

Re: Thank You; How Many VarBinary for each Ascii Char Aes Encrypted KeySize=256,BlockSize=256

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.framework.aspnet.security/2005-02/0273.html>

From: Joe Kaplan \((MVP - ADSI)\) (*joseph.e.kaplan_at_removethis.accenture.com*)

Date: 02/25/05

Date: Fri, 25 Feb 2005 10:28:01 -0600

SQL is definitely not my thing and I've never used a varbinary column.

With AES, if you input 50 bytes, you should get an even multiple of 256 bits (32 bytes) back, so I'd expect it will take 64 bytes to store 50 plain input bytes. UTF8 should produce 50 bytes for 50 ASCII characters.

I still like the idea of using varchar and converting your encrypted output to base64. Then you store in SQL as a simple string. Seems easier to deal with to me.

Joe K.

"Phil C." <charlestek@rcn.com> wrote in message
news:ufEZxw0GFHA.2744@tk2msftngp13.phx.gbl...

> *Joe,*

>

> *Thanks again for the detailed advice.*

> *VarBinary seems also somewhat nebulous to me, as the definition I get from*

> *Robert Viera's*

> *Sql Server 2000 Programming Book says:*

> *"Size in Bytes: 'Varies' ", "Variable length binary data with a maximum*

> *length of*

> *8,000 bytes."*

>

> *So lets say I use UTF8, for 50 ascii characters I would expect 50 bytes,*

> *and from the above VarBinary*

> *definition, this implies that I could get away with the database column as*

> *VarBinary 1 ???*

>

> *Phil*

>

>

> *"Joe Kaplan (MVP - ADSI)" <joseph.e.kaplan@removethis.accenture.com> wrote*

> in message news:uEISEj0GFHA.1172@TK2MSFTNGP12.phx.gbl...
>> I'd suggest the best thing to do would be to try it out and see. AES
>> uses padding backed on the block size, so you should get consistent sizes
>> back. Assuming you are using UTF8 encoding to convert your plain text to
>> a byte array for encryption, you could potentially get variable sizes of
>> input data, but if all of the characters you are encoding are ASCII, then
>> that should be consistent as well.
>>
>> You might also consider converting your encrypted data to Base64 to store
>> in the db. That might be easier to deal with than storing as raw binary.
>> It will be 4/3 the size of the original byte array, but then you can just
>> use varchar.
>>
>> Joe K.
>>
>> "Phil C." <charlestek@rcn.com> wrote in message
>> news:OHdnoOsGFHA.3916@TK2MSFTNGP12.phx.gbl...
>>> Hi. I'm wanting to encrypt customer name, address, etc. information
>>> using Aes with a KeySize of 256 and a BlockSize of 256. Either for each
>>> ascii character or say for a maximum length 50 characters for a field,
>>> how many bytes will this generate and how do I translate
>>> this into the number of VarBinary ???items that I allocate in my Sql
>>> Server 2000 table??
>>>
>>> Phil
>>> Boston, MA
>>>
>>
>>
>
>