

Forum:[Hack Forums](#)

Thread: [\[VB.NET\] XTEA Encryption \[Source\]](#)

d3c0mpil3r - November 13, 2010, 5:42 am

XTEA Encryption

I am back :)

XTEA is TEA's precursor. This is based on TEA Encryption with little improvements. More info can be found [here!](#)

Source :

Code Public Class XTea

'Leave a thanks....

'- decompiler

Private Shared f_key As UInteger()

Public Sub New(ByVal password As String)

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, " ").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 UInteger = 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
    z += (y << 4 Xor y >> 5) + y Xor sum + k(sum >> 11 And 3)
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
    z -= (y << 4 Xor y >> 5) + y Xor sum + k(sum >> 11 And 3)
    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

Output :

[img]http://ploader.net/files/743101b5744d2c56f961988109d931e8.gif[/img]

Note : You need to input a password between 6 (or 7 char min.) to 16 (max.) for this to work.

Enjoy!?

Big mess there! Sorry guys...

DarkShadowz - November 13, 2010, 6:40 am

Hm, could you try to decrease the amount of code? Just wondering if that was possible as people would like to use this in their crypter, and they would like small stubs xD.

tang77 - November 13, 2010, 6:50 am

Nice... but it's create a lot of chars...

This Girl Is On Fire - November 13, 2010, 8:43 am

How hard would this be to crack? Bruteforce etc..

Grieve™ - November 13, 2010, 8:53 am

very nice decompiler thanks for this!

Mr. Anderson - November 13, 2010, 8:57 am

oh wow this is epic! thanks!

d3c0mpil3r - November 13, 2010, 9:43 am

Thanks everyone, RC6 is what I am working. Hope I can get it working :)

(Nov 13, 2010 07:40 AM)DarkShadowz Wrote: [\[CITE\]](#) Hm, could you try to decrease the amount of code? Just wondering if that was possible as people would like to use this in their crypter, and they would like small stubs xD.

I gave the source. Now its up to you how you optimize the code :)

(Nov 13, 2010 09:43 AM)exprezzed Wrote: [\[CITE\]](#) How hard would this be to crack? Bruteforce etc.. You can salt the encryption. That will make it even stronger. But choose a random password or something and you are good to go.

D0T. - November 13, 2010, 10:04 am

(Nov 13, 2010 07:40 AM)DarkShadowz Wrote: [\[CITE\]](#) Hm, could you try to decrease the amount of code? Just wondering if that was possible as people would like to use this in their crypter, and they would like small stubs xD.

Just create a DLL, would drastically decrease the amount of code, and would make it easier to feature this in crypters and such.

Mr. Anderson - November 13, 2010, 10:32 am

Can I port this to C#? I will give credits.

d3c0mpil3r - November 14, 2010, 3:37 am

(Nov 13, 2010 11:32 AM)Mr. Anderson Wrote: [\[CITE\]](#) Can I port this to C#? I will give credits. Yes you can.

Convert it in C# or use a DLL.

memesbro - November 18, 2010, 7:57 pm

nicee, is this polymorphic?

d3c0mpil3r - November 19, 2010, 1:53 am

(Nov 18, 2010 08:57 PM)Chity Snipa Wrote: [\[CITE\]](#) nicee, is this polymorphic? This isn't a polymorphic encryption.

You can modify it to get a different output every time and call it polymorphic ?

klusbert - December 24, 2010, 2:05 pm

trying to use this to encrypt and decrypt tibia packets.

I set up a test app to just test the functions.
I do Like this.

```
Key = New UInteger(5) {}  
Packet = New UInteger(10) {}
```

```
For i As Integer = 0 To 5  
    Key(i) = i
```

```
Next
For i As Integer = 5 To 10
    Packet(i) = i
Next
XTea.code(Packet, Key)
```

This get me overflowed everytime.

EDIT:
Same thing with only string. and I use encrypt.

GodWall - December 24, 2010, 2:11 pm

Very nice work as always bro :)

d3c0mpil3r - December 25, 2010, 2:26 am

(Dec 24, 2010 03:05 PM)klusbert Wrote: [\[CITE\]](#) trying to use this to encrypt and decrypt tibia packets.

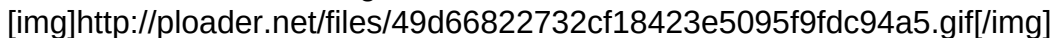
Spoiler ([Click to View](#))

I set up a test app to just test the functions.
I do Like this.

```
Key = New UInteger(5) {}
Packet = New UInteger(10) {}
```

```
For i As Integer = 0 To 5
    Key(i) = i
Next
For i As Integer = 5 To 10
    Packet(i) = i
Next
XTea.code(Packet, Key)
```

This get me overflowed everytime.

EDIT:
Same thing with only string. and I use encrypt.
Disable overflow checking :


Gingin - December 25, 2010, 2:41 am

Here's the XTEA functions in C#, in case someone needs them. For third party developers, you'll have to read they key from the clients memory.

```
Code public unsafe static bool XteaEncrypt(ref byte[] buffer, ref int length, int index, uint[] key)
{
    if (key == null)
        return false;

    int msgSize = length - index;

    int pad = msgSize % 8;
    if (pad > 0)
    {
```

```

msgSize += (8 - pad);
length = index + msgSize;
}

fixed (byte* bufferPtr = buffer)
{
uint* words = (uint*)(bufferPtr + index);

for (int pos = 0; pos < msgSize / 4; pos += 2)
{
uint x_sum = 0, x_delta = 0x9e3779b9, x_count = 32;

while (x_count-- > 0)
{
words[pos] += (words[pos+1] << 4 ^ words[pos+1] >> 5) + words[pos+1] ^ x_sum
+ key[x_sum & 3];
x_sum += x_delta;
words[pos+1] += (words[pos] << 4 ^ words[pos] >> 5) + words[pos] ^ x_sum
+ key[x_sum >> 11 & 3];
}
}
}

return true;
}

public unsafe static bool XteaDecrypt(ref byte[] buffer, ref int length, int index, uint[] key)
{
if (length <= index || (length - index) % 8 > 0 || key == null)
return false;

fixed (byte* bufferPtr = buffer)
{
uint* words = (uint*)(bufferPtr + index);
int msgSize = length - index;

for (int pos = 0; pos < msgSize / 4; pos += 2)
{
uint x_count = 32, x_sum = 0xC6EF3720, x_delta = 0x9E3779B9;

while (x_count-- > 0)
{
words[pos + 1] -= (words[pos] << 4 ^ words[pos] >> 5) + words[pos] ^ x_sum
+ key[x_sum >> 11 & 3];
x_sum -= x_delta;
words[pos] -= (words[pos + 1] << 4 ^ words[pos + 1] >> 5) + words[pos + 1] ^ x_sum
+ key[x_sum & 3];
}
}
}

length = (int)(BitConverter.ToUInt16(buffer, index) + 2 + index);
return true;
}

```

d3v1l401 - July 15, 2011, 7:14 am

dude,i fkin love you!

i was searching exactly for this!

Marcusramse1 - July 15, 2011, 10:04 am

Nice encryption :D I tried to make one once.. Failed.

INFA?OUS - July 15, 2011, 10:09 am

Great share! thanks for this :D

d3c0mpil3r - July 15, 2011, 10:15 am

No problem guys.

btwXXTEA Encryption ([Click to View](https://hackforums.net/showthread.php?tid=993836))<https://hackforums.net/showthread.php?tid=993836>

felicixus - July 15, 2011, 7:17 pm

Wonderful job. Great man. You are just great :)

IsraX0r - July 16, 2011, 3:49 am

Very nice, I suggest you to make it polymorphic to make it even better.

INFA?OUS - July 16, 2011, 7:57 am

im getting an error..

Code Public Class Form1

Dim xtea As XTea

Private Sub Button1_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)

Handles Button1.Click

xtea = New XTea(TextBox3.Text)

TextBox2.Text = xtea.EncryptString(TextBox1.Text)

End Sub

the error is...

Code Error 1 'EncryptString' is not a member of 'XTea_Encryption.XTea'.

Any thoughts?

d3c0mpil3r - July 16, 2011, 10:01 am

(Jul 16, 2011 07:57 AM)INF4MOUS Wrote: [\[CITE\]](#) im getting an error..

Code Public Class Form1

Dim xtea As XTea

Private Sub Button1_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)

Handles Button1.Click

xtea = New XTea(TextBox3.Text)

TextBox2.Text = xtea.EncryptString(TextBox1.Text)

End Sub

the error is...

Code Error 1 'EncryptString' is not a member of 'XTea_Encryption.XTea'.

Any thoughts?

Their is no method named 'EncryptString'. Read the source!

You call it like:

Code Dim x as new XTea("password")

x.Encrypt("data_to_encrypt")

Ovan - August 11, 2011, 10:39 am

Could you help me?

I have a file encrypted with XTEA and I have the key, but when I want to decrypt the file I ever get an Overflow Error :/

Ethereal - August 11, 2011, 10:43 am

(Nov 13, 2010 06:42 AM)d3c0mpil3r Wrote: [CITE](#) XTEA is TEA's precursor.

XTEA = Extended TEA, so its a subsequent version, not a precursor ^^

Aside from that, it looks okay. Above poster gravedug, by the way.

Stenography - October 8, 2011, 5:49 am

Epic encryption..

Now trying how add this to my crypter and delete that gay detectable rc4.