

Re: Encrypt and Decrypt a file using .NET 2.0?

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.languages.csharp/2007-04/msg03237.html>

- *From:* "William Stacey [C# MVP]" <william.stacey@xxxxxxxxxx>
 - *Date:* Mon, 23 Apr 2007 22:17:20 -0400
-

Works over here. Well with text files. It is not a good sample. Try something more like:

```
using System;
using System.IO;
using System.Security;
using System.Security.Cryptography;
using System.Runtime.InteropServices;
using System.Text;

namespace Demo
{
    public class Class1
    {
        // Call this function to remove the key from memory after use for
        security
        [System.Runtime.InteropServices.DllImport("KERNEL32.DLL", EntryPoint
        = "RtlZeroMemory")]
        public static extern bool ZeroMemory(IntPtr Destination, int
        Length);

        // Function to Generate a 64 bits Key.
        public static string GenerateKey()
        {
            // Create an instance of Symetric Algorithm. Key and IV is
            generated automatically.
            DESCryptoServiceProvider desCrypto =
            (DESCryptoServiceProvider)DESCryptoServiceProvider.Create();

            // Use the Automatically generated key for Encryption.
            return ASCIIEncoding.ASCII.GetString(desCrypto.Key);
        }

        public static void EncryptFile(string sInputFilename, string
        sOutputFilename, string sKey)
        {
            DESCryptoServiceProvider DES = new DESCryptoServiceProvider();
```

Re: Encrypt and Decrypt a file using .NET 2.0?

```
using (FileStream inFile = new FileStream(sInputFilename,
    FileMode.Open, FileAccess.Read) )
using (FileStream outFile = new FileStream(sOutputFilename,
    FileMode.Create, FileAccess.Write))
using (ICryptoTransform desencrypt =
    DES.CreateEncryptor(Encoding.ASCII.GetBytes(sKey),
    Encoding.ASCII.GetBytes(sKey)))
using (CryptoStream cryptoStream = new CryptoStream(outFile,
    desencrypt, CryptoStreamMode.Write))
{
    byte[] bytearrayinput = new byte[inFile.Length];
    inFile.Read(bytearrayinput, 0, bytearrayinput.Length);
    cryptoStream.Write(bytearrayinput, 0,
    bytearrayinput.Length);
    cryptoStream.Flush();
    outFile.Flush();
}
}

public static void DecryptFile(string sInputFilename, string
sOutputFilename, string sKey)
{
    //A 64 bit key and IV is required for this provider.
    //Set secret key For DES algorithm.
    DESCryptoServiceProvider DES = new DESCryptoServiceProvider();

    using (FileStream inFile = new FileStream(sInputFilename,
    FileMode.Open, FileAccess.Read))
    using (FileStream outFile = File.OpenWrite(sOutputFilename))
    using (ICryptoTransform desdecrypt =
    DES.CreateDecryptor(Encoding.ASCII.GetBytes(sKey),
    Encoding.ASCII.GetBytes(sKey)))
    using (CryptoStream cryptoStream = new CryptoStream(inFile,
    desdecrypt, CryptoStreamMode.Read))
    {
        // Read from the cryptoStream until EOF and write decrypted
        bytes to outFile.
        byte[] ba = new byte[1024];
        int count = 0;
        while ((count = cryptoStream.Read(ba, 0, ba.Length)) > 0)
        {
            outFile.Write(ba, 0, count);
        }
        outFile.Flush();
    }
}

public static void DoCrypto()
{
    // Must be 64 bits, 8 bytes.
    // Distribute this key to the user who will decrypt this file.
```

Re: Encrypt and Decrypt a file using .NET 2.0?

```
string sSecretKey;

// Get the Key for the file to Encrypt.
sSecretKey = GenerateKey();

// For additional security Pin the key.
GCHandle gch = GCHandle.Alloc(sSecretKey, GCHandleType.Pinned);

// Encrypt the file.
EncryptFile(@"C:\MyData.txt", @"C:\Encrypted.txt", sSecretKey);
Console.WriteLine("Encrypted");

// Decrypt the file.
DecryptFile(@"C:\Encrypted.txt",
@"C:\Decrypted.txt",sSecretKey);
Console.WriteLine("Decrypted.");

// Remove the Key from memory.
ZeroMemory(gch.AddrOfPinnedObject(), sSecretKey.Length * 2);
gch.Free();

Console.WriteLine("Done.");
Console.WriteLine("Cat Decrypted.txt:");
Cat(@"c:\decrypted.txt");
}

public static void Cat(string path)
{
    Console.WriteLine(File.ReadAllText(path));
}
}
}
```

--
William Stacey [C# MVP]
PCR concurrency library: www.codeplex.com/pcr
PSH Scripts Project www.codeplex.com/psobject

"JDeats" <Jeremy.Deats@xxxxxxxx> wrote in message
news:1177376866.469669.265330@xx
| I have some .NET 1.1 code that utilizes this technique for encrypting
| and decrypting a file.
| <http://support.microsoft.com/kb/307010>
|
| In .NET 2.0 this approach is not fully supported (a .NET 2.0 build
| with these methods, will appear to encrypt and decrypt, but the
| resulting decrypted file will be corrupted. I tried encrypting a .bmp
| file and then decrypting, the resulting decrypted file under .NET 2.0
| is garbage, the .NET 1.1 build works as expected).

Re: Encrypt and Decrypt a file using .NET 2.0?

Re: Encrypt and Decrypt a file using .NET 2.0?

|
| I would like to know why this approach is no longer supported, aside
| from building a .NET 1.1 class library and referencing it in my .NET
| 2.0 project, what is the proper way to encrypt and decrypt a file
| using .NET 2.0 and the DES encryption algorithm.
|

.