslim*

**PENGELOLAAN LINGKUNGAN UNTUK PENGENDALIAN BANJIR**

*Skunda Diliarosta*



**Kopertis Wilayah X  
Sumbar, Riau, Jambi & Kepri**

## PENERAPAN KRIPTOGRAFY UNTUK KEAMANAN DATA

---

*Harun Mukhtar*

### ABSTRAK

*Kriptografy merupakan seni pengkodean yang sangat berguna untuk mengamankan data baik data pada komputer pribadi maupun data pada komputer jaringan yang terkoneksi dengan jaringan global Internet, seni Kriptografy jua dapat diterapkan pada pengiriman data lewat internet seperti email, dengan diterapkannya seni bela diri kriptografy pencurian data akan terbatas hal ini dikarenakan pencuri akan mempunyai kerjaan tambahan untuk membaca pengkodean dari sebuah persandian data tersebut. dalam jurnal ini penerapan kriptografy dengan menggunakan metoda RC4 dan digabungkan dengan metoda biasa yang disebut exor, sistem keamanan dari enkripsi data ini tergantung pada kerahasiaan key bagi pemilik bukan tergantung pada algoritmanya. pengkodean dalam sistem yang dibangun harus dilengkapi dengan Deskripsi, deskripsi adalah suatu istilah untuk mengembalikan data kebentuk semula sehingga dapat dibaca kembali.*

*Kata kunci : Kriptografy, Enkripsi, Deskripsi*

### PENDAHULUAN

Perkembangan Teknologi Informasi yang begitu cepat berdampak pada pandangan manusia dan organisasi untuk berubah. Perubahan tersebut dimulai dari pikir manusia yang cenderung untuk maju dalam penguasaan teknologi. Teknologi ini disebut dengan Internet dan Jaringan Komunikasi yang berbasis pada penggunaan komputer, dengan adanya Internet tersebut berbagai macam layanan komunikasi disajikan seperti *web, e-mail, milis, newsgroups* dan sebagainya. Dengan semakin maraknya pemanfaatan layanan komunikasi Internet tersebut, maka permasalahan baru bermunculan apalagi ditambah dengan adanya *hacker* dan *cracker* yang justru

mengganggu kenyamanan pengguna internet. Banyak pengguna yang merasa terganggu oleh adanya orang-orang yang tak bertanggung jawab tersebut dengan menyiasati pengamanan komunikasi yang dikomunikasikannya, atau menyiasati dengan cara menjaga keaslian dari informasi yang diterimanya.

Berdasarkan hal ini muncul berbagai bidang ilmu pengkodean dalam pengiriman pesan diantaranya Kriptografi, Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan yang dikirim dari satu tempat ke tempat lain. Bidang ilmu kriptografi saat ini mulai digemari oleh banyak orang karena dengan menguasai seni dan tekni kriptografi seseorang akan dapat menjaga komputernya sendiri tanpa harus mengeluarkan modal besar jika dibandingkan menyewa atau membeli software khusus untuk keamanan data.

### Pengenalan Masalah

Ketika seseorang atau sekelompok orang maupun perusahaan atau instansi bermaksud untuk berkomunikasi dengan rekan-rekan bisnisnya atau siapa saja yang diinginkan, dan dalam berkomunikasi tersebut mengandung informasi yang bersifat rahasia sehingga tidak semua orang boleh mengetahuinya, sudahlah pasti membutuhkan sistem yang dapat melindungi kerahasiaan data dan pesan tersebut. Dokumen ataupun data biasanya dikirimkan melalui *e-mail* lewat internet, namun tidak dapat dipungkiri bahwasannya internet merupakan *Public network* sehingga memiliki resiko yang amat besar untuk diakses oleh orang yang tidak berhak. Dengan demikian dibutuhkan sistem yang mampu meminimalisasi kebocoran informasi penting yang sangat rahasia dan rawan jika diketahui oleh orang lain yang tidak berhak.

Pesan sebelum dikirim lewat *e-mail* Internet, terlebih dahulu dikodekan dengan cara mengacak secara random sehingga menghasilkan pesan berupa simbol- simbol atau kode-kode acak yang tidak dimengerti maksud dan tujuannya. Pesan berupa kode-kode inilah yang kemudian dikirimkan melalui jalur komunikasi yakni *e-mail* yang merupakan salah satu fasilitas internet yang cukup handal dalam pengiriman pesan ke penerima yang memang berhak mendapatkan pesan tersebut. Dalam membaca pesan rahasia yang telah dikirimkan penerima haruslah merubah kode-kode tersebut kedalam

bentuk asli sehingga pesan tersebut dapat dibaca kembali. Dalam melakukan proses perubahan tersebut diperlukan sebuah kunci atau kata sandi yang sama dengan kata sandi atau *key* milik pengirim pesan.

Dengan demikian dibutuhkan sebuah program aplikasi yang mampu merubah pesan dengan cara mengkodekan pesan secara random terhadap pesan rahasia sebelum dikirimkan melalui jalur komunikasi yang dikenal dengan *e-mail* ke penerima dan program tersebut juga harus mampu mengembalikan kode-kode yang terbentuk kedalam pesan asli agar dapat dibaca oleh penerima pesan tersebut.

### SISTEM YANG DIHARAPKAN

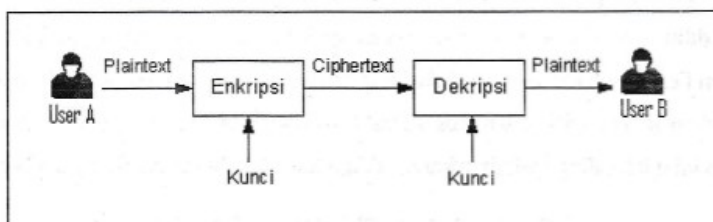
Berdasarkan pengenalan masalah yang telah diuraikan diatas, maka sistem yang akan dibangun harus memenuhi harapan dari semua pengguna, harapan tersebut diuraikan sebagai berikut :

1. Sistem berfungsi sebagai media untuk menyediakan fasilitas dalam proses pengkodean pesan, sehingga pesan tersebut tidak dapat dibaca oleh orang yang tidak dikehendaki oleh pengirim pesan (Enkripsi).
2. Sistem juga berfungsi mengembalikan pesan pengkodean ke bentuk pesan asli dengan menyamakan kata sandi (*key*), sehingga pesan tersebut dapat dibaca kembali (Deskripsi).
3. Sistem yang akan dibangun ini memiliki program utama yang terdiri dari Enkripsi Teks, dan Enkripsi File. Enkripsi Teks berguna untuk mengenkrip file berextension (.txt dan .rtf) yakni mampu mengenkrip teks yang diketikkan dalam Teks Editor pada menu utama. Enkripsi File berguna mengenkrip file secara langsung tanpa harus membuka file tersebut dengan hanya melihat nama file yang ingin dienkrip. document yang dienkrip haruslah dokumen teks berextension doc (.doc atau .txt).
4. Sistem yang dibangun ini juga mempunyai fasilitas tambahan yang sangat berarti dalam menjalankan aktifitas diinternet, fasilitas tersebut ialah mampu melakukan *browsing* dengan fungsi mirip dengan Microsoft Internet Explorer.

## DESAIN DAN REKAYASA SISTEM

Desain dan Rekayasa yang akan diuraikan meliputi arsitektur sistem yang akan dibangun, Diagram aliran data yang diperlukan ialah Diagram Konteks, Data Flow Diagram dari proses-proses program, Bagan Alir (*flowchart*) yang menunjukkan aliran sistem dan Rancangan Antar Muka Program. Gambar dibawah ini akan menunjukkan Arsitektur aplikasi yang akan dibangun, Arsitektur Aplikasi ini mensimulasi penggunaan sistem yang dilakukan oleh dua orang berbeda dan pada tempat berbeda yang tidak saling berhubungan. User A melakukan Enkripsi data pada komputer si A, kemudian User melakukan Deskripsi data pada komputer si B dengan key yang dimiliki oleh si A.

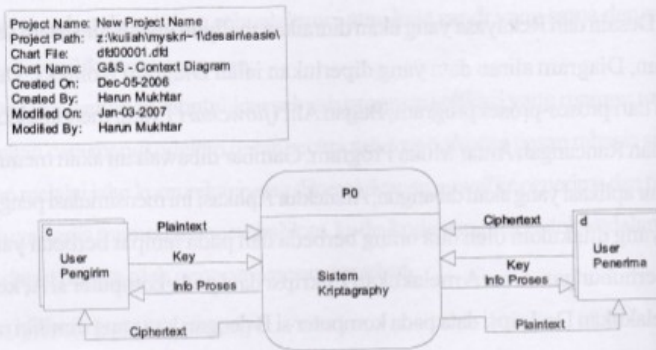
Gambar 1. Arsitektur Sistem



Program aplikasi yang dirancang memiliki kemampuan dalam memfasilitasi pengguna dalam dua proses utama yakni :

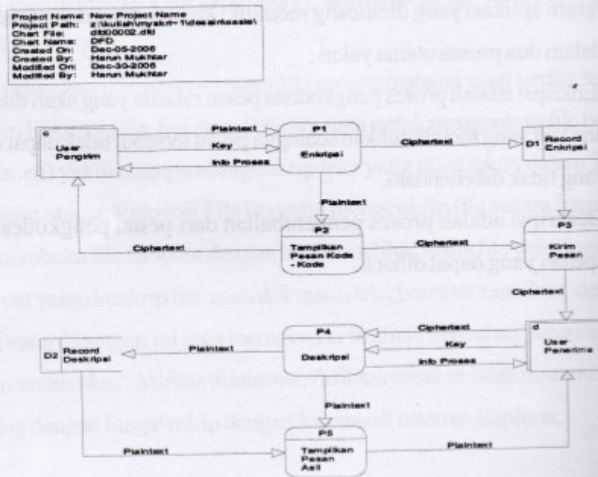
1. Proses Enkripsi adalah proses pengkodean pesan rahasia yang akan dikirimkan ke pengguna lain yang membutuhkan sehingga pesan tersebut tidak dapat dibaca oleh orang yang tidak dikehendaki.
2. Proses Deskripsi adalah proses pengembalian dari pesan pengkodean kedalam bentuk pesan yang dapat dibaca.

Gambar 2. Diagram Konteks



Pada Diagram Konteks atau sering juga disebut Diagram Aliran Data level 0, dapat dilihat aliran sistem informasi secara garis besarnya. Proses yang terjadi dalam Sistem Pesan Rahasia ini terdiri dari dua proses utama, yaitu proses Enkripsi yang dilakukan oleh Pengirim, dan proses Deskripsi yang dilakukan oleh Penerima. Kedua proses ini tidak saling berkaitan karena dilakukan oleh dua orang user yang berbeda

Gambar 3. Data Flow Diagram level 1



Gambar diatas merupakan gambaran secara detail dari sistem yang dibuat. Sistem terdiri dari dua proses utama seperti yang telah dijelaskan sebelumnya yaitu proses Enkripsi dan proses Deskripsi, sementara itu proses menampilkan pesan baik pesan kode-kode maupun pesan Asli merupakan proses tambahan dalam program. Proses pengiriman pada Data Flow Diagram level 1 merupakan proses diluar sistem.

Proses Enkripsi merupakan proses menyandikan pesan secara random yang menghasilkan pesan dalam bentuk kode-kode yang tidak dapat dipahami dan tidak dapat dibaca. Proses Deskripsi merupakan proses mengubah kembali dari pesan kode-kode ke pesan asli sehingga dapat dibaca kembali. Untuk memperjelas prosedur yang terjadi dari kedua proses tersebut, penulis membuat suatu bagan alir program (*flowchart*). *Flowchart* berguna untuk memberikan gambaran aliran program atau prosedur sistem secara logika.

#### DIAGRAM ALIR (FLOWCHART)

Bagan Alir Program (*program flowcart*) merupakan suatu bahan yang menggambarkan arus logika dari data yang akan diproses dalam suatu program dari awal sampai akhir. Diagram Alir yang digambarkan disini terbagi menjadi dua Diagram Alir yaitu Diagram Alir Program Enkripsi dan Diagram Alir Program Deskripsi. Diagram Alir ini merupakan gambaran proses yang terjadi didalam kedua Diagram Alir ini, Diagram Alir lainnya adal Diagram Fungsi RC4, Diagram Alir EnkripXOR dan Diagram Alir DeskripXOR.

Diagram Alir Program Enkripsi diatas diawali dengan menuliskan plainteks dan kemudian dilanjutkan dengan proses enkripsi, sebelum melakukan proses enkrip dengan xor dan metoda RC4 sistem medeteksi plainteks dan key yang ada, jika tidak ditemukan maka sistem akan melakukan perulangan sampai plainteks dan kunci ditemukan, begitu plainteks dan kunci ditemukan sistem melanjutkan proses enkripsi dengan fungsi EnkripXOR kemudian hasil dari enkrip fungsi EnkripXor dienkrip kembali dengan menggunakan fungsi RC4. setelah melakukan proses enkripsi sistem melakukan pemecahan jumlah karakter atau panjang chiperteks, dengan demikian proses enkripsi

selesai ditandai dengan berakhirnya proses program. Fungsi RC4 merupakan fungsi untuk merubah pesan kedalam kode-kode yang tidak dimengerti.

Gambar 4. Diagram Alir Program Enkripsi

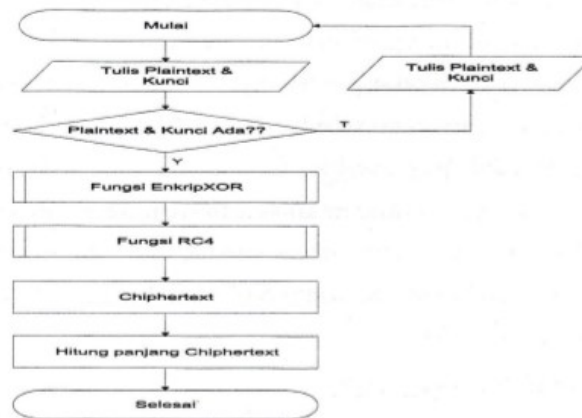
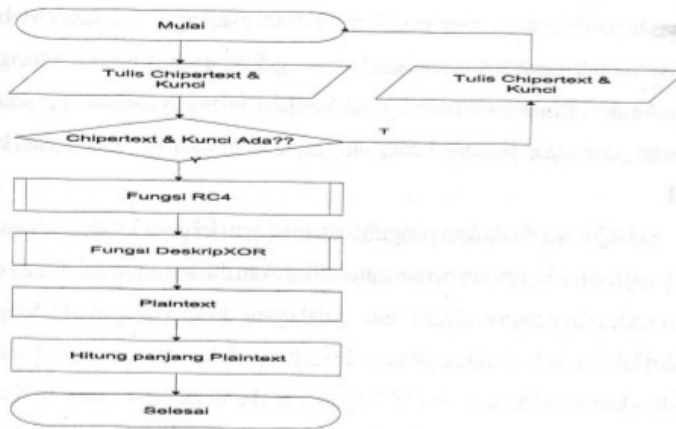


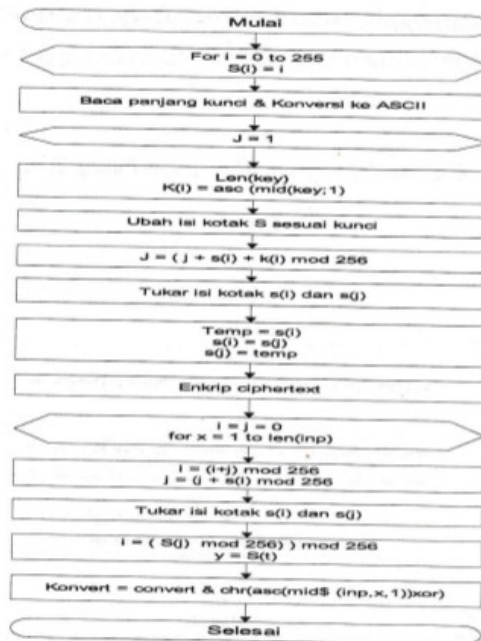
Diagram Alir Program Diskripsi dibawah ini diawali dengan menuliskan chiperteks dan kunci kemudian dilanjutkan dengan proses deskripsi, proses deskripsi merupakan kebalikan dari proses enkripsi diatas fungsi yang digunakan juga sama yaitu fungsi RC4 namun untuk fungsi Xor berbeda yakni dengan menggunakan fungsi DeskripXOR. Proses dialukan dengan cara mendeskrip pesan yang terenkrip dengan fungsi RC4 selanjutnya hasil dari deskrip dengan fungsi RC4 di deskrip kembali dengan menggunakan fungsi DeskripXOR



Gambar 5. Diagram Alir Program Deskripsi



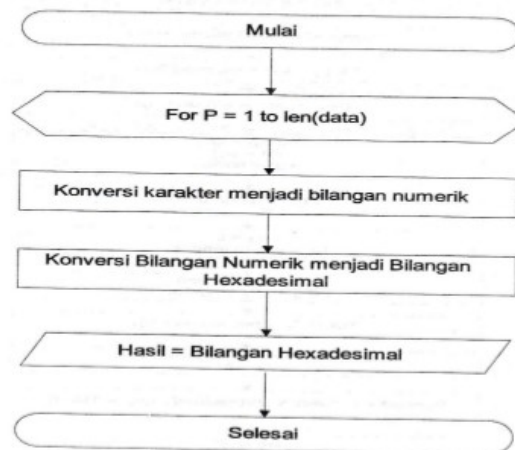
Gambar 6. Diagram Alir Fungsi RC4



Pembentukan fungsi RC4 diawali dengan menerjemahkan panjang I yang merupakan panjang dari program enkrip tersebut, panjang adalah jumlah table yang digunakan untuk menentukan panjang byte yang diinginkan, semakin panjang jumlah table maka akan semakin sulit untuk jebol. Setelah panjang byte ditentukan selanjutnya dilakukan pembacaan panjang kunci yang digunakan sekaligus melakukan konversi ASCII.

Selanjutnya dilakukan perubahan nilai atau isi pada kotak S sesuai dengan kunci yang telah ada, setelah pemindahan dilakukan dilakukan pertukan isi kotak  $S(i)$  ke  $J(i)$  untuk selanjutnya dilakukan enkrip data yang dikenal dengan istilah ciphertext. Setelah dilakukan enkrip pada ciphertext dilakukan pertukaran kembali untuk selanjutnya dilakukan konversi karakter ASCII dengan mengkombinasikan ke mode Xor, proses sudah selesai dan mendapatkan hasil berupa kode-kode yang tidak dapat dimengerti oleh manusia dan juga oleh computer itu sendiri. Agar dapat melakukan pembacaan maka harus dilakukan perubahan kembali ke bentuk semula dengan cara sama seperti saat melakukan enkrip ciphertext hal ini disebut dengan deskripsi dan datanya disebut plaintext.

Gambar 7. Diagram Alir Fungsi Enkrip XOR



Pada gambar diatas dijelaskan diagram alir fungsi enkripsi dengan melakukan perubahan ke bilangan hexadesimal, istilah yang dipakai dalam buku ini adalah EnkripXor, Istilah ini memang tidak ada pada teknik pemrograman kriptografi namun tidak salah jika kita mau memberi istilah sendiri karena memang teknik ini belum memiliki nama yang pasti. Teknik ini dimulai dengan melakukan pembacaan panjang data yang akan dienkrip, selanjutnya dilakukan konversi karakter menjadi blangan numeric, setelah menjadi bilangan numeric dilakukan konversi lagi menjadi bilangan hexadecimal, hasil dari konversi terakhir adalah bilangan heksa decimal.

Gambar 8. Diagram Alir Fungsi DeskripXOR

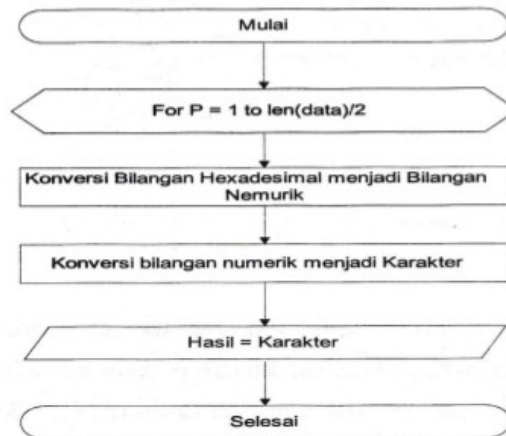


Diagram alir diatas ini merupakan diagram dengan hasil terbalik dari diagram alir sebelumnya, diagram alir ini disebut diagram alir fungsi deskripsi dengan menggunakan fungsi xor, deskripsi ini diberi nama DeskripXor hamper sama dengan EnkripXor hanya bedanya fungsinya saja kalo EnkripXor berguna untuk mengenkrip data sedangkan DeskripXor berfungsi untuk mendeskrip data.

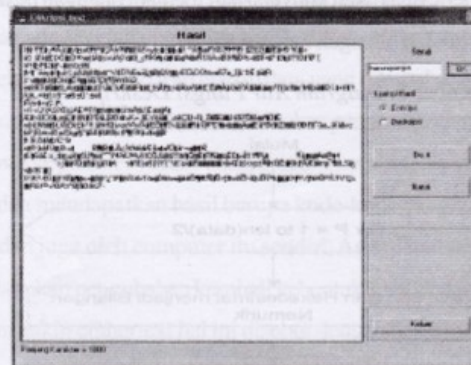
Program deskripxor dimulai dengan pembacaan panjang data yang sudah dienkrip untuk dilakukan deskripsinya, setelah dilakukan pembacaan panjang data maka selanjutnya dilakukan konversi dari bilangan hexadecimal menjadi bilangan numeric,

selanjutnya dikonversi kembali menjadi karakter dengan demikian hasil yang didapat berupa karakter seperti sebelum dilakukan enkripsi.

### PENERAPAN KRIPTOGRAFY PADA TEKS

Form ini adalah form antar muka user yang berguna untuk mengenkrip data teks yang telah diketikkan pada Form Utama

Gambar 9. Enkripsi Teks



Teks yang telah terenkrip diletakkan pada teks yang sama, yakni sebagai pengganti teks sebelumnya. Enkripsi teks dan deskripsi teks memiliki fungsi yang sama yaitu akan berfungsi jika user sudah menuliskan kata sandi sebagai *Key* pada sistem Enkripsi Teks.

Do it berfungsi untuk mengembalikan teks baik yang telah terenkrip maupun telah dideskrip ke menu utama yakni pada tipe Teks Editor. Enkripsi dan deskripsi akan berjalan jika fungsi enkrip pada modul telah berjalan normal, pada program ini terdiri dari 3 fungsi yang berguna untuk enkrip dan deskrip teks file dan gambar, yaitu Enkrip dengan metoda Xor, deskrip dengan metoda Xor, dan Fungsi RC4 yang diketikkan pada modul program. Dibawah ini dijelaskan prosedur fungsi dari ketiga fungsi tersebut. Ketiga fungsi ini listingnya diletakkan pada modul program CRC4.BAS

```
Function EnskripXOR(Kode As String, data As String) As String
    Dim Putar As Long
    Dim DataKeluar As String
    Dim temp As Integer
    Dim tempstring As String
    Dim Nilai1 As Integer
    Dim Nilai2 As Integer
    For Putar = 1 To Len(data)
        Nilai1 = Asc(Mid$(data, Putar, 1))
        Nilai2 = Asc(Mid$(Kode, ((Putar Mod Len(Kode)) + 1), 1))
        temp = (Nilai1 Xor Nilai2)
        tempstring = Hex(temp)
        If Len(tempstring) = 1 Then tempstring = "0" & tempstring
        DataKeluar = DataKeluar + tempstring
    Next Putar
    EnskripXOR = DataKeluar
End Function
```

Prosedur FungsiXOR diatas ini menggunakan fungsi Asc untuk mengubah karakter menjadi angka (bilangan numerik), kemudian dengan fungsi aritmatika xor dihasilkan suatu bilangan, kemudian bilangan tersebut dikonversi kedalam bilangan heksadesimal dengan menggunakan fungsi hex. Kesemua data yang akan dienkrip dilakukan per karakter menggunakan fungsi mid\$.

```
Function DeskripXOR(Kode As String, data As String) As String
    Dim Putar As Long
    Dim DataKeluar As String
    Dim Nilai1 As Integer
    Dim Nilai2 As Integer
    For Putar = 1 To (Len(data) / 2)
```

```
    Nilai1 = Val("&H" & (Mid$(data, (2 * Putar) - 1, 2)))
    Nilai2 = Asc(Mid$(Kode, ((Putar Mod Len(Kode)) + 1), 1))
    DataKeluar = DataKeluar + Chr(Nilai1 Xor Nilai2)
Next Putar
DeskripXOR = DataKeluar
End Function
```

Prosedur fungsi DeskripXOR merupakan kebalikan dari prosedur fungsi EnkripXOR, yakni melakukan pengubahan dari kode Hexsadesimal menjadi bilangan numerik. Untuk selanjutnya dengan Xor terhadap bilangan dari kata kunci dihasilkan suatu bilangan yang kemudian diubah menjadi karakter. Setelah selesai melakukan proses pada salah satu fungsi diatas baik EnkripXOR maupun DeskripXOR selanjutnya program akan melakukan proses pada fungsi RC4, listing programnya dapat diperhatikan dibawah ini:

```
Public Function cRC4(inp As String, key As String) As String
On Error Resume Next
Dim S(0 To 255) As Byte, K(0 To 255) As Byte, i As Long
Dim j As Long, temp As Byte, Y As Byte, t As Long, x As Long
Dim Outp As String
For i = 0 To 255
S(i) = i
Next
j = 1
For i = 0 To 255
If j > Len(key) Then j = 1
K(i) = Asc(Mid(key, j, 1))
j = j + 1
Next i
j = 0
```

```
For i = 0 To 255
j = (j + S(i) + K(i)) Mod 256
temp = S(i)
S(i) = S(j)
S(j) = temp
Next i
i = 0
j = 0
For x = 1 To Len(inp)
i = (i + 1) Mod 256
j = (j + S(i)) Mod 256
temp = S(i)
S(i) = S(j)
S(j) = temp
t = (S(i) + (S(j) Mod 256)) Mod 256
Y = S(t)
Outp = Outp & Chr(Asc(Mid(inp, x, 1)) Xor Y)
Next
cRC4 = Outp
End Function
```

Fungsi ini menggunakan perulangan (*loop*) yakni For...Next yang artinya membuat kenaikan, kenaikan yang dimaksudkan bisa saja kenaikan plus maupun minus tergantung dari kebutuhan. Program diatas ini menjelaskan Inisialisasi S didalam larik  $S_0, S_1, \dots, S_{255}$ , dalam program Visual Basic 6.0 dituliskan sebagai berikut :

```
For i = 0 To 255
S(i) = i
Next
```

Selanjutnya proses akan melakukan penambahan *byte* semu (*padding*), jika panjang kunci tidak mencapai 256 *byte* sehingga panjang kunci menjadi 256 *byte*, misal kunci dilanbangan dengan U kecil dari 256, maka akan ditambah *byte* semu sampai panjang *byte* mencapai 256. setelah itu proses melakukan permutasi terhadap nilai – nilai dalam larik S dengan perintah sebagai berikut :

```
j = 0
For i = 0 To 255
j = (j + S(i) + K(i)) Mod 256
temp = S(i)
S(i) = S(j)
S(j) = temp
Next i
```

Setelah proses selesai langkah terakhir dari fungsi RC4 ialah membangkitkan aliran kunci (*keystream*) dan melakukan enkrip. Proses pembangkitan aliran-aliran kunci dipilih dengan mengambil nilai S(i) dan S(j) dan menjumlahkan dengan modulo 256. hasil penjumlahan adalah indeks t sedemikian sehingga S(t) menjadi kunci – aliran K yang kemudian digunakan untuk mengenkrip plainteks ke idx. prosedur untuk membangkitkan kunci dan sekaligus mengenkripsi sebagai berikut :

```
i = 0
j = 0
For x = 1 To Len(inp)
i = (i + 1) Mod 256
j = (j + S(i)) Mod 256
temp = S(i)
S(i) = S(j)
S(j) = temp
t = (S(i) + (S(j) Mod 256)) Mod 256
Y = S(t)
```



```
Outp = Outp & Chr(Asc(Mid(inp, x, 1)) Xor Y)
Next
```

Demikian uraian prosedur fungsi enkripsi baik menggunakan Xor maupun RC4, fungsi ini dapat digunakan untuk mengenkrip semua jenis data hanya tinggal pengembangannya saja dalam suatu aplikasi. Prosedur yang perlu ditambahkan pada Form Enkripsi Teks terletak pada *Command Ok*, hal ini diperlukan untuk memberikan perintah kepada program agar melakukan tugas sesuai yang diinginkan pengguna. Sebelum mengklik tombol Ok perlu dilakukan pilihan pada *Option*, *Option* yang disediakan terdiri dari 2 pilihan yakni enkripsi dan deskripsi, selain itu juga user harus memasukkan kata kunci sesuai yang diinginkan, prosedur yang diperlukan dalam program sebagai berikut :

```
Private Sub Command1_Click()
If Text1 = "" Then
    MsgBox ("masukkan sandinya.... gitulo !!")
    Exit Sub
Else
    If Option1.Value = True Then
        RTF1.Text = EnskripXOR(Text1.Text, RTF1.Text)
        hEnkrip = cRC4(RTF1.Text, Text1)
        RTF1.Text = hEnkrip
        Label3.Caption = "Panjang Karakter = " & Len(RTF1.Text)
    Else
        hdeskrip = cRC4(RTF1.Text, Text1)
        RTF1.Text = hdeskrip
        RTF1.Text = DeskripXOR(Text1.Text, RTF1.Text)
        Label3.Caption = "Panjang Karakter = " & Len(RTF1.Text)
    End If
End If
End Sub
```

Prosedur ini mempunyai fungsi untuk mengubah teks pada RTF1. Text kedalam bentuk kode-kode yang tidak dapat dibaca kemudian dikembalikan ke bentuk semula dengan menggunakan kunci yang sama. Program ini berjalan setelah melakukan dua kali proses pada prosedur fungsi, yakni fungsi Xor dan RC4. Teks yang telah dienkrip maupun yang telah dideskrip dihitung penjang karakternya dengan menggunakan perintah &Len, sehingga pengguna mengetahui jumlah karakter yang telah terenkrip maupun dideskrip.

### KESIMPULAN

Dari penjelasan yang telah disajikan diatas sebelumnya mengenai teknik pengacakan data yang disebut kriptography dapat diambil kesimpulan sebagai berikut:

1. Kriptography modern merahasiakan kunci (key) saja tanpa harus menjaga algoritmanya, artinya keamanan data atau pesan tidak tergantung pada algoritmanya tetapi tergantung pada kerahasiaan kunci yang dimilikinya.
2. Ukuran panjang key pada fungsi RC4 sangat berguna untuk mengamankan data, semakin panjang byte yang digunakan akan semakin sulit untuk dipecahkan.
3. Telah berhasil dibangun suatu aplikasi yang dapat digunakan untuk mengenkrip data atau pesan yang akan dikirimkan kepengguna lain yang membutuhkan ataupun untuk keperluan pribadi.
4. Aplikasi ini juga masih memiliki kekurangan yakni pada ekripsi file, hal ini dikarenakan kemungkinan kerusakan pada file yang telah dienkrip sangat besar. Kemungkinan kerusakan ini dikarenakan tidak adanya file cadangan hal ini disebabkan ketidak mampuan aplikasi dalam membuat file berexstention baru.

---

**DAFTAR PUSTAKA**

- Aji, R.Kresno, Hartato, Agus, Siswanto, Denny, Chandra Wiratama, Tommy, (2002), *Kejahatan Internet, Trik Aplikasi dan Penanggulangannya*, Elex Media Komputindo Kelompok Gramedia, Jakarta
- Amperiyanto, Tri, (2003), *Bermain – main dengan Internet*, Elex Media Komputindo Kelompok Gramedia, Jakarta
- Arius, Doni, (2006), *Computer Security*, Andi, Yogyakarta
- Hadi, Rahadian, (2001), *Pemrograman Windows API dengan Microsoft Visual Basic*, Elex Media Komputindo Kelompok Gramedia, Jakarta
- Kristanto, Andri, (2003), *Keamanan Data Pada Jaringan Komputer*, Gava Media, Yogyakarta
- Kristanto, Andri, (2003), *Perancangan Sistem Informasi dan Aplikasinya*, Gava Media, Yogyakarta
- Kristanto, Andri, (2003), *Jaringan komputer*, Gava Media, Yogyakarta
- Kurniawan, Yusuf, (2004), *Kriptografi, Keamanan Internet dan Jaringan Komunikasi*, Informatika, Bandung