# Lab: Data Encryption

- This is worth 10 points.
- The due date is Saturday, April 4 Midnight.
- Use the following naming convention: homework, underscore, last name, first initial, and extension (e.g., Lab_Encrypt_ImG.docx).

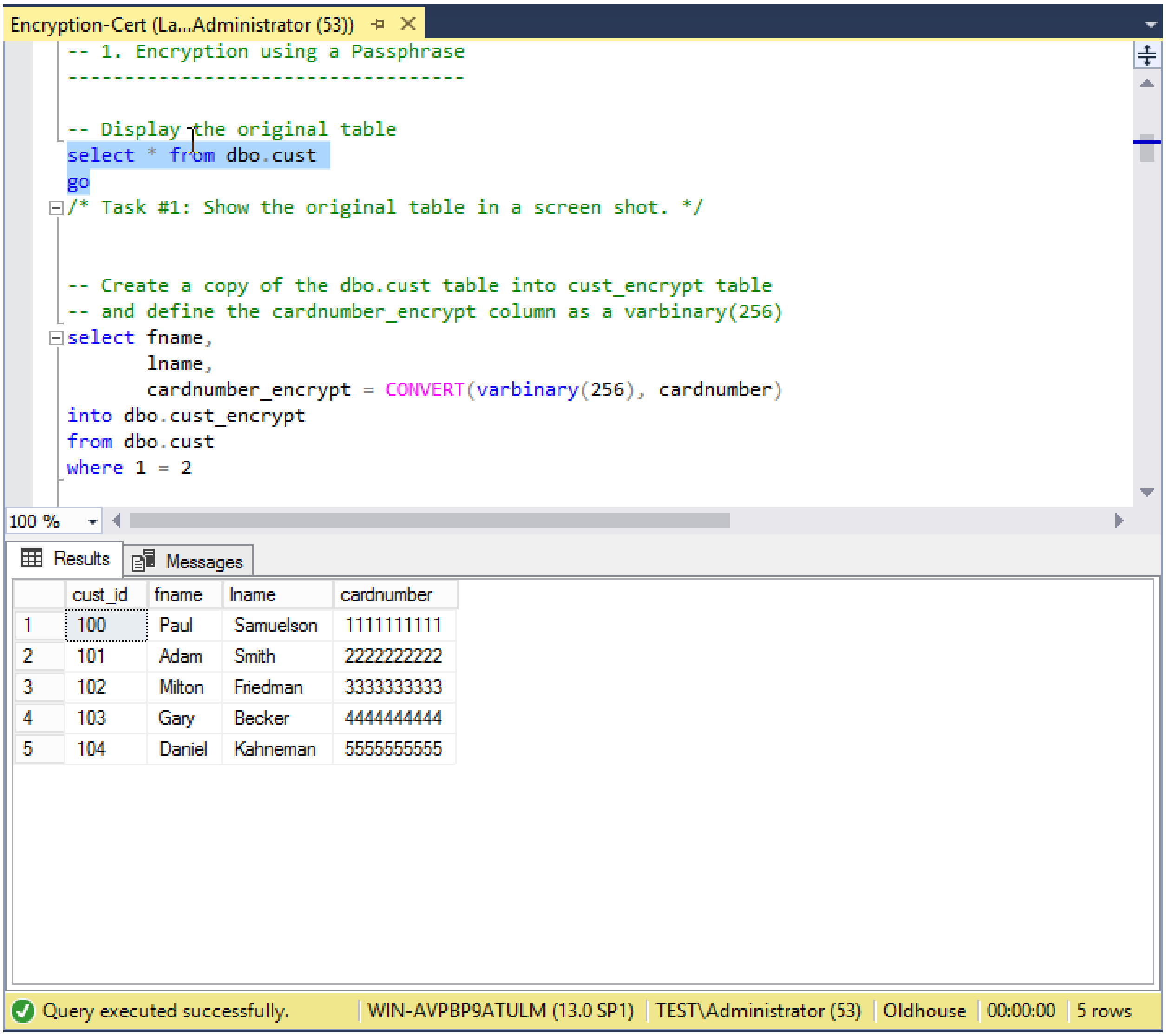
## 1. Preparation

First, if your SQL Server does not have Oldhouse database, create it using this script: **Oldhouse-Table-Create (Lab).sql**.

Next, perform the lab using this script: **Encryption-Cert (Lab).sql**.

## 2. Deliverables

```
-- Display the original table
select * from dbo.cust
go
/* Task #1: Show the original table in a screen shot. */
```

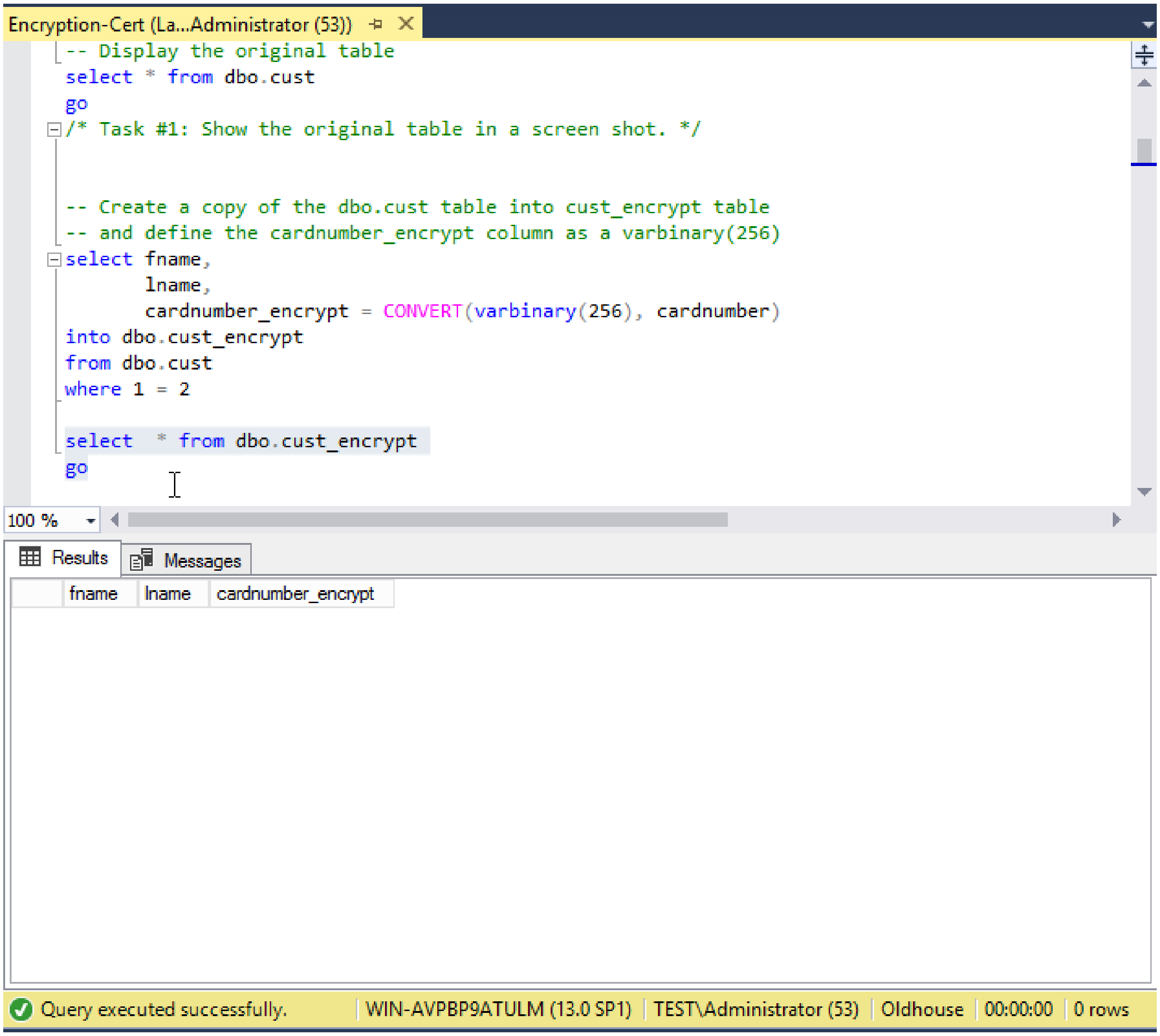


```
-- 1. Encryption using a Passphrase
-----------------------------------

-- Display the original table
select * from dbo.cust
go
/* Task #1: Show the original table in a screen shot. */


-- Create a copy of the dbo.cust table into cust_encrypt table
-- and define the cardnumber_encrypt column as a varbinary(256)
select fname,
       lname,
       cardnumber_encrypt = CONVERT(varbinary(256), cardnumber)
into dbo.cust_encrypt
from dbo.cust
where 1 = 2
```

| | cust_id | fname | lname | cardnumber |
|---|---|---|---|---|
| 1 | 100 | Paul | Samuelson | 1111111111 |
| 2 | 101 | Adam | Smith | 2222222222 |
| 3 | 102 | Milton | Friedman | 3333333333 |
| 4 | 103 | Gary | Becker | 4444444444 |
| 5 | 104 | Daniel | Kahneman | 5555555555 |

✓ Query executed successfully. | WIN-AVPBP9ATULM (13.0 SP1) | TEST\Administrator (53) | Oldhouse | 00:00:00 | 5 rows

```
-- Display the encrypted table
select * from dbo.cust_encrypt
go
```



```sql
-- Display the original table
select * from dbo.cust
go
/* Task #1: Show the original table in a screen shot. */


-- Create a copy of the dbo.cust table into cust_encrypt table
-- and define the cardnumber_encrypt column as a varbinary(256)
select fname,
       lname,
       cardnumber_encrypt = CONVERT(varbinary(256), cardnumber)
into dbo.cust_encrypt
from dbo.cust
where 1 = 2

select  * from dbo.cust_encrypt
go
```

| | fname | lname | cardnumber_encrypt |
|---|---|---|---|

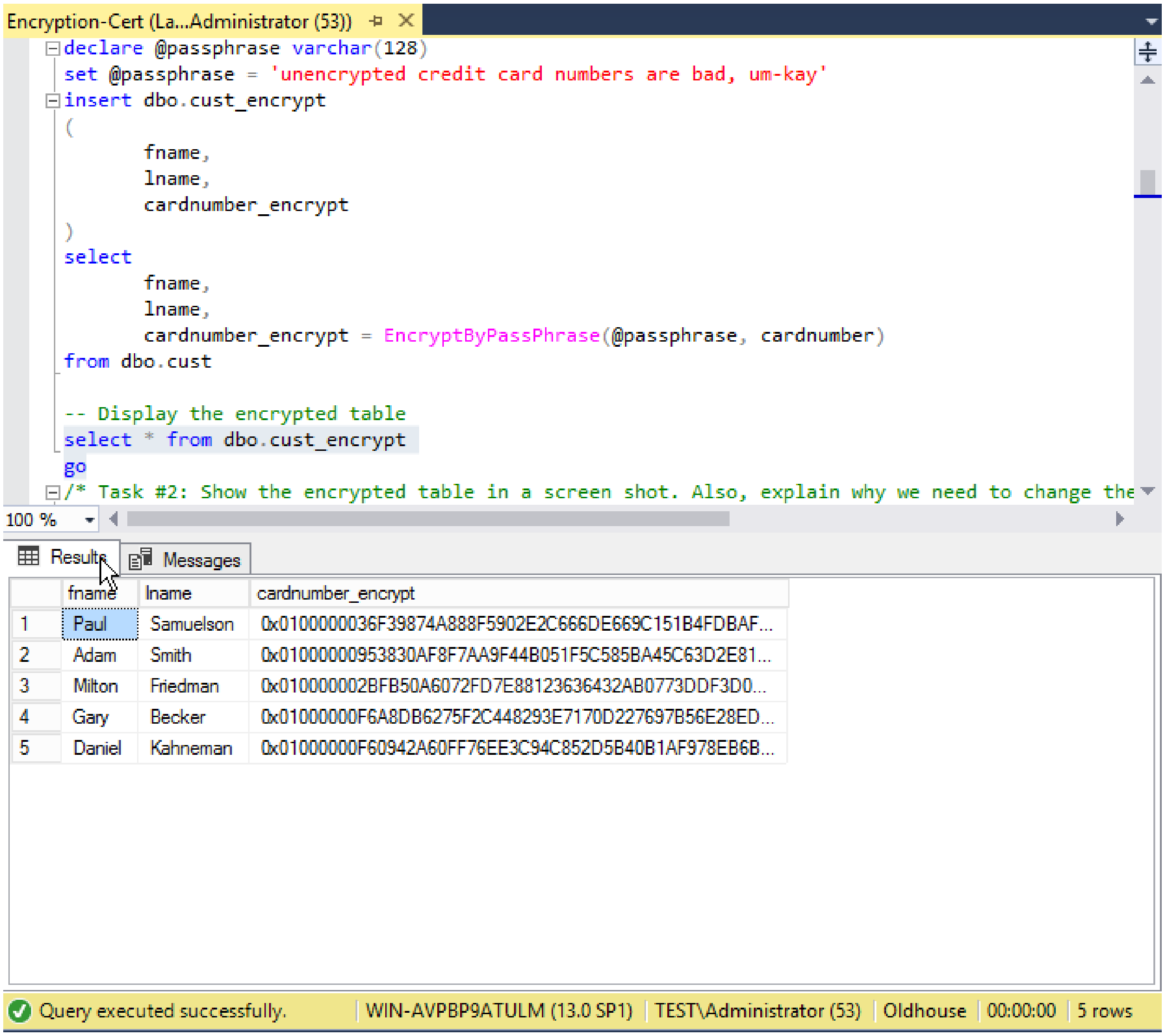
Query executed successfully. | WIN-AVPBP9ATULM (13.0 SP1) | TEST\Administrator (53) | Oldhouse | 00:00:00 | 0 rows

```sql
/* Task #2: Show the encrypted table in a screen shot. Also, explain why we need to
change the data type for encryption. */
```

So we made a new table with a new row cardnumber_encrypt where we stored the card numbers of users encrypted .

We needed to change the data type for encryption in order to use the encryptbypass phrase function so that we can encrypt the new data in the new cust encrypt table. And so that we can populate the new table.

```sql
-- Display the encrypted table
select * from dbo.cust_encrypt
go
```



```
declare @passphrase varchar(128)
set @passphrase = 'unencrypted credit card numbers are bad, um-kay'
insert dbo.cust_encrypt
(
        fname,
        lname,
        cardnumber_encrypt
)
select
        fname,
        lname,
        cardnumber_encrypt = EncryptByPassPhrase(@passphrase, cardnumber)
from dbo.cust

-- Display the encrypted table
select * from dbo.cust_encrypt
go
/* Task #2: Show the encrypted table in a screen shot. Also, explain why we need to change the
```

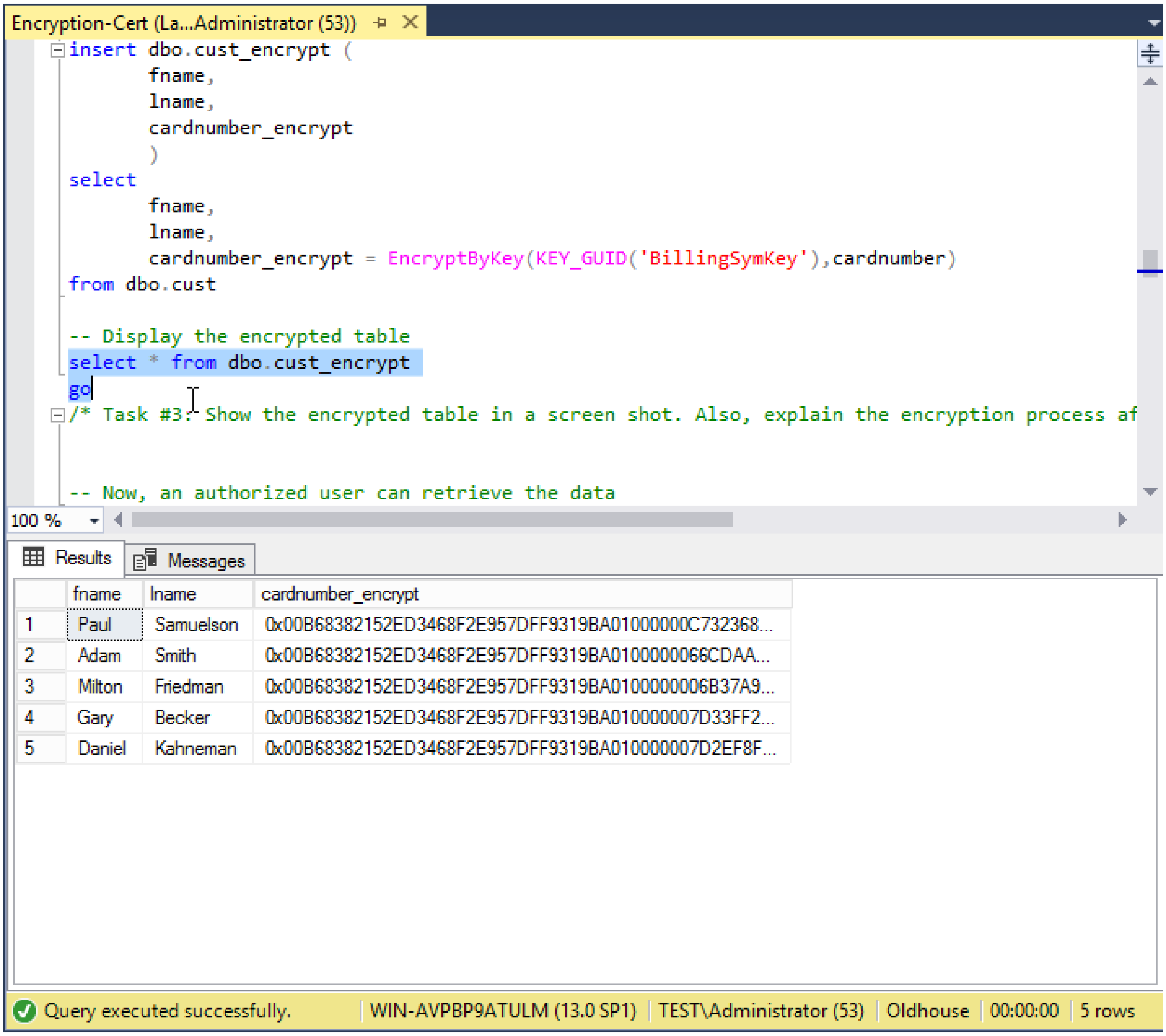
|  | fname | lname | cardnumber_encrypt |
|---|---|---|---|
| 1 | Paul | Samuelson | 0x0100000036F39874A888F5902E2C666DE669C151B4FDBAF... |
| 2 | Adam | Smith | 0x01000000953830AF8F7AA9F44B051F5C585BA45C63D2E81... |
| 3 | Milton | Friedman | 0x010000002BFB50A6072FD7E88123636432AB0773DDF3D0... |
| 4 | Gary | Becker | 0x01000000F6A8DB6275F2C448293E7170D227697B56E28ED... |
| 5 | Daniel | Kahneman | 0x01000000F60942A60FF76EE3C94C852D5B40B1AF978EB6B... |

Query executed successfully. | WIN-AVPBP9ATULM (13.0 SP1) | TEST\Administrator (53) | Oldhouse | 00:00:00 | 5 rows

```
/* Task #3: Show the encrypted table in a screen shot. Also, explain the encryption
process after Task #2. */
```

In this task we encrypted the data using Certificate, we first executed the command to create a master key with an encrypted password and then we created the certificate in the oldhouse database, and then we cleared out the table by truncating it and then we used the Certificate to decrypt the key and then we made the rows using the key and encrypted it.

```
-- Display the decrypted table
select fname,
          lname,
          cardnumber = convert(nvarchar(25), DecryptByKey(cardnumber_encrypt))
from dbo.cust_encrypt
go
```



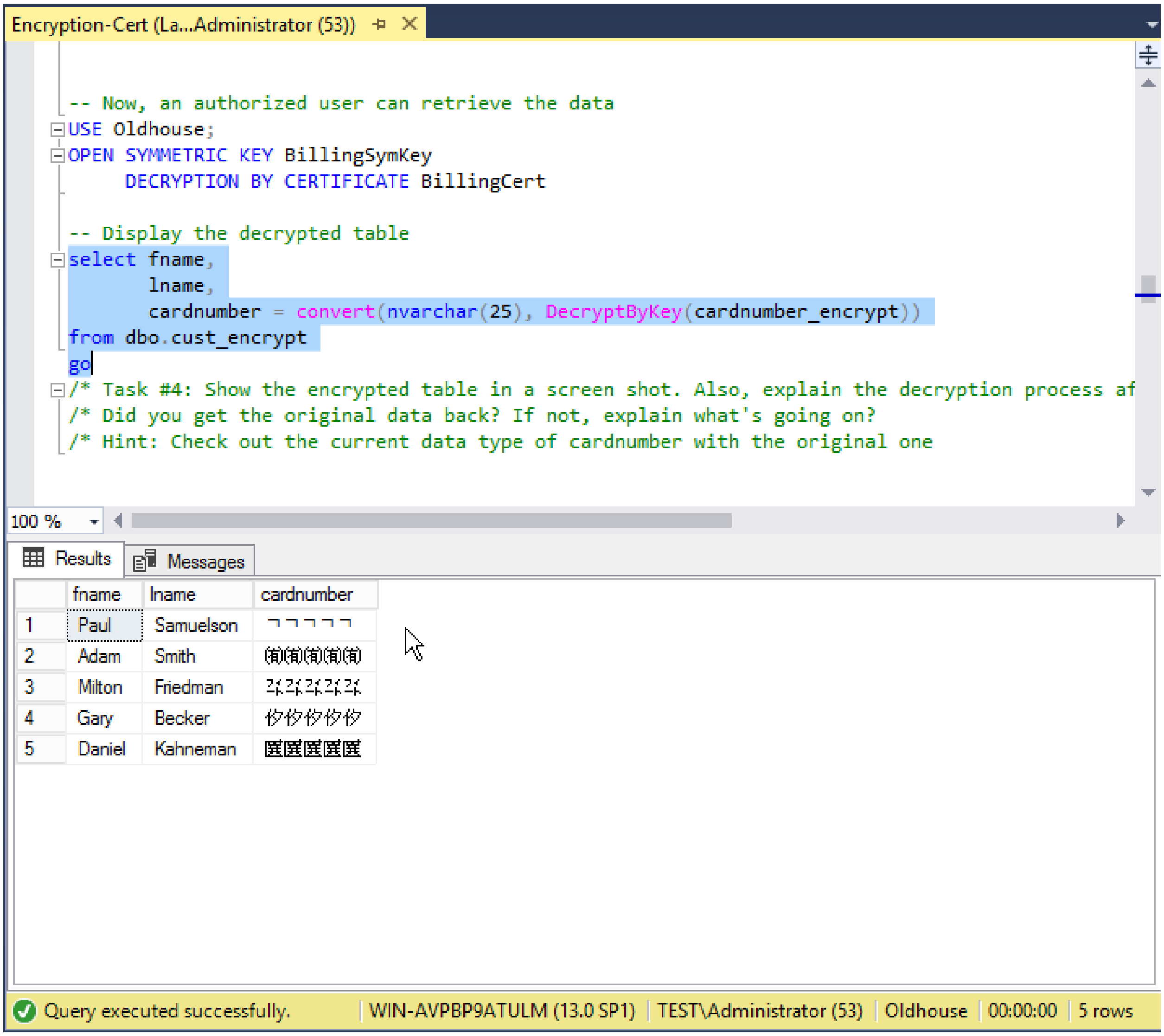
```
insert dbo.cust_encrypt (
        fname,
        lname,
        cardnumber_encrypt
        )
select
        fname,
        lname,
        cardnumber_encrypt = EncryptByKey(KEY_GUID('BillingSymKey'),cardnumber)
from dbo.cust

-- Display the encrypted table
select * from dbo.cust_encrypt
go
/* Task #3: Show the encrypted table in a screen shot. Also, explain the encryption process af


-- Now, an authorized user can retrieve the data
```

|   | fname | lname | cardnumber_encrypt |
|---|---|---|---|
| 1 | Paul | Samuelson | 0x00B68382152ED3468F2E957DFF9319BA01000000C732368... |
| 2 | Adam | Smith | 0x00B68382152ED3468F2E957DFF9319BA0100000066CDAA... |
| 3 | Milton | Friedman | 0x00B68382152ED3468F2E957DFF9319BA0100000006B37A9... |
| 4 | Gary | Becker | 0x00B68382152ED3468F2E957DFF9319BA010000007D33FF2... |
| 5 | Daniel | Kahneman | 0x00B68382152ED3468F2E957DFF9319BA010000007D2EF8F... |

```
Query executed successfully.    WIN-AVPBP9ATULM (13.0 SP1)    TEST\Administrator (53)    Oldhouse    00:00:00    5 rows
```

/* Task #4: Show the encrypted table in a screen shot. Also, explain the decryption process after Task #3.      */

As an authorized user we were able to retrieve data by using the oldhouse database and we were able to display the decrypted table as an authorized user with the key.



```
-- Now, an authorized user can retrieve the data
USE Oldhouse;
OPEN SYMMETRIC KEY BillingSymKey
     DECRYPTION BY CERTIFICATE BillingCert

-- Display the decrypted table
select fname,
       lname,
       cardnumber = convert(nvarchar(25), DecryptByKey(cardnumber_encrypt))
from dbo.cust_encrypt
go
/* Task #4: Show the encrypted table in a screen shot. Also, explain the decryption process af
/* Did you get the original data back? If not, explain what's going on?
/* Hint: Check out the current data type of cardnumber with the original one
```

|  | fname | lname | cardnumber |
|---|---|---|---|
| 1 | Paul | Samuelson | ㄱㄱㄱㄱㄱ |
| 2 | Adam | Smith | ㈲㈲㈲㈲㈲ |
| 3 | Milton | Friedman | [illegible] |
| 4 | Gary | Becker | 伇伇伇伇伇 |
| 5 | Daniel | Kahneman | 匿匿匿匿匿 |

Query executed successfully. | WIN-AVPBP9ATULM (13.0 SP1) | TEST\Administrator (53) | Oldhouse | 00:00:00 | 5 rows

```
/* Did you get the original data back? If not, what's wrong?                */
/* Hint: Check out the current data type of cardnumber with the original one   */
```

We did not get the original data back because the card number column was changed due to using a different key the first time to encrypt it we used EncryptByPassPhrase and then in task 3 we used Encrypt ByKey so there was two encryptions, which was the reason why when we decrypted it the results were not the same as the original.