Journey to SQL Authority with Pinal Dave

SQL, SQL Server, MySQL, Big Data and NoSQL

APRIL 28, 2009 BY PINAL DAVE

SQL SERVER – Introduction to SQL Server Encryption and Symmetric Key Encryption Tutorial with Script

SQL Server 2005 and SQL Server 2008 provide encryption as a new feature to protect data against hackers' attacks. Hackers might be able to penetrate the database or tables, but owing to encryption they would not be able to understand the data or make use of it. Nowadays, it has become imperative to encrypt crucial security-related data while storing in the database as well as during transmission across a network between the client and the server.

Encryption hierarchy is marked by three-level security. These three levels provide different mechanisms for securing data across networks and local servers. Different levels of hierarchies allow multiple instances of services (e.g., SQL Server Services) to run on one physical server.

- **Windows Level** – Highest Level – Uses Windows DP API for encryption
- **SQL Server Level** - Moderate Level – Uses Services Master Key for encryption
- **Database Level** – Lower Level – Uses Database Master Key for encryption

There are two kinds of keys used in encryption:

- **Symmetric Key** – In Symmetric cryptography system, the sender and the receiver of a message share a single, common key that is used to encrypt and decrypt the message. This is relatively easy to implement, and both the sender and the receiver can encrypt or decrypt the messages.
- **Asymmetric Key** – Asymmetric cryptography, also known as Public-key cryptography, is a system in which the sender and the receiver of a message have a pair of cryptographic keys – a public key and a private key – to encrypt and decrypt the message. This is a relatively complex system where the sender can use his key to encrypt the message but he cannot decrypt it. The receiver, on the other hand, can use his key to decrypt the message but he cannot encrypt it. This intricacy has turned it into a resource-intensive process.

Yet another way to encrypt data is through certificates. A public key certificate is a digitally signed statement that binds the value of a public key to the identity of the person, device, or service that holds the corresponding private key. A Certification Authority (CA) issues and signs certifications.

Download complete script here (http://www.pinaldave.com/sql-script-bank/script-downloads-1/sql-server-introduction-to-sql-server-encryption-and-symmetric-key-encryption-tutorial-with-script/).

Please create a sample database that we will be use for testing Encryption. There are two different kinds of encryptions available in SQL Server:

- **Database Level** – This level secures all the data in a database. However, every time data is written or read from database, the whole database needs to be decrypted. This is a very resource-intensive process and not a practical solution.
- **Column (or Row) Level** – This level of encryption is the most preferred method. Here, only columns containing important data should be encrypted; this will result in lower CPU load compared with the whole database level encryption. If a column is used as a primary key or used in comparison clauses (WHERE clauses, JOIN conditions) the database will have to decrypt the whole column to perform operations involving those columns.

Let's go over a simple instance that demonstrates the encryption and the decryption process executed with Symmetric Key and Triple DES encryption algorithm.

```
/* Create Database  */
USE master
GO
CREATE DATABASE EncryptTest
ON PRIMARY ( NAME = N'EncryptTest', FILENAME = N'C:\EncryptTest.mdf')
LOG ON ( NAME = N'EncryptTest_log', FILENAME = N'C:\EncryptTest_log.ldf')
GO
```

First, let's create a sample table and then populate it with sample data. We will now encrypt one of the two columns of the table.

```
/* Create table and insert data in the table */
USE EncryptTest
GO
CREATE TABLE TestTable (FirstCol INT, SecondCol VARCHAR(50))
GO
INSERT INTO TestTable (FirstCol, SecondCol)
SELECT 1,'First'
UNION ALL
SELECT 2,'Second'
UNION ALL
SELECT 3,'Third'
UNION ALL
SELECT 4,'Fourth'
UNION ALL
SELECT 5,'Fifth'
GO
/* Check the content of the TestTable */
USE EncryptTest
GO
```

```
SELECT *
FROM TestTable
GO
```

The preceding code will return the result depicted in the subsequent figure.

	FirstCol	SecondCol
1	1	First
2	2	Second
3	3	Third
4	4	Fourth
5	5	Fifth

Result of the SQL query

Every database can have one master key. Database master key is a symmetric key used to protect the private keys of certificates and asymmetric keys present in the database. It uses Triple DES algorithm together with user-provided password to encrypt the keys.

```
/* Create Database Master Key */
USE EncryptTest
GO
CREATE MASTER KEY ENCRYPTION
BY PASSWORD = 'SQLAuthority'
GO
```

Certificates are used to safeguard encryption keys, which are used to encrypt data in the database. SQL Server 2005 has the capability to generate self-signed X.509 certificates.

```
/* Create Encryption Certificate */
USE EncryptTest
GO
CREATE CERTIFICATE EncryptTestCert
WITH SUBJECT = 'SQLAuthority'
GO
```

The symmetric key can be encrypted by using various options such as certificate, password, symmetric key, and asymmetric key. A number of different algorithms can be employed for encrypting key. The supported algorithms are DES, TRIPLE_DES, RC2, RC4, RC4_128, DESX, AES_128, AES_192, and AES_256.

```
/* Create Symmetric Key */
USE EncryptTest
GO
CREATE SYMMETRIC KEY TestTableKey
WITH ALGORITHM = TRIPLE_DES ENCRYPTION
BY CERTIFICATE EncryptTestCert
GO
```

Now add a column of type varbinary to the original table, which will store the encrypted value for the SecondCol.

```
/*  Encrypt Data using Key and Certificate
Add Columns which will hold the encrypted data in binary */
USE EncryptTest
GO
ALTER TABLE TestTable
ADD EncryptSecondCol VARBINARY(256)
GO
```

Before the key is used, it needs to be decrypted using the same method that was used for encrypting it. In our example, we have used a certificate for encrypting the key. Because of the same reason, we are using the same certificate for opening the key and making it available for use. Subsequent to opening it and making it available for use, we can use the encryptkey function and store the encrypted values in the database, in the EncryptSecondCol column.

```
/* Update binary column with encrypted data created by certificate and key */
USE EncryptTest
GO
OPEN SYMMETRIC KEY TestTableKey DECRYPTION
BY CERTIFICATE EncryptTestCert
UPDATE TestTable
SET EncryptSecondCol = ENCRYPTBYKEY(KEY_GUID('TestTableKey'),SecondCol)
GO
```

We can drop the original SecondCol column, which we have now encrypted in the EncryptSecondCol column. If you do not want to drop the column, you can keep it for future comparison of the data when we decrypt the column.

```
/* DROP original column which was encrypted for protect the data */
USE EncryptTest
GO
ALTER TABLE TestTable
DROP COLUMN SecondCol
GO
```

We can run a SELECT query on our database and verify if our data in the table is well protected and hackers will not be able to make use of it even if they somehow manage to reach the data.

```
/* Check the content of the TestTable */
USE EncryptTest
GO
SELECT *
FROM TestTable
GO
```

	FirstCol	EncryptSecondCol
1	1	0x003B444CCFA3B040AEE7FF980C76B82301000000CEFE6F...
2	2	0x003B444CCFA3B040AEE7FF980C76B823010000007C11369...
3	3	0x003B444CCFA3B040AEE7FF980C76B82301000000BA407B...
4	4	0x003B444CCFA3B040AEE7FF980C76B823010000004623AC...
5	5	0x003B444CCFA3B040AEE7FF980C76B823010000002886EB...

Result of the previous SQL query

Authorized user can use the decryptbykey function to retrieve the original data from the encrypted column. If Symmetric key is not open for decryption, it has to be decrypted using the same certificate that was used to encrypt it. An important point to bear in mind here is that the original column and the decrypted column should have the same data types. If their data types differ, incorrect values could be reproduced. In our case, we have used a VARCHAR data type for SecondCol and EncryptSecondCol.

```
/* Decrypt the data of the SecondCol  */
USE EncryptTest
GO
OPEN SYMMETRIC KEY TestTableKey DECRYPTION
BY CERTIFICATE EncryptTestCert
SELECT          CONVERT(VARCHAR(50),DECRYPTBYKEY(EncryptSecondCol))          AS
DecryptSecondCol
FROM TestTable
GO
```

	FirstCol	DecryptSecondCol
1	1	First
2	2	Second
3	3	Third
4	4	Fourth
5	5	Fifth

If you drop the database after the entire processing is complete, you do not have to worry about cleaning up the database. However, in real world on production servers, the database is not dropped. It is a good practice for developers to close the key after using it. If keys and certificates are used only once or their use is over, they can be dropped as well. Dropping a database will drop everything it contains – table, keys, certificates, all the data, to name a few.

```
/* Clean up database  */
USE EncryptTest
GO
CLOSE SYMMETRIC KEY TestTableKey
GO
DROP SYMMETRIC KEY TestTableKey
GO
DROP CERTIFICATE EncryptTestCert
GO
DROP MASTER KEY
```

```
GO
USE [master]
GO
DROP DATABASE [EncryptTest]
GO
```

Summary

Encryption is a very important security feature of SQL Server 2005. Long keys and asymmetric keys create unassailable, stronger encryption and stronger encryption uses lots of CPU to encrypt data. Stronger encryption is slower to process. When there is a huge amount of data to encrypt, it is suggested to encrypt it using a symmetric key. The same symmetric key can be encrypted further with an asymmetric key for additional protection, thereby adding the advantage of a stronger encryption. It is also recommended to compress data before encryption, as encrypted data cannot be compressed.

Click to Download Scripts (http://www.pinaldave.com/sql-script-bank/script-downloads-1/sql-server-introduction-to-sql-server-encryption-and-symmetric-key-encryption-tutorial-with-script/)

Reference : **Pinal Dave (http://blog.SQLAuthority.com (http://blog.sqlauthority.com/))**

This entry was posted in Pinal Dave, SQL, SQL Authority, SQL Query, SQL Scripts, SQL Security, SQL Server, SQL Tips and Tricks, T SQL, Technology and tagged SQL Server Encryption. Bookmark the permalink.

97 thoughts on "*SQL SERVER – Introduction to SQL Server Encryption and Symmetric Key Encryption Tutorial with Script*"

Atif Shehzad | **April 28, 2009 at 11:57 am**

Encryption is a complicated task for beginners to implement. You have provided a very good path to start on for implementation of encryption.

Reply

abhijit | **November 2, 2011 at 1:22 pm**

I m bit new to this field of DBA i wanted to know is there any codes available to encrypt the entire database as we have a huge database maintained in sqlserver 2005 . I know that it is not safe to encrypt the entire database but we ha such kind of requirement moreover the in the application end they don't want to encrypt it. i want the process to be as the data comes through the application end into the database it should be encrypted and stored and while retrieving the data it must be decrypted with a certificate/key as provided and shown. I don't want to use any 3rd party tools as it has been instructed. i searched through the net and found that we can encrypt columns and stored procedure through asymmetric/symmetric key but i need to encrypt the entire database(selected tables is also ok) can you all help me in that.

Reply

Mitesh L Shah | **April 28, 2009 at 12:02 pm**

Hi Pinal
Wonderful explaination, it was really very nice to read this artical. Thanks a lot for sharing this knowledge.

Reply

chetan kumar | **August 31, 2011 at 5:43 am**

how to decrypt the md5.It is in encryption format,I have millions of records in text file…

Reply

Brian Tkatch | **April 28, 2009 at 6:06 pm**

Pinal thanx for the informative beginners article.

Reply

Pradeep | **April 29, 2009 at 12:32 am**

Nice

Is will work with Express edititons ?

Reply

Dexter | **April 30, 2009 at 12:27 pm**

If I want to specify the exact value of the Triple DES key that will encrypt the data, do I specify that value in the PRIVATE KEY field in CREATE CERTIFICATE?

Thanks for the great explanation!

Dexter

Reply

anuj | **May 11, 2009 at 12:36 pm**

create database SecurityDemo

use SecurityDemo
go
create master key encryption by password = 'pass@word1'
go

Server: Msg 170, Level 15, State 1, Line 1
Line 1: Incorrect syntax near 'master'.

Reply

kelvin | **December 5, 2011 at 9:38 pm**

the first quot is not a quote. try this create master key encryption by password = 'pass@word1'

Reply

anuj | **May 11, 2009 at 12:39 pm**

sir i am writing a correct syntax for creating master key but it give an error .
i am not understanding what is error while my syntax is correct.

Reply

Ethan Nelson | **May 21, 2009 at 1:07 am**

Pinal,

I have a situation where I'm required to maintain an asymmetric key off-server in a web app. How can I securely pass the key? I cannot use the below because DDL statements cannot be parameterized.

OPEN SYMMETRIC KEY PtripSafe DECRYPTION BY
ASYMMETRIC KEY PtripSafeKey
WITH password = ?

If I type the password into the ? position, the profiler sees it and exposes it on the database server to an administrator.

-Ethan Nelson

Reply

Hossam | **May 30, 2009 at 5:25 pm**

Nice

But i have to use VARBINARY data type becouse when i try to encrypte char column displayee as a Null ???!!!

Reply

namtrung | **June 30, 2009 at 9:27 pm**

thanks
but,how to encrypt tablename and fieldname?
i don't want to public them.

Reply

01 | **August 16, 2009 at 11:54 pm**

thanks about article but what will happen if the symmetric key deleted, in fact your data is lost!

back up is available for master key and CERTIFICATE but not for symmetric keys!

so what is the Solution?

Reply

invincible | **September 2, 2009 at 4:19 pm**

Pinal bhai decryption is not working and its not feasible to alter table for encryption. Find some other solution and notify me soon…

Reply

Amit Saraswat | **September 3, 2009 at 12:19 pm**

hi Pinal Dave,

Wonderful explaination,

it was really very nice to read this artical. Thanks a lot for sharing this knowledge.

Reply

Arun Kasturi | October 20, 2009 at 8:29 pm

The article is very usefull. Also can you please explain if the database with certificate and symmetric keys has to be moved to another SQL Server? How to restore back the encryption on the database?

Thanks in advance.
Arun

Reply

N.Raja | January 8, 2010 at 5:31 am

Will appreciate if the scenarios of losing the passwords of Symmetric, Asymmetric and Certificates are explained. Basically looking for a procedure to recover the keys if the Passwords are lost. As per the understanding, a copy of the key is also encrypted using DB Master Key. Do we have a set of commands to recover from that.

Regards

Reply

Feodor | January 20, 2010 at 12:57 am

I am new to encryption and I would like to thank you for the great article.
I have a question, though. When you write about the two levels of encryption (database and column), do you mean that the database encryption is the transparent data encryption, or is this something different?

Reply

Feodor | January 20, 2010 at 1:08 am

Also, what happens when we move encrypted database to another server? How do we back up the database master key, the master db certificate, the user database key? How do we restore the keys and certificates?

Reply

Asif.S | January 21, 2010 at 6:44 pm

Try this.
****

In order to restore the encrypted database backup on another SQL Server instance we need to first export the certificate we created on the instance on which the encrypted database backup was created. To export the certificate to a file, I'll connect on my default instance and run this query.

USE master
GO
BACKUP CERTIFICATE NorthwindCert
TO FILE = 'C:\NorthwindCert_File.cer'

WITH PRIVATE KEY (FILE = 'C:\NorthwindCert_Key.pvk' ,
ENCRYPTION BY PASSWORD = 'mY_P@$$w0rd')
GO
****

Then, we'll need to copy the certificate and the private key file to the other SQL Server instance.
Since I am running my default and my TEST instances on the same server, I'll just refer to those
files when I do the import process. Now, on the TEST instance, import the certificate by first
creating a master key.

USE master
GO

CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'EnKrYpt3d_P@$$w0rd'
GO
****

The password provided here is different from the one you used in the default instance as you are
creating a new master key for this instance. After a master key has been created, you can create
a certificate by importing the certificate we created earlier.

CREATE CERTIFICATE NorthwindCert
FROM FILE = 'C:\NorthwindCert_File.cer'
WITH PRIVATE KEY (FILE = 'C:\NorthwindCert_Key.pvk',
DECRYPTION BY PASSWORD = 'mY_P@$$w0rd');
GO

****

Reply

        Asif.S | **January 22, 2010 at 4:21 pm**

Try this.
****

In order to restore the encrypted database backup on another SQL Server instance we need to first
export the certificate we created on the instance on which the encrypted database backup was
created. To export the certificate to a file, I'll connect on my default instance and run this query.

USE master
GO
BACKUP CERTIFICATE NorthwindCert
TO FILE = 'C:\NorthwindCert_File.cer'
WITH PRIVATE KEY (FILE = 'C:\NorthwindCert_Key.pvk' ,
ENCRYPTION BY PASSWORD = 'mY_P@$$w0rd')
GO
****

Then, we'll need to copy the certificate and the private key file to the other SQL Server instance.
Since I am running my default and my TEST instances on the same server, I'll just refer to those
files when I do the import process. Now, on the TEST instance, import the certificate by first
creating a master key.

USE master
GO

CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'EnKrYpt3d_P@$$w0rd'
GO
****

The password provided here is different from the one you used in the default instance as you are creating a new master key for this instance. After a master key has been created, you can create a certificate by importing the certificate we created earlier.

CREATE CERTIFICATE NorthwindCert
FROM FILE = 'C:\NorthwindCert_File.cer'
WITH PRIVATE KEY (FILE = 'C:\NorthwindCert_Key.pvk',
DECRYPTION BY PASSWORD = 'mY_P@$$w0rd');
GO

****

Reply

cvnrao | **February 17, 2010 at 10:25 am**
how to encrypt a existing data in a column with out changing the structure of a table.

What I mean to say is that if a table has two fields say name and account no.. I want to encrypt accountno field with out adding any column to this table.

Thanks

RAO

Reply

Arun | **February 18, 2010 at 1:34 pm**
Hi,

I have Question Sql data Encryption? I want to encrypt the data in Sql 2005 & 2008 .
What are the data type can we use ?
If it is Only Varbinary data type then Please let me know the reason and what is the length of varbinary should we use.

Reply

Pinal Dave | **February 19, 2010 at 7:09 pm**
Hello Arun,

Only varbinary dataype can be encrypted was the limitation in SQL Server 2005. In SQL Server 2008, TDE support all data types.

Regards,
Pinal Dave

Reply

Feodor Georgiev | **February 19, 2010 at 10:42 pm**

Great tutorial!

Reply

Arun | **February 22, 2010 at 6:28 pm**

Hi Pinal Dave,

Thank you very much for the response.

Can you tell me, this is the way to call procedure for encryption type as below ?

```
EXEC @KEY= 'TestTableKey' , @CERTIFICATE ='EncryptTestCert'
GO

CREATE PROCEDURE spEncryption
@KEY VARCHAR(200),
@CERTIFICATE VARCHAR(200)

AS
BEGIN

DECLARE @dyKeyExecute varchar(2000)

SET @dyKeyExecute = ''

CREATE MASTER KEY ENCRYPTION
BY PASSWORD = 'SQLAuthority'

SET @dyKeyExecute = 'CREATE CERTIFICATE ' + @CERTIFICATE
SET @dyKeyExecute = @dyKeyExecute + 'WITH SUBJECT = ' + 'SQLAuthority'

EXEC (@dyKeyExecute)

SET @dyKeyExecute = ''
SET @dyKeyExecute = 'CREATE SYMMETRIC KEY ' + @KEY
SET @dyKeyExecute = @dyKeyExecute + 'WITH ALGORITHM = TRIPLE_DES ENCRYPTION
BY CERTIFICATE' + @CERTIFICATE

EXEC (@dyKeyExecute)

SET @dyKeyExecute =''
SET @dyKeyExecute ='OPEN SYMMETRIC KEY' + @KEY + 'DECRYPTION BY CERTIFICATE'
+ @CERTIFICATE
EXEC (@dyKeyExecute)
GO

SELECT CONVERT(VARCHAR(50),DECRYPTBYKEY(EncryptSecondCol)) AS
DecryptSecondCol
FROM TestTable
```

/**drop the key**/

CLOSE SYMMETRIC KEY TestTableKey
GO
DROP SYMMETRIC KEY TestTableKey
GO
DROP CERTIFICATE EncryptTestCert
GO
DROP MASTER KEY
GO

END

Reply

Arun | **February 22, 2010 at 6:55 pm**

Hi Pinal Dave,

I have written the dynamic sql for key, since I have a double, since it can be read from
SELECT * FROM sys.symmetric_keys
SELECT * FROM sys.certificates

so any one who knows this can access the data more over.. before executing the script , we are opening

OPEN SYMMETRIC KEY TestTableKey DECRYPTION
BY CERTIFICATE EncryptTestCert

so this key is visible to everyone who open's the stored procedure .

Please guide me on this.

Thanks
Arun

Reply

noreen | **March 13, 2010 at 1:03 am**
how to add values to encrypted tables/columns

Reply

Pinal Dave | **March 13, 2010 at 10:46 pm**
Hello Noreen,

There are various functions in SQL Server 2008 to encrypt and decript data. In this article I demonstrated the use of ENCRYPTBYKEY and DECRYPTBYKEY functions. There are more functions to encrypt by certificate and password.

Regards,
Pinal Dave

Reply

sunil yoganna | **March 26, 2010 at 4:00 pm**

Hi Pinal,

i thought encryption and DEcryption is complecated after reading this article i am much comfortable usin Encryption and
DEcryption key

Reply

Aparna | **April 28, 2010 at 2:11 am**

I have a situation where the data should go encrypted from one server to another

Server B should have the encrypted data and the data should be inserted from Server A using a SP to insert data to server B The Master Key,certificate and the Symmetric key has been created on Server B.I created a SSIS package which has a connection to serverB and run the following commands

OPEN SYMMETRIC KEY Keyvalue
DECRYPTION BY CERTIFICATE certvalue

and then run the following insert stmt on ServerA

INSERT INTO serverB.DB.dbo.tableB
(
MemID,
SSN)

SELECT ENCRYPTBYKEY(KEY_GUID('Keyvalue'),
CONVERT(VARBINARY(256), MemId)),
ENCRYPTBYKEY(KEY_GUID('Por_Mem_UytRfvg598'), CONVERT(VARBINARY(256), SSN))
from DB..tableA

but the encryption process wouldnt work .Please advice if this approach is right or any other way to inser the encrypted data to serverB and be able to decrypt successfully

Reply

Aparna | **April 28, 2010 at 2:12 am**

I have a situation where the data should go encrypted from one server to another

Server B should have the encrypted data and the data should be inserted from Server A using a SP to insert data to server B The Master Key,certificate and the Symmetric key has been created on Server B.I created a SSIS package which has a connection to serverB and run the following commands

OPEN SYMMETRIC KEY Keyvalue
DECRYPTION BY CERTIFICATE certvalue

and then run the following insert stmt on ServerA

```
INSERT INTO serverB.DB.dbo.tableB
(
MemID,
SSN)

SELECT ENCRYPTBYKEY(KEY_GUID('Keyvalue'),
CONVERT(VARBINARY(256), MemId)),
ENCRYPTBYKEY(KEY_GUID('Keyvalue'), CONVERT(VARBINARY(256), SSN))
from DB..tableA
```

but the encryption process wouldnt work .Please advice if this approach is right or any other way to inser the encrypted data to serverB and be able to decrypt successfully

Reply

walid | **May 17, 2010 at 4:55 pm**
when i try to write in SQL2005 Management studio new query

```
USE EncryptTest
GO
CREATE MASTER KEY ENCRYPTION
BY PASSWORD = 'SQLAuthority'
GO
```

Line 1: Incorrect syntax near 'MASTER'.

why? what is wrong here?
and if option to active for this issue inside SQL2005 or it work without settings please advice

Reply

An | **May 23, 2010 at 7:03 am**
I want to distribute key to users! please tell me way to distribute key. Thanks you!

Reply

Adam | **July 9, 2010 at 3:05 pm**
Pinal Dave

Hello

I am havibg problems restoring a db, that has been encpted. I noticed in object explorer my Db does not have a + next to it. I cannot restore or detach it. Not sure how to recover. Any help would be very much appriciated.

Thank you

Reply

REV | <u>September 4, 2010 at 3:35 pm</u>

Hello

Column (or Row) Level encryption is not a Transparent one not so?

i.e when using C# application the encryption must be done at the level of code not in sql server.

Is this true? if not how could i deal with encryted data column from C# application?

<u>Reply</u>

Yogendra | <u>October 4, 2010 at 1:02 pm</u>

How can we encrypt the integer data in a column in sql server 2005.

<u>Reply</u>

keerthika | <u>November 11, 2010 at 9:26 am</u>

Your tutorials are really very good

<u>Reply</u>

Tom | <u>December 16, 2010 at 5:31 pm</u>

In sybase we have column level encrypt/ decrypt based on user role. Do we have the same in sqlserver 2008.

sybase code :-

grant decrypt on [owner.]tablename[(columnname [{,columnname}])]
to user | group | role

<u>Reply</u>

Aakash | <u>January 9, 2011 at 1:35 pm</u>

Is it possible to encrypt the Numeric fields? I am using the sql server 2008 workgroup editon.

<u>Reply</u>

Gagan | <u>March 9, 2011 at 8:55 am</u>

Hi ,

Thanks for the information. There is one more thing that, what if someone wants to change the Algorithm for master key creation ?
When you create a master key it automatically gets created with "T DES". The syntax of creating a master key is:

CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'somepassword'

What if someone wants it to be "AES". Can that be done. I have surfed through various resources but could not find anything.

Thanks and Regards
Gagan

Reply

Salman Kazi | **March 18, 2011 at 3:20 am**

Once we are done with the encrypthion, finally you are dropping the column. After that how I am going to insert a new record.

Reply

sathish | **May 31, 2011 at 10:17 am**

Hi Pinal,

Very Nice Article to start the encryption of column in the table.
Its my turn to work with encryption column in my project.
I search lot of articles but i found a good article from you.
Great Going…

Thanks
With Warm Regards
Sathish. P

Reply

mahesh | **June 15, 2011 at 6:36 pm**

thanks…

Reply

mobin19 | **June 16, 2011 at 6:27 pm**

Hi Pinal,

I have a situation, where I made a script of my original database (along with data) using Database publishing wizard and I ran that script on another computer, but my encryption keys were been scripted.

I even tried backing up the encryption keys and restored the keys to another computer in a similar fashion as told by Asif.S in the comments. But still I am not able to decrypt the data, i get null as the decrypted data. Please help me ASAP.

Regards,
Mobin Molai.

Reply

Rahul | **July 18, 2011 at 7:06 pm**

How to Decrypt data in sql which was already store in by MD5 algo using 123 as key….

Reply

joan | **August 16, 2011 at 12:55 pm**

Is it possible to decrypt a data without knowing how the file was encrypted?

Reply

Ashish | **August 21, 2011 at 1:36 am**

Is it possible to encrypt /Decrypt XML data in SQL server 2005 ?

Reply

Dayo | **September 28, 2011 at 7:15 am**

Please I have a big problem at hand at my new job. The problem is that I discovered that the application is encrypting all the primary key in the database. And I don't have no information on how to decrypt from the backend and my company's contract with the people that developed the application has long expired. So get them to make changes to the application will cost a lot. I need help on how to go about it if there is anyway at all without going back to the developer.

Reply

madhivanan | **September 28, 2011 at 5:12 pm**

Do you have source for the application? You can debug the application to know what type of encrption is used

Reply

sabahmed | **October 9, 2011 at 11:41 pm**

How to encrypt a column having datatype timestamp???

Reply

Jatin Soni | **October 31, 2011 at 11:51 pm**

Hi Pinal,

My client wants to have ssh2 encryption. I can't find this encryption in allowed list of sql encryption. Can u let me know if there is any way to impliment this in sql.

Reply

Ramya | **November 16, 2011 at 10:56 pm**

Hi Pinal,
Your Information is very useful. I created,

```
IF NOT EXISTS
(SELECT * FROM sys.symmetric_keys WHERE symmetric_key_id = 101)
CREATE MASTER KEY ENCRYPTION BY
PASSWORD = 'xxxxx password'
GO

CREATE CERTIFICATE PCredit
WITH SUBJECT = 'Credit Card Numbers';
GO

CREATE SYMMETRIC KEY CreditCards_Key11
WITH ALGORITHM = AES_256
ENCRYPTION BY CERTIFICATE PCredit;
GO
```

This is done in development machine.
I usually take sql database backup and restore in QA server to test.

When i did the sql backup I didnot find the certificate and symmetric keys in QA server.

How do I take the back up of the certificte and symmetric keys and restore in QA server.

Thank you.

Reply

meric | **November 21, 2011 at 8:07 pm**
Hello Mr Pinal,

There is so weird case when i attempt to encrypt a clear text with a SymmetricKey… Anytime when i try to encrypt the "same" data with the "same" SymmetricKey, then encrypted data is resulted diffenet (different 128bytes of data).. However i can successfully get back the orjinal cleare data, i kindly ask you to the way to get the "same" encrypted when i encrypt the "same" data with the "same" SymmetricKey ? Is that possible ?

Reply

fa | **December 19, 2011 at 1:47 pm**
difference stroed procedure with function?

Reply

sanket | **December 26, 2011 at 4:54 pm**
hi pinal,
suppose am inserting new row to employee table. i want encrypted version of ssn column. is it possible to encrypt ssn at the time of inserting new data to table ? thanx for any help..

Reply

amin | **January 15, 2012 at 10:08 pm**

hi
I wil use of encrype sql server in login but I dont Kwon .you can Help me
with image and discription

thanks

Reply

Prakash Somasundaran | February 2, 2012 at 5:51 pm

Hi,

I have an situation I want encrypted data to be able to get through a select statement.

eg:Select Co1,Col2,encrypt(Amount) as Col3,Col4 from PS_TABLE.

We have a people soft application where data needs to be encrypted,it should be available to all other applications thru mere select statement .

I should be able to include create keys,open keys inside a function.This is not possible.Or else I should be able to call a stored procedure inside function.This is also not possible.

Any help appriciated.

Thanks in advance,

Prakash

Reply

sue | February 14, 2012 at 12:24 am

Prakash – do you actually mean decrypt? I cannot understand why you would want to display encrypted data? What is the purpose of displaying something if no one can read it?

Reply

Peter | February 15, 2012 at 11:49 pm

Pinal, thank you for that great article. I have a (possibly stupid) beginner follow-up question, if possible.

In your article, you say to do this to decrypt and read the data.

OPEN SYMMETRIC KEY TestTableKey DECRYPTION
BY CERTIFICATE EncryptTestCert
SELECT CONVERT(VARCHAR(50),DECRYPTBYKEY(EncryptSecondCol)) AS
DecryptSecondCol
FROM TestTable

Fine. This works great. Here is the question:

How is this safe ? Can't any stranger with access to the system run this SQL statement ?? Yes, hopefully, access is restricted appropriately. But that covers security for the entire database. If we want to provide extra security to a particular column, presumably it's because database access was penetrated somehow.

In other words, if you have access to the database, don't you ALSO have access to the encrypted data, give the SQL statement above ??

Thanks so much if you can address this!!!

<u>Reply</u>

Prakash Somasundaran | <u>February 16, 2012 at 5:21 pm</u>
Let me post the same mail with better explanation:

We have a situation like this:
We have a peoplesoft database which has a column called ps_amount which should be hidden.We want to encrypt this field.
We decided to go with SQL Server Symmetric encryption.
Now we have down stream applications which will read data from people soft.
We want down stream applications to be able to read from the table using a view.
The view should look like this select col1,col2,encrypt(col3),col4 from PS_TABLE.
Which means that encrypt should be coded as follows:
I should be able to include the code for create keys(master,certificate and symmetric keys),open keys(symmetric keys) inside a function.This is not possible because CREATE KEY ,OPEN KEY statements are not allowed in a function.
Or else I should be able to call a stored procedure inside function.But calling a stored procedure inside function is not allowed.
We tried the possibility of SELECT trigger in SQL where we could add this code for create keys & open keys.But SELECT trigger feature is not available in SQL Server.
We even tried Login Triggers.But in Login triggers the open key is available only in that session.The whole trigger is a batch.Thus encrypt function will give an error.
We also need a Decrypt function which should work in similar fashion.

<u>Reply</u>

Prakash Somasundaran | <u>February 16, 2012 at 5:23 pm</u>
Hi Everyone,

Let me post the same mail with better explanation:

We have a situation like this:
We have a peoplesoft database which has a column called ps_amount which should be hidden.We want to encrypt this field.
We decided to go with SQL Server Symmetric encryption.
Now we have down stream applications which will read data from people soft.
We want down stream applications to be able to read from the table using a view.
The view should look like this select col1,col2,encrypt(col3),col4 from PS_TABLE.
Which means that encrypt should be coded as follows:
I should be able to include the code for create keys(master,certificate and symmetric keys),open

keys(symmetric keys) inside a function.This is not possible because CREATE KEY ,OPEN KEY statements are not allowed in a function.
Or else I should be able to call a stored procedure inside function.But calling a stored procedure inside function is not allowed.
We tried the possibility of SELECT trigger in SQL where we could add this code for create keys & open keys.But SELECT trigger feature is not available in SQL Server.
We even tried Login Triggers.But in Login triggers the open key is available only in that session.The whole trigger is a batch.Thus encrypt function will give an error.
We also need a Decrypt function which should work in similar fashion.

Thanks,

Prakash
Database Architect.

Reply

Rajesh Lohakare | February 23, 2012 at 1:58 pm

Hi Pinal,

I have a database in which the data is encrypted.now i want to restore that database on another instance of SqlServer.But i dont know master key Password.Is there any way to get master key password.

Thanks in advance.

Rajesh Lohakare

Reply

sara | February 25, 2012 at 6:39 pm

hi Pinal ,,,thank you for that great article . I did a simple instance , every thing is fine but when i dettach db & move it to the other SQL server with out certificate, it is attached very simple, Am i wrong? what's the problem?

Reply

ajmal kahn | March 3, 2012 at 1:20 pm

yeah it's fine.

can you tell me how to insert the data in sql server 2005 in encryption format
.
if you know the answer .please contact me at this e-mail address.
[email removed]

Reply

usmi | March 12, 2012 at 9:15 pm

Okay, what I lost/forgot my key or certificate password ??

Pls advise how could I Recover my passwords or Data etc..

Reply

Brian Y | **June 7, 2012 at 8:18 pm**

Do you do any kind of on-site workshops or classes around the US? I would love to pay and participate…

Reply

muzammil | **June 12, 2012 at 2:16 pm**

when i select the encrypted column,it shows only one character from each word

Reply

vilastips2invest | **April 12, 2013 at 11:40 pm**

muzammil, did you ever get this solved, i am having the same problem, let me know how, thanks.

Reply

ASHVIN | **June 29, 2012 at 11:57 am**

HI I HAVE PROBLEM IN RETRIEVE DATA AFTER ENCRYPTION…
I FIRST ENCRYPT DATA THEN DROP SYMMETRIC KEY AND CERTIFICATE
NOW I WANT TO DECREPIT THAT DATA ..BUT IT GIVES NULL VALU..
PLZ SUGGEST

Reply

Spark | **July 12, 2012 at 12:26 pm**

The process of moving encrypted database seems to be incorrect. it shows use master to create master key but we created master key in user database and not in master db. also after restoring DB, when we eecute create certifiate, it gives error open master key.

Reply

ugo | **July 18, 2012 at 1:42 pm**

Hi Guys,
when one wants to encrypt the whole databases on ones server, does one encrypt the model and msdb database as well? or is it's encryption covered my the Master key and tempdb encryption?

Reply

sony | **July 31, 2012 at 9:58 pm**

Hi Pinal – Great article. How do I retain the same encrypted value if the source values are same

Reply

Mike | **August 10, 2012 at 3:41 am**

Do the keys used for database encryption expire? Or, once you set up db level encryption can you leave it alone forever?

Reply

Syam Mohan P | **August 13, 2012 at 1:12 pm**

Hi Pinal,

This article is good and working fine with verchar and nvarchar datatypes. But my question is, i can see the key and certificate name in the secuirty part. So anyone can decrypt the data by see the name of the key and certificate right with the below script.

```
USE EncryptTest
GO
OPEN SYMMETRIC KEY TestTableKey DECRYPTION
BY CERTIFICATE EncryptTestCert
SELECT CONVERT(VARCHAR(50),DECRYPTBYKEY(EncryptSecondCol)) AS
DecryptSecondCol
FROM TestTable
GO
```

[email removed]

Thanks in advance.

Regards
Syam Mohan P
Rober BOSCH Engineering and Business Solutions

Reply

denny | **August 31, 2012 at 12:34 pm**

Hi pinal Dave,
Good artice helped a lot thanks for the post

Reply

Niraj | **September 17, 2012 at 8:42 pm**

I am trying applying AES 256 bit encryption(SYM KEY) on an existing DB on SQL server 2005.

I successfully applied encryption/decryption anyhow (Thanks to this article). But I suffered, because I have changed around 100 tables in DB, using cursor, to change the actual column datatypes to VARBINARY(max).

As you know, this impacted the existing DB procedures and triggers applied on these tables. I don't want to change the procedures again.

Could anyone please suggest me applying the encryption with out changing the schema?

For example, once we get the encrypted binary data, can we CONVERT/CAST them into VARCHAR and UPDATE the existing column itself(i.e. still in encrypted varchar format), and later applying varchar to varbinary format followed by actual AES decryption?

Reply

Niraj | September 17, 2012 at 9:25 pm

Its worked for me. The column was showing blank for select column.
I tried as below:

Encryption
— — — — — — —

OPEN SYMMETRIC KEY TableEncrKey_AES256 DECRYPTION
BY CERTIFICATE EncryptDBCert
UPDATE myTable SET col_actual_invarchar =
CONVERT(varchar(max),ENCRYPTBYKEY(KEY_GUID('TableEncrKey_AES256'),col_actual_inv

Decryption
— — — — — — —-
OPEN SYMMETRIC KEY TableEncrKey_AES256 DECRYPTION BY CERTIFICATE
EncryptDBCert SELECT CONVERT(VARCHAR(max),DECRYPTBYKEY(col_actual_invarchar))
FROM abcde_new

Reply

gen | October 4, 2012 at 12:03 pm

when i follow the above steps, in last steps only return 1 character. my original string is 5 characters long. so after encrypt, i get decrypted string only 1 character.

Reply

ay7agafay7taimaa | October 18, 2012 at 4:57 pm

what if I want to insert value to the encrypted column and select it again with decrypt

Reply

Arunprasath | October 21, 2012 at 12:38 pm

Sir,
When I am creating Database Master Key, the following error occurs.
Kindly suggest.

Msg 15466, Level 16, State 2, Line 1
An error occurred during decryption.

Reply

svk | December 1, 2012 at 7:53 am

using below for decrypting , but gett an error

```
AS
BEGIN

SET NOCOUNT ON;
OPEN SYMMETRIC KEY SymmetricKey1
DECRYPTION BY CERTIFICATE Certificate1 WITH PASSWORD = 'Password';
SELECT CAST(DECRYPTBYKEY(kcode) as varchar(250))
FROM keycode
CLOSE SYMMETRIC KEY SymmetricKey1;
END
```

error

The private key password is invalid.

The key 'SymmetricKey1' is not open. Please open the key before using it

Reply

Paul | **December 6, 2012 at 8:11 pm**

Awesome work here. A huge help for me! Much appreciated!

Reply

Rahul Saxena | **December 12, 2012 at 1:11 pm**

sir i want to kn that how to secure TestTableKey, EncryptSecondCol.
if a preson known this sql qurrey ……..OPEN SYMMETRIC KEY TestTableKey DECRYPTION
BY CERTIFICATE EncryptTestCert
SELECT CONVERT(VARCHAR(50),DECRYPTBYKEY(EncryptSecondCol)) AS
DecryptSecondCol
FROM TestTable…………..then find original SecondCol ………
plz how to secure dis pint…………………

Reply

Shamim | **January 13, 2013 at 3:49 pm**

Hi thanks, well explanation…

Reply

joe | **January 15, 2013 at 5:39 am**

i have created 3 sql triggers using sql 2008 r2 64 bit. the backup server containing the unencrypted triggers has been lost. I do have the key used when creating the trigger. Is there a way to regain the code, like scripting it out or removing the encryption key just long enough to back it up and then re-apply the encryption?

Reply

Navaneeth | **February 9, 2013 at 2:57 pm**

In this article the Symmetric Key and Triple DES encryption is used.But if i go to SSMS then i can see 'EncryptTestCert'(certificate used in this article) can be easily found in certificate folder and 'TestTable'(symmetric key) can be found in symmetric keys folder in SSMS under that database. So anyone who can login to SSMS can easily decrypt database by using it. So how it can be prevented? Also any other methods?

Reply

sundar | March 11, 2013 at 3:36 pm

I had try to encrypt password by using md5() but i got this error "'MD5' is not a recognized built-in function name. ".. what is the problem sir.. can you please help me..

Reply

Jennifer | March 16, 2013 at 11:50 am

hi.
My group has to do a real time project for our institute nd its based on library management. I have been given the task to handel the data base. other group members are doing the user end design using VB-2012. im using SQL server 2005. I ve created the loing in tabel but need to put password encryption. nd need to make the userid as the master key. can you plz help.
Hoping to get a early response.

Tank you.

Reply

samba | April 2, 2013 at 4:55 pm

if i want encrypt password at time of insertion then what is the way? can you give me a suggestion. thank you

Reply

Poov | April 24, 2013 at 2:12 am

If you want to encrypt "Password" filed,
1) define the datatype varbinary(256) at the time of creation itself.
2) Create Db Master Key / Certificate and Symmetric Key
3) Insert by using ENCRYPTBYKEY(KEY_GUID('TestTableKey'),'givnPassword')

when you want to validate the value need to be decript.

Reply

Pingback: SQL SERVER – Weekly Series – Memory Lane – #027 | SQL Server Journey with SQL Authority

Dennis Miller | May 4, 2013 at 4:46 pm

Awesome your blog like it

Reply

Ahmed Abdi | May 20, 2013 at 2:13 pm

thanks pinal for you clear explanation. really it is helpfull

Reply

Poov | May 30, 2013 at 12:27 am

Thanks for this article. When I modify the existing view after encryption of a column, it gives error. any help …..? The view is given below:

CREATE VIEW [dbo].[v_Users_Pin]
AS

OPEN SYMMETRIC KEY sym_my_Key DECRYPTION
BY CERTIFICATE my_Certificate

SELECT
UserID
, Owner_No
, CONVERT(VARCHAR(8),DECRYPTBYKEY(PIN)) AS PIN
FROM dbo.Users

CLOSE SYMMETRIC KEY sym_my_Key

GO
— — — — — — — — —–
when i Parse it gives the following error: (it seems it is expecting SELECT work after "AS")
Incorrect syntax near the keyword 'OPEN'.

Thanks in advance

Reply

venkata | June 1, 2013 at 12:41 am

can someone tell me if I can have clustered indexed column and I wanted that to be encrypt it. If I do a search on that column – will it work fine. if not please suggest an approach. thanks in advance.

Reply

Blog at WordPress.com. | Customized Misty Lake Theme.