

Re: DES Decrypt Not Working

Source: <http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.general/2004-05/2679.html>

From: Jon Skeet [C# MVP] (skeet_at_pobox.com)

Date: 05/27/04

Date: Thu, 27 May 2004 08:58:07 +0100

JustMe <andrewpery@hotmail.com> wrote:

> My code (in VB.Net) will encrypt data fine (I guess...) but when I try
> to decrypt it, it returns the exact same byte array that I passed to
> *be* decrypted! Your advice would be most appreciated. My code is
> pretty simple (too simple?)....

```
>  
> Function EncryptData(ByVal bData() As Byte) As Byte()  
> Dim eDES As New DESCryptoServiceProvider  
> Dim eMS As New MemoryStream(bData.Length)  
> Dim EncStr As New CryptoStream(eMS, _  
> eDES.CreateEncryptor(DESKey, DESiv),  
> CryptoStreamMode.Write)  
> EncStr.Write(bData, 0, bData.Length)  
> EncStr.FlushFinalBlock()  
> Dim bResult(eMS.Position) As Byte  
> eMS.Position = 0  
> eMS.Read(bResult, 0, bResult.Length)  
> EncStr.Close()  
> eMS.Close()  
> eDES.Clear()  
> Return bResult  
> End Function  
>  
> Function DecryptData(ByVal bData() As Byte) As String  
> Dim DES As New DESCryptoServiceProvider  
> Dim MS As New MemoryStream(bData.Length)  
> Dim DecStr As New CryptoStream(MS, _  
> DES.CreateDecryptor(DESKey, DESiv),  
> CryptoStreamMode.Read)  
> MS.Write(bData, 0, bData.Length)  
> DecStr.FlushFinalBlock()  
> MS.Position = 0  
> Dim Ret As String = New StreamReader(MS).ReadToEnd  
> DecStr.Close()  
> MS.Close()  
> DES.Clear()  
> Return Ret  
> End Function
```

microsoft.public.dotnet.general: Re: DES Decrypt Not Working

Well, you're relying on Stream.Read returning all the bytes you requested in one chunk, which is in general unsafe but should be okay with a MemoryStream. The MemoryStream.ToArray method makes it easier to get the data in a MemoryStream, to be honest.

I note that you're decrypting to a string though, having *encrypted* a byte array. This could well be part of the problem – was the data to be encrypted a UTF-8 encoded version of a string?

--

Jon Skeet - <skeet@pobox.com>

<http://www.pobox.com/~skeet>

If replying to the group, please do not mail me too