Subject: APGAR cipher to C#/VB.Net
Posted by halo2pac on Mon, 26 Jan 2009 00:28:50 GMT
View Forum Message <> Reply to Message

A few others and I are attempting to convert the XWISP APGAR Cipher into C#/Vb.Net, we are very close but are stuck.

We need to Convert this:
Perl:

```
sub apgar_enc {
  my @v = map ord, split //, shift;
  my @r;
  my $U="abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789./";
  for (my $i = 0; $i < 8; $i++) {
    my $a = $v[$i];
    my $index=(($a & 1
                ? $a << ($a & 1) & $v[8-$i]
                : $a ^ $v[8-$i])
                & 0x3f);
    push @r, substr($U,$index,1)
  }
  join '', @r;
}
```

Into VB.Net or C#.

I have attempted both, resulting on a circle of problems.

My VB.Net Tries:

#1

```
"CODE"    Private Function apgar(ByVal pass As String) As String
        If pass.Length = 8 Then
            Dim v(7)
            Dim j As Integer
            For j = 0 To 7
                v(j) = pass.Substring(j, 1)
            Next

            Dim r As String = "" '  my @r;

            Dim U As String =
"abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789"
            Dim i As Integer
            For i = 0 To 7
                Dim a As String = v(i)
                Dim temp As Long
                If (Asc(a) And 1) Then
```

```
            temp = Asc(a) << (Asc(a) And 1) And Asc(v(7 - i))
        Else
            temp = Asc(a) Xor Asc(v(7 - i))
        End If
        Dim index As Integer = (temp And 63)
        r &= U.Substring(index, 1) 'push @r, substr($U,$index,1)
    Next

    Return r
  End If
End Function
```

#2

```
"CODE"    Private Function apgar2(ByVal pass As String) As String
    If pass.Length = 8 Then
        Dim v(7) As String
        Dim j As Integer
        For j = 0 To 7
            v(j) = pass.Substring(j, 1)
        Next

        Dim c As String =
"abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789"
        Dim u(61) As String
        Dim s As Integer
        For s = 0 To 61
            u(s) = c.Substring(s, 1)
        Next

        Dim r As String = "" '  my @r;

        Dim i As Integer = 0

        While i < 8
            Dim left As String = v(i)
            Dim right As String = v(UBound(v) - i)

            Dim l As Integer
            If (Asc(left) And 1) Then
                l = ((Asc(left) << 1) Xor (Asc(left) And 1)) And Asc(right)
            Else
                l = Asc(left) Xor Asc(right)
            End If

            r &= u(l And 63)

            i += 1
```

```
            End While

            Return r
        End If
    End Function

#3
"CODE"    Private Function apgar(ByVal pass As String) As String
        '       sub apgar_enc { # Convert plaintext pass to apgar crypted format for XWIS
        '  my @v = map ord, split //, shift;
        '  my @r;
        '  my
$U="abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789./";
        '  for (my $i = 0; $i < 8; $i++) {
        '    my $a = $v[$i];
        '    my $index=(($a & 1
        '                ? $a << ($a & 1) & $v[8-$i]
        '                : $a ^ $v[8-$i])
        '                & 0x3f);
        '    push @r, substr($U,$index,1)
        '  }
        '           Join() '', @r;
        '}
        If pass.Length = 8 Then
            Dim v(7)
            Dim j As Integer
            For j = 0 To 7
                v(j) = pass.Substring(j, 1)
            Next

            ' Dim v() As String = Split(pass, "") '  my @v = map ord, split //, shift
            Dim r As String = "" '  my @r;

            Dim U As String =
"abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789"
            Dim i As Integer
            For i = 0 To 7
                Dim a As String = v(i)
                Dim temp As Integer
                If (AscW(a) And 1) Then
                    temp = AscW(a) << (AscW(a) And 1) And AscW(v(7 - i))
                Else
                    temp = AscW(a) Xor AscW(v(7 - i))
                End If
                Dim index As Integer = (temp And 63)
                r &= U.Substring(index, 1) 'push @r, substr($U,$index,1)
            Next
```

```
        Return r
      End If
   End Function
```

C# - By Aca20031

```
"CODE"using System;
using System.Collections.Generic;
//using System.Linq;
using System.Text;


namespace apgar
{
   public class Encryptor
   {
        const string chars =
@"abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789./";
        public static string Encrypt(string data)
        {
           string result = "";
           char[] array = data.ToCharArray();
           for (int i = 0; i < 8; i++)
           {
              byte left = (byte)(array[i] & 0xFF);
              byte right, x;
              if (i == 0)
                 right = 0;
              else
                 right = (byte)(array[data.Length - i]);

              x = (left & 1) == 1 ? (byte)(((left << 1) ^ (left & 1)) & right) : (byte)(left ^ right);
              //Console.WriteLine(x & 63);
              result += chars.Substring(x & 63, 1);

           }
           return result;
        }
   }
}
```

C# Mixed mine and Aca's

#1

```
"CODE"using System;
using System.Collections.Generic;
```

```
//using System.Linq;
using System.Text;

namespace apgar
{
   public class Encryptor
   {
      const string chars =
@"abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789./";
      public static string Encrypt(string data)
      {
         string result = "";
         char[] array = data.ToCharArray();
         for (int i = 0; i < 8; i++)
         {
            byte left = (byte)(array[i] & 0xFF);
            byte right, x;
            if (i == 0)
               right = 0;
            else
               right = (byte)(array[data.Length - i]);

            x = (left & 1) == 1 ? (byte)(((left << 1) ^ (left & 1)) & right) : (byte)(left ^ right);

            result += chars.Substring(x & 63, 1);

         }
         return result;
      }
   }
}

#2
"CODE"       public static string Encrypt(string data)
      {
         char[] array = data.ToCharArray(); //my @v = map ord, split //, shift;
         string r = "";
         const string U =
"abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789./";
         for (int i = 0; i < 8; i++)
         {
            char a = array[i]; //my $a = $v[$i];
            int index;
            if (((int)a & 1) == 1)
            {
               index = (a << (a & 1) & array[7 - i]) & 0x3f;
            }
            else
```

```
            {
                index = (a ^ array[7 - i]) & 0x3f;
            }

            r += U.Substring(index, 1);
        }
        return r;
    }

#3
"CODE"      public static string Encrypt(String str)
    {
        String u =
"abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789./";
        Char[] v = str.ToCharArray();
        String r = String.Empty;

        for (Int16 i = 0; i < 8; i++)
        {
            Char a = v[i];
            Boolean b = Convert.ToBoolean(a & 1);
            Int32 index = (b ? a << (a & 1) & v[7 - i] : a ^ v[7 - i]) & 0x3f;
            r += u.Substring(index, 1);
        }

        return r;
    }

#4
"CODE"using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;

namespace Ren_Encryption___Perl_to_CSharp {
   public class Encryptor {
      const string chars =
@"abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789./";
      public static string Encrypt(string data) {
         string result = "";
         char[] array = data.ToCharArray();
         for (int i = 0; i < 8; i++) {
            char c = array[i];
            //  my $index=(($a & 1
            //? $a << ($a & 1) & $v[8-$i]
            //: $a ^ $v[8-$i])
            //& 0x3f);
```

```
            int index = (((((int)c) & 1) != 0 ? (((int)c) << (((int)c) & 1)) & array[8-i] : (((int)c) ^
array[8-i])) & 0x3F);
            //   push @r, substr($U,$index,1)
            result += chars.Substring(index, 1);

         }
         return result;
      }
   }
}
```

Dave's C# Code:

```
"CODE"/// <summary>
/// Xwis Password Encryption
/// </summary>
static String apgar(String str) {
   String u = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789./";
   Char[] v = str.ToCharArray();
   String r = String.Empty;

   for (Int16 i = 0; i < 8; i++) {
      Char a = v[i];
      Boolean b = Convert.ToBoolean(a & 1);
      Int32 index = (b ? a << (a & 1) & v[7 - i] : a ^ v[7 - i]) & 0x3f;
      r += u.Substring(index, 1);
   }

   return r;
}
```

small rainbow table of values:

```
Pass entered | APGAR | What Aca's (#1) code does
aaaaaaaa aaaaaaaa abbbbbbb
aaaaaaa1 aaaaaaaG abbbbbbH
zzzzzzzz 6aaaaaaa 6aaaaaaa
password WaIMMsbf WaINNtbf
AbCdEfGh akgcacck akhcbcdk
99999999 aWWWWWWW aXXXXXXX
chicken1 azcecchG azcfddhG
```

We would really appreciate if Blazer, DanPaul, or anyone could help.

Subject: Re: APGAR cipher to C#/VB.Net

I think this will work in VB:

```
    Private Function apgar(ByVal pass As String) As String
        If pass.Length = 8 Then
            Dim v(7)
            Dim j As Integer
            For j = 0 To 7
                v(j) = pass.Substring(j, 1)
            Next

            Dim r As String = "" '  my @r;

            Dim U As String =
"abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789./"
            Dim i As Integer
            For i = 0 To 7
                Dim t1 as integer
                If i = 0 Then
                  t1 = 0
                Else
                  t1 = Asc(v(8 - i))
                End If
                Dim a As String = v(i)
                Dim temp As Long
                If (Asc(a) And 1) Then
                    temp = (Asc(a) << 1) And t1
                Else
                    temp = Asc(a) Xor t1
                End If
                Dim index As Integer = (temp And 63)
                r &= U.Substring(index, 1) 'push @r, substr($U,$index,1)
            Next

            Return r
        End If
    End Function
```

First you missed the ./ off the end of the string U. It needs to be 64 characters long.

Second, the "7 - i" should have read "8 - i" like in the original Perl.

Third, the "8-$i" in the original Perl points to the null terminator when $i is zero (for a string s that is 8 characters long, s[8] returns the null terminator). So Asc(8-i) when i = 0 needs to return 0, as in my revised version.

Fourth, a small optimisation: since we only ever get to this line

temp = Asc(a) << (Asc(a) And 1) And Asc(v(7 - i))

if Asc(a) And 1 = 1, I replaced the former by the latter.

I tested it on some of the strings in your table and it looks to be working.

Hope that helps

CarrierII's brother (ahydra)

Subject: Re: APGAR cipher to C#/VB.Net
Posted by halo2pac on Mon, 26 Jan 2009 21:09:10 GMT
View Forum Message <> Reply to Message

CarrierII wrote on Mon, 26 January 2009 09:30First you missed the ./ off the end of the string U. It needs to be 64 characters long.
thought that was some sort of Perl escape thingy.

CarrierII wrote on Mon, 26 January 2009 09:30Second, the "7 - i" should have read "8 - i" like in the original Perl.

Third, the "8-$i" in the original Perl points to the null terminator when $i is zero (for a string s that is 8 characters long, s[8] returns the null terminator). So Asc(8-i) when i = 0 needs to return 0, as in my revised version.

ya I was wondering why there was an 8. (this is why im not coding my stuff in perl :S)

CarrierII wrote on Mon, 26 January 2009 09:30Fourth, a small optimization: since we only ever get to this line

temp = Asc(a) << (Asc(a) And 1) And Asc(v(7 - i))

if Asc(a) And 1 = 1, I replaced the former by the latter.
beautiful! I think I tried that at some point (i didnt paste all 600 attempts :S) but I screwed up on other areas.

CarrierII wrote on Mon, 26 January 2009 09:30I tested it on some of the strings in your table and it looks to be working.
IT WORKS!

CarrierII wrote on Mon, 26 January 2009 09:30Hope that helps
Immensely.

CarrierII wrote on Mon, 26 January 2009 09:30CarrierII's brother (ahydra)
Well thank you very much ahydra.

This has to be the toughest thing I have ever attempted to code.

Also thanks much to the following people who helped me and aca20031:
Roshambo
Zack
Dave
Ghostshaw
... I hope I am not forgetting anyone.. if i am... pm me and I will thank you xD
