

Forum:[Hack Forums](#)

Thread: [rsa encryption exception \(Key not valid for use in specified state.\)](#)

x factor fan - August 1, 2016, 6:03 pm

hi friends..

today i was woking on a app that would encrypt a file to keep it safe from other ppl (i would pick a file to encrypt then i would need to enter passwords to unlock file).. the code works very good but the problem is when i encrypt a file over 255 bytes i get eception :(that say Key not valid for use in specified state).. what can be problem? the key is fine.. any help would be great. thanks friends)..

my code..

Code static public byte[] RSAEncrypt(byte[] DataToEncrypt, RSAParameters RSAKeyInfo, bool DoOAEPPadding)

```
{
    try
    {
        byte[] encryptedData;
        //Create a new instance of RSACryptoServiceProvider.
        using (RSACryptoServiceProvider RSA = new RSACryptoServiceProvider())
        {

            //Import the RSA Key information. This only needs
            //toinclude the public key information.
            RSA.ImportParameters(RSAKeyInfo);

            //Encrypt the passed byte array and specify OAEP padding.
            //OAEP padding is only available on Microsoft Windows XP or
            //later.
            encryptedData = RSA.Encrypt(DataToEncrypt, DoOAEPPadding);
        }
        return encryptedData;
    }
    //Catch and display a CryptographicException
    //to the console.
    catch (CryptographicException e)
    {
        Console.WriteLine(e.Message);

        return null;
    }
}
```

encryptedData = RSAEncrypt(dataToEncrypt, RSA.ExportParameters(false), false);
i am russian by the way sorry for my english ((

HFDone - August 2, 2016, 12:46 am

RSA.ExportParameters(true)

x factor fan - August 2, 2016, 7:45 am

(Aug 2, 2016 12:46 AM)HFDone Wrote: [\[CITE\]](#) RSA.ExportParameters(true)
hi.. i tried that and it gave me unspecified error exception ((

?

debug - August 2, 2016, 9:01 am

The problem is your RSA key format. I had a similar issue.

Use this command on unix to format it correctly:
openssl rsa -in server.key -out server_new.key

6e756c6c - August 2, 2016, 9:23 am

The problem is RSA can only encrypt data with a length less than or equal to it's key size in bytes. So if you have a 4096 RSA key it can encrypt up to 512 bytes of data. Instead, you should be encrypting with AES or if you are really set on using RSA then you need to:

- A.) Encrypt with AES, then encrypt the AES key using RSA and append this to the cipher text.
- B.) Encrypt your data in chunks of 128, 256, 512, etc. bytes. This is going to be VERY slow so I would not recommend it.

x factor fan - August 2, 2016, 12:56 pm

(Aug 2, 2016 09:23 AM)Fire+Rain Wrote: [\[CITE\]](#) The problem is RSA can only encrypt data with a length less than or equal to it's key size in bytes. So if you have a 4096 RSA key it can encrypt up to 512 bytes of data. Instead, you should be encrypting with AES or if you are really set on using RSA then you need to:

- A.) Encrypt with AES, then encrypt the AES key using RSA and append this to the cipher text.
- B.) Encrypt your data in chunks of 128, 256, 512, etc. bytes. This is going to be VERY slow so I would not recommend it.

thank u for the info.. i will try later and report back.. ?

x factor fan - August 7, 2016, 11:53 pm

hello friends, i have switched to aes encryption but i am facing 1 big problem ((

i was able to create a encrypt function very easily (And it work) but i am struggle on how to make decrypt function..

my encrypt function:

```
Code public static void EncryptFile(string filePath, byte[] key, byte[] iv)
{
    if (File.Exists(filePath))
    {
        try
        {
            byte[] fileBytes = File.ReadAllBytes(filePath);
            byte[] encryptedFile;
            using (AesCryptoServiceProvider encryptAES = new AesCryptoServiceProvider())
            {
                encryptAES.Key = key;
```

```

        encryptAES.IV = iv;

        ICryptoTransform encryptor = encryptAES.CreateEncryptor(encryptAES.Key,
encryptAES.IV);

        using (MemoryStream msEncrypt = new MemoryStream())
        {
            using (CryptoStream csEncrypt = new CryptoStream(msEncrypt, encryptor,
CryptoStreamMode.Write))
            {
                using (StreamWriter swEncrypt = new StreamWriter(csEncrypt))
                {
                    swEncrypt.Write(csEncrypt);
                }
                encryptedFile = msEncrypt.ToArray();
            }
        }

        File.WriteAllBytes(filePath, encryptedFile);
    }
}
catch (Exception)
{
}
}
}

```

i am getting my key and iv from this function and storing them in 2 seperate variables..

```

Code public static byte[] GenerateKey()
{
    using (AesCryptoServiceProvider tempAES = new AesCryptoServiceProvider())
    {
        return tempAES.Key;
    }
}

public static byte[] GenerateInitializationVector()
{
    using (AesCryptoServiceProvider tempAES = new AesCryptoServiceProvider())
    {
        return tempAES.IV;
    }
}

```

i am now trying to figure out how to write a decrypt function.. this is how far i got before i get stuck ((
:D

```

Code public static void DecryptFile(string filePath, byte[] key, byte[] iv)
{
    if (File.Exists(filePath))
    {
        byte[] file = File.ReadAllBytes(filePath);
        byte[] decryptedFile;
        try

```

```
{
    using (AesCryptoServiceProvider decryptAES = new AesCryptoServiceProvider())
    {
        decryptAES.Key = key;
        decryptAES.IV = iv;

        ICryptoTransform decryptor = decryptAES.CreateDecryptor(decryptAES.Key,
decryptAES.IV);

    }
```

```
    }
    catch (Exception)
    {
    }
```

```
}
```

```
}
```

any help would be appreciated my friends)) ?

so i guess no one wants to help me ((