

Re: Cryptography RC4

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.languages.csharp/2008-01/msg00227.html>

- *From:* rossum <rossum48@xxxxxxxxxxxxx>
 - *Date:* Fri, 04 Jan 2008 00:44:56 +0000
-

On Thu, 3 Jan 2008 11:56:02 -0800, surcon
<surcon@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote:

Hi everyone,

I would like to know whether .NET framework 2.0 provides support for deriving an RC4 encryption key. Any suggestions would be greatly appreciated. I have:

```
TripleDESCryptoServiceProvider des = new TripleDESCryptoServiceProvider();  
des.IV = new byte[8];  
PasswordDeriveBytes pdb = new PasswordDeriveBytes(password, new byte[0]);
```

```
When I try to create the object DES.key  
des.Key = pdb.CryptDeriveKey("RC4", "MD5" 128, des.IV);
```

It throw the exception at this line that algorithm is not supported but there is no problem if replacing RC4 by RC2.

Best Regards

From your code fragments, you appear to be deriving a DES key, not an

RC4 key: "des.Key = ...". You cannot use RC4 as the algname parameter of CryptDeriveKey, the only allowed algorithms are DES, 3DES and RC2. See <http://blogs.msdn.com/shawnfa/archive/2004/04/14/113514.aspx> for more details.

RC4 is pretty flexible about the size of key it takes, the specification allows keys up to 256 bytes long, with a default of 128 bytes. It should be possible to use a DES sized key with RC4.

The major question is why you want to use either DES or RC4, both are rather old and rather broken. Neither can be considered secure at present – better to use AES (=Rijndael), or if you need a stream cypher then AES in CTR mode.

rossum

Re: Cryptography RC4