

Re: Total confused and need help with small encryption and decryption methods

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.languages.csharp/2007-04/msg00414.html>

- *From:* rossum <rossum48@xxxxxxxxxxxx>
 - *Date:* Tue, 03 Apr 2007 21:06:12 +0100
-

On 3 Apr 2007 10:18:00 -0700, manmit.walia@xxxxxxxx wrote:

Hello Everyone,

Long time ago, I posted a small problem I had about converting a VB6 program to C#. Well with the help with everyone I got it converted. But I overlooked something and don't understand why it is doing this. Below is my code, I would be greatfull if someone can guide me through the right path or even help me solve this issue.

Problem: The old tool which was written in VB6 works perfect. But I needed to convert this to C# using since there are new tools we are creating that would like to leverage this style of security. The problem is that the encryption method is not working as it should. The decryption method works perfect. Just having problems with the encryption part.

Test Values:

Current Encrypted Value – 0835262B27
Value returned using Decrypt method – anna

Current Decrypted Value – anna
Value returned using Encrypted method – 35262B27

*** As you can see the encryption method is returning something different then the original encrypted value. *** PLEASE HELP !!! ***

CODE:

```
static byte[] ParseHex(string text)
{
    byte[] ret = new byte[text.Length / 2];
    for (int i = 0; i < ret.Length; i++)
    {
        ret[i] = Convert.ToByte(text.Substring(i * 2, 2), 16);
    }
    return ret;
}
```

Re: Total confused and need help with small encryption and decryption methods

```
}
```

```
public static string Decrypt("THEFELDGROUP", string encrypted)
```

This line does not compile. You probably should have written something like:

```
public static string Decrypt(string password, string encrypted)
```

```
{
byte[] binary = ParseHex(encrypted);
char[] chars = new char[binary.Length];
for (int i = 0; i < chars.Length; i++)
{
chars[i] = (char)(binary[i] ^ password[i % password.Length]);
}
return new string(chars);
}
```

```
public static string Encrypt("THEFELDGROUP", string strG)
```

Again this line does not compile:

```
public static string Encrypt(string strPass, string strG)
```

```
{
char[] cHexDigits = {
'0', '1', '2', '3', '4', '5', '6', '7',
'8', '9', 'A', 'B', 'C', 'D', 'E', 'F'
};

// the encoded integer value of the current character in the string
byte byteEncoded;

System.Text.StringBuilder sbReturned = new
System.Text.StringBuilder();

for (int i = 0; i < strG.Length; ++i)
{
// encode the current character
byteEncoded = (byte)(((int)strG[i] ^ ((int)strPass[i %
strPass.Length]));

// output the Hex character value of the above encoded value
sbReturned.Append(cHexDigits[byteEncoded >>
4]).Append(cHexDigits[byteEncoded & 0xF]);
}
```

Re: Total confused and need help with small encryption and decryption methods

Re: Total confused and need help with small encryption and decryption methods

```
}  
  
return sbReturned.ToString();  
}
```

Your code does not have the "08" because you are encoding a four character plaintext into a four byte (= 8 hex digits) cyphertext. I suggest you have a close look at the VB original to see where the initial "08" comes from, then you need to reproduce that in your C# version. We do not have enough information here to see its origin.

Your encryption scheme, a stream cypher with a repeating key, is not very secure. Good enough to deter casual observation but easily breakable by anyone seriously interested. Repeating any part of the keystream is a big weakness for any stream cypher.

rossum

.