

Forum:[Hack Forums](#)

Thread: [vb.net aes doesnt remove padding?](#)

mcly - June 12, 2014, 4:29 am

TL;DR : The aes decryption does not remove padding from my php encrypted data

Quote:So i have a php page that returns encrypted content, the client downloads this content and then decrypts it using aes, viewing this decrypted "text" it looks just like the original message, but when i tried to display the data, it seems like there are like 20 spaces after the decrypted text (the status code displays the message up until to the decrypted message, then there is space that covers the rest of the message)

So i've when you debug this, you can only see the decrypted message, no space, no "0", no nothing, just the decrypted message in quotes

for example : "hello"

Now when i viewed the length of this string, the length was way above it was supposed to be (32) which leads to the conclusion that there is some random space/nulls (which is probably padding) that didn't get removed from the aes decryption function..

hexing this string showed that the "hello" part existed, but after that it was filled with around twenty 0's

So i've made a temporary fix by hexing the string, then removing the 0's and converting the hex back to a string..

Now let's show you some code i'm using, first of all, yes the keysize, the blocksize, the Ciphermode and the padding for both php and vb.net match (i use mcrypt_encrypt for php, which only supports zero padding as i've read, vb.net uses zero padding too)

Anyway, here is my php aes encryption code

PHP Code

```
<?php
function encryptRJ256($string_to_encrypt){
    $key = "_mykeyhere_";
    $iv = "_mykeyhere_";
    $rtn = mcrypt_encrypt(MCRYPT_RIJNDAEL_256, $key, $string_to_encrypt,
MCRYPT_MODE_CBC, $iv);
    $rtn = base64_encode($rtn);
    return($rtn);}

```

Seems pretty simple right? Anyway, here is my matching vb.net code

PHP Code

```
<?php
Public Function PHPDecrypt(ByVal prm_text_to_decrypt As String) As String
    Try

```

```

Dim sEncryptedString As String = prm_text_to_decrypt
Dim myRijndael As New RijndaelManaged
myRijndael.Padding = PaddingMode.Zeros
myRijndael.Mode = CipherMode.CBC
myRijndael.KeySize = 256
myRijndael.BlockSize = 256
Dim key() As Byte = System.Text.Encoding.ASCII.GetBytes("_mykeyhere_") ' Key
Dim IV() As Byte = System.Text.Encoding.ASCII.GetBytes("_mykeyhere_") 'IV
Dim decryptor As ICryptoTransform = myRijndael.CreateDecryptor(key, IV)
Dim sEncrypted As Byte() = Convert.FromBase64String(sEncryptedString)
Dim fromEncrypt() As Byte = New Byte(sEncrypted.Length) {}
Dim msDecrypt As New MemoryStream(sEncrypted)
Dim csDecrypt As New CryptoStream(msDecrypt, decryptor, CryptoStreamMode.Read)
csDecrypt.Read(fromEncrypt, 0, fromEncrypt.Length)
Return System.Text.Encoding.ASCII.GetString(fromEncrypt)
Catch ex As Exception
Return prm_text_to_decrypt
End Try
End Function

```

Now this will result in me getting a message that is properly decrypted, but has the padding not removed (as i described, "hello" gets decrypted fine, but it contains 0's from the padding.. (the amount of 0's are always different and go from 20-40)

Can someone help me or guide me to what im doing wrong?

Only3 - June 12, 2014, 6:01 am

all u need here <http://www.php.net/manual/en/function.mcrypt-encrypt.php>

mcly - June 12, 2014, 9:39 am

(Jun 12, 2014 06:01 AM)Only3 Wrote: [\[CITE\]](#) all u need here

<http://www.php.net/manual/en/function.mcrypt-encrypt.php>

Did you read my post mate? :(

Im using this, and the encryption is working fine, the decryption (the padding removal part) is the problem (i believe)

Only3 - June 12, 2014, 10:48 am

did u read about padding there ? No !

here working example read the replys u cant just c&p

<http://stackoverflow.com/questions/1278974/php-encryption-vb-net-decryption>

mcly - June 12, 2014, 11:53 am

(Jun 12, 2014 10:48 AM)Only3 Wrote: [\[CITE\]](#) did u read about padding there ? No !

here working example read the replys u cant just c&p

<http://stackoverflow.com/questions/1278974/php-encryption-vb-net-decryption>

Yes i did!

I understand the code and i did not "blindly" copy paste it without trying to understand it, why do you accuse me of that?

PHP uses zero as default pedding method, maybe you should read it up?

<http://www.php.net/manual/en/function.mcrypt-encrypt.php>

Code # creates a cipher text compatible with AES (Rijndael block size = 128)

to keep the text confidential

only suitable for encoded input that never ends with value 00h

(because of default zero padding)

The encryption process does not work without a padding (because otherwise it wouldn't fit to a multiply of 8 or 16 i believe)

Anyway, even if it didn't use ANY padding at all, how comes the decrypted messages have 20-40 null bytes (zeros) appended to the text? (Clearly, that has to be the ZERO padding)

My question is not how to add padding to the php encryption method, it rather is how to remove the padding, normally it should do that in the decryption process (that is why you have to specify the padding method before you can decrypt)

Here is, (in case you didn't notice) a part of the padding from my vb.net decryption code to show you that i infact DID declare the correct padding

```
Code Dim myRijndael As New RijndaelManaged
    myRijndael.Padding = PaddingMode.Zeros
    myRijndael.Mode = CipherMode.CBC
    myRijndael.KeySize = 256
```

Can anyone tell me what im doing wrong? Maybe someone experienced in here?

Banks? - June 12, 2014, 8:07 pm

[Stream.Read\(byte\[\], int, int\)](#) returns an integer indicating the amount of bytes read. Just get that value and then resize the array to what was returned.

mcly - June 13, 2014, 3:37 am

(Jun 12, 2014 08:07 PM)Banks? Wrote: [\[CITE\] Stream.Read\(byte\[\], int, int\)](#) returns an integer indicating the amount of bytes read. Just get that value and then resize the array to what was returned.

Im pretty sure that that would just return the length of the string + the 0 bytes, so that would be kind of useless!?

Because the response from the php site would obviously be lets say

hello000000 (something like that encrypted ofcourse)

Now the decryption method is supposed to remove the 0 (zero padding) while decrypting, but it doesn't do that.. Now when i read the length of this , it will obviously return the wrong value for me to just take the substring for the hello..

The only way this would work is if the server would respond with the encrypted data+ data length, but encrypting the data length response would cause the same problem.. If i return the data length in plaintext without encryption, then im pretty sure that that would compromise the encryption security (im pretty sure that knowing the data length would compromise the encryption security)

But the big main question is, why does my decryption not remove the zero padding? What am i doing wrong? Does noone of you guys use aes encryption for php/vb.net? Dont you have a crypter too that uses encrypted traffic?

Banks? - June 13, 2014, 11:06 am

(Jun 13, 2014 03:37 AM)mcly Wrote: [\[CITE\]](#) Im pretty sure that that would just return the length of the string + the 0 bytes, so that would be kind of useless!?

Because the response from the php site would obviously be lets say

hello000000 (something like that encrypted ofcourse)

Now the decryption method is supposed to remove the 0 (zero padding) while decrypting, but it doesnt do that.. Now when i read the length of this , it will obviously return the wrong value for me to just take the substring for the hello..

The only way this would work is if the server would respond with the encrypted data+ data length, but encrypting the data length response would cause the same problem.. If i return the data length in plaintext without encryption, then im pretty sure that that would compromise the encryption security (im pretty sure that knowing the data length would compromise the encryption security)

But the big main question is, why does my decryption not remove the zero padding? What am i doing wrong? Does noone of you guys use aes encryption for php/vb.net? Dont you have a crypter too that uses encrypted traffic?

Have you tried what I told you to try?

mcly - June 13, 2014, 12:07 pm

(Jun 13, 2014 11:06 AM)Banks? Wrote: [\[CITE\]](#) Have you tried what I told you to try?

Sure, but where is the point? I dont understand it..

It returns the length of the string+padding (32 as double)

the string i expected (without the padding) has the length of 8

Like i said, the problem seems to be that the decryption does not remove the zero padding.. I just dont understand why it does not

Banks? - June 16, 2014, 3:42 am

<http://forums.asp.net/t/1545978.aspx?AES+Rijndael+encryption+help>

This might help you.