

Forum:[Hack Forums](#)

Thread: [Help with XTEA Cryption](#)

0van - August 29, 2011, 4:59 am

Hey,

can someone help me with my XTEA Code?

Code Public Class XTea

Private Shared f_key As UInteger()

Public Sub New(ByVal password As String)

MsgBox(password)

f_key = FormatKey(password)

End Sub

Public Function Encrypt(ByVal input As String) As String

If input.Length = 0 Then

Throw New ArgumentException("Invalid input length!")

End If

If input.Length Mod 2 <> 0 Then

input += ControlChars.NullChar

End If

Dim dataBytes As Byte() = System.Text.ASCIIEncoding.ASCII.GetBytes(input)

Dim cipher As String = String.Empty

Dim tempData As UInteger() = New UInteger(1) {}

For i As Integer = 0 To dataBytes.Length - 1 Step 2

tempData(0) = dataBytes(i)

tempData(1) = dataBytes(i + 1)

code(tempData, f_key)

cipher += ConvertUIntToString(tempData(0)) + ConvertUIntToString(tempData(1))

Next

Return cipher

End Function

Public Function Decrypt(ByVal Data As String) As String

Dim x As Integer = 0

Dim tempData As UInteger() = New UInteger(1) {}

Dim dataBytes As Byte() = New Byte((Data.Length \ 8) * 2 - 1) {}

For i As Integer = 0 To Data.Length - 1 Step 8

tempData(0) = ConvertStringToUInt(Data.Substring(i, 4))

tempData(1) = ConvertStringToUInt(Data.Substring(i + 4, 4))

decode(tempData, f_key)

dataBytes(x) = CByte(tempData(0))

x += 1

dataBytes(x) = CByte(tempData(1))

x += 1

```

Next
Dim decipheredString As String = System.Text.ASCIIEncoding.ASCII.GetString(dataBytes, 0,
dataBytes.Length)
If decipheredString(decipheredString.Length - 1) = ControlChars.NullChar Then
    decipheredString = decipheredString.Substring(0, decipheredString.Length - 1)
End If
Return decipheredString
End Function

```

```

Private Shared Function FormatKey(ByVal Key As String) As UInteger()
    If Key.Length <= 5 Then
        Throw New ArgumentException("Key must be between 6 and 16 characters in length")
    End If

```

```

    Key = Key.PadRight(16, "c").Substring(0, 16)

```

```

    Dim formattedKey As UInteger() = New UInteger(4) {}

```

```

    Dim j As Integer = 0
    For i As Integer = 0 To Key.Length - 1 Step 4
        formattedKey(j) = ConvertStringToUInt(Key.Substring(i, 4))
        j += 1
    Next
    Return formattedKey
End Function

```

```

Private Shared Sub code(ByVal v As UInteger(), ByVal k As UInteger())

```

```

    Dim y As UInteger = v(0)
    Dim z As UInteger = v(1)
    Dim sum As UInt64 = 0
    Dim delta As UInteger = &H9E3779B9UI

```

```

    For i = 0 To 31
        y += (z << 4 Xor z >> 5) + z Xor sum + k(sum And 3)
        sum += delta
        [color=#FF0000]z += (y << 4 Xor y >> 5) + y Xor sum + k(sum >> 11 And 3)[/color]
    Next

```

```

    v(0) = y
    v(1) = z
End Sub

```

```

Private Shared Sub decode(ByVal v As UInteger(), ByVal k As UInteger())

```

```

    Dim y As UInteger = v(0)
    Dim z As UInteger = v(1)
    Dim sum As UInteger = &HC6EF3720UI
    Dim delta As UInteger = &H9E3779B9UI

```

```

    For i = 0 To 31
        [color=#FF0000]z -= (y << 4 Xor y >> 5) + y Xor sum + k(sum >> 11 And 3)[/color]
        sum -= delta
        y -= (z << 4 Xor z >> 5) + z Xor sum + k(sum And 3)
    Next

```

```
v(0) = y
v(1) = z
End Sub
```

```
Private Shared Function ConvertStringToUInt(ByVal Input As String) As System.UInt32
    Dim output As UInt32
    output = Convert.ToUInt32(Input(0))
    output += (Convert.ToUInt32(Input(1)) << 8)
    output += (Convert.ToUInt32(Input(2)) << 16)
    output += (Convert.ToUInt32(Input(3)) << 24)
    Return output
End Function

Private Shared Function ConvertUIntToString(ByVal Input As System.UInt32) As String
    Dim output As New System.Text.StringBuilder()
    output.Append(Convert.ToChar(Input And &HFF))
    output.Append(Convert.ToChar((Input >> 8) And &HFF))
    output.Append(Convert.ToChar((Input >> 16) And &HFF))
    output.Append(Convert.ToChar((Input >> 24) And &HFF))
    Return output.ToString()
End Function
```

End Class

Error:

Quote:Do not divide with 0!

Modestep - August 29, 2011, 5:46 am

(Aug 29, 2011 04:59 AM)Ovan Wrote: [\[CITE\]](#) Hey,
can someone help me with my XTEA Code?

Code Public Class XTea

```
    Private Shared f_key As UInteger()
```

```
    Public Sub New(ByVal password As String)
```

```
        MsgBox(password)
```

```
        f_key = FormatKey(password)
```

```
    End Sub
```

```
    Public Function Encrypt(ByVal input As String) As String
```

```
        If input.Length = 0 Then
```

```
            Throw New ArgumentException("Invalid input length!")
```

```
        End If
```

```
        If input.Length Mod 2 <> 0 Then
```

```
            input += ControlChars.NullChar
```

```
        End If
```

```
        Dim dataBytes As Byte() = System.Text.ASCIIEncoding.ASCII.GetBytes(input)
```

```
        Dim cipher As String = String.Empty
```

```
        Dim tempData As UInteger() = New UInteger(1) {}
```

```
        For i As Integer = 0 To dataBytes.Length - 1 Step 2
```

```
            tempData(0) = dataBytes(i)
```

```

tempData(1) = dataBytes(i + 1)
code(tempData, f_key)
cipher += ConvertUIntToString(tempData(0)) + ConvertUIntToString(tempData(1))
Next

```

```

Return cipher
End Function

```

```

Public Function Decrypt(ByVal Data As String) As String
Dim x As Integer = 0
Dim tempData As UInteger() = New UInteger(1) {}
Dim dataBytes As Byte() = New Byte((Data.Length \ 8) * 2 - 1) {}
For i As Integer = 0 To Data.Length - 1 Step 8
tempData(0) = ConvertStringToUInt(Data.Substring(i, 4))
tempData(1) = ConvertStringToUInt(Data.Substring(i + 4, 4))
decode(tempData, f_key)
dataBytes(x) = CByte(tempData(0))
x += 1
dataBytes(x) = CByte(tempData(1))
x += 1
Next
Dim decipheredString As String = System.Text.ASCIIEncoding.ASCII.GetString(dataBytes, 0,
dataBytes.Length)
If decipheredString(decipheredString.Length - 1) = ControlChars.NullChar Then
decipheredString = decipheredString.Substring(0, decipheredString.Length - 1)
End If
Return decipheredString
End Function

```

```

Private Shared Function FormatKey(ByVal Key As String) As UInteger()
If Key.Length <= 5 Then
Throw New ArgumentException("Key must be between 6 and 16 characters in length")
End If

```

```

Key = Key.PadRight(16, "c").Substring(0, 16)

```

```

Dim formattedKey As UInteger() = New UInteger(4) {}

```

```

Dim j As Integer = 0
For i As Integer = 0 To Key.Length - 1 Step 4
formattedKey(j) = ConvertStringToUInt(Key.Substring(i, 4))
j += 1
Next
Return formattedKey
End Function

```

```

Private Shared Sub code(ByVal v As UInteger(), ByVal k As UInteger())
Dim y As UInteger = v(0)
Dim z As UInteger = v(1)
Dim sum As UInt64 = 0
Dim delta As UInteger = &H9E3779B9UI

```

```

For i = 0 To 31

```

```

y += (z << 4 Xor z >> 5) + z Xor sum + k(sum And 3)
sum += delta
[color=#FF0000]z += (y << 4 Xor y >> 5) + y Xor sum + k(sum >> 11 And 3)[/color]
Next

```

```

v(0) = y
v(1) = z
End Sub

```

```

Private Shared Sub decode(ByVal v As UInteger(), ByVal k As UInteger())
Dim y As UInteger = v(0)
Dim z As UInteger = v(1)
Dim sum As UInteger = &HC6EF3720UI
Dim delta As UInteger = &H9E3779B9UI

```

```

For i = 0 To 31
[color=#FF0000]z -= (y << 4 Xor y >> 5) + y Xor sum + k(sum >> 11 And 3)[/color]
sum -= delta
y -= (z << 4 Xor z >> 5) + z Xor sum + k(sum And 3)
Next

```

```

v(0) = y
v(1) = z
End Sub

```

```

Private Shared Function ConvertStringToUInt(ByVal Input As String) As System.UInt32
Dim output As UInt32
output = Convert.ToUInt32(Input(0))
output += (Convert.ToUInt32(Input(1)) << 8)
output += (Convert.ToUInt32(Input(2)) << 16)
output += (Convert.ToUInt32(Input(3)) << 24)
Return output
End Function

```

```

Private Shared Function ConvertUIntToString(ByVal Input As System.UInt32) As String
Dim output As New System.Text.StringBuilder()
output.Append(Convert.ToChar(Input And &HFF))
output.Append(Convert.ToChar((Input >> 8) And &HFF))
output.Append(Convert.ToChar((Input >> 16) And &HFF))
output.Append(Convert.ToChar((Input >> 24) And &HFF))
Return output.ToString()
End Function

```

End Class

Error:

Isn't the error explaining it all? Do not divide by zero

Banks? - August 29, 2011, 5:48 am

It means you must have a key. Without a key, the data cannot be encrypted, nor decrypted.

Ovan - August 29, 2011, 8:15 am

I've got a key!

And i don't know where i divide by zero -."

