

Lab: SQL Server Encryption

- This is an in-class lab, and worth 10 points.
- The due date is Thursday, April 5 Midnight.
- Use the following naming convention: homework, underscore, last name, first initial, and extension (e.g., Lab_Encrypt_ImG.docx).

1. Preparation

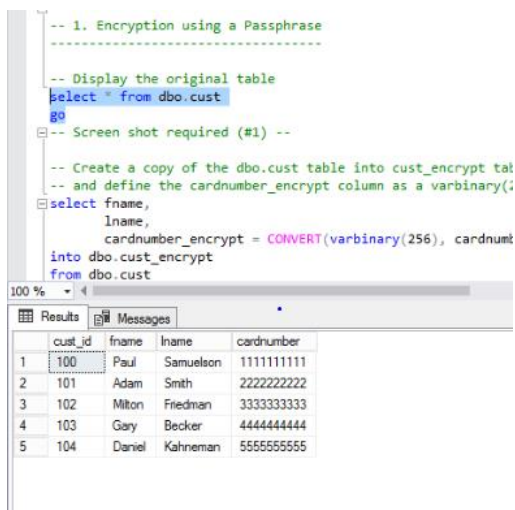
First, if your SQL Server does not have Oldhouse database, create it using this script: **Oldhouse-Table-Create (Lab).sql**.

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

2. Deliverables

- Report the results using screenshots as indicated.

```
-----  
-- 1. Encryption using a Passphrase  
-----  
  
-- Display the original table  
select * from dbo.cust  
go  
-- Screen shot required (#1) --
```



```
-- Display the encrypted table
```

```
select * from dbo.cust_encrypt
go
-- Screen shot required (#2) --
```

-- Display the encrypted table

```
select * from dbo.cust_encrypt
go
-- Screen shot required (#2) --
```

	fname	lname	cardnumber_encrypt
1	Paul	Samuelson	0x010000007E667827F2A6E52CBB7D3234FB400E2E5DDE8A...
2	Adam	Smith	0x0100000084872B45713ABABAD75C1644295C38F282F2267...
3	Milton	Friedman	0x01000000198C89F367D07AE965A3A29CE04BA48E7393AA4...
4	Gary	Becker	0x01000000028EA921A669032F652B31AA49841C82553E4D6...
5	Daniel	Kahneman	0x01000000A0E9984FB34337241D238173C7D821F6123F0AD...

-- 2. Encryption using Certificate

```
-- Display the encrypted table
select * from dbo.cust_encrypt
go
-- Screen shot required (#3) --
```

-- Display the encrypted table

```
select * from dbo.cust_encrypt
go
-- Screen shot required (#3) --

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

select fname,
       lname,
       cardnumber = convert(nvarchar(25), DecryptByKey(cardnumber_encrypt))
from dbo.cust_encrypt
go
```

	fname	lname	cardnumber_encrypt
1	Paul	Samuelson	0x00A96902E1B5FC4C9E3983C1D517D46801000000E89BA2...
2	Adam	Smith	0x00A96902E1B5FC4C9E3983C1D517D468010000002A1FD17...
3	Milton	Friedman	0x00A96902E1B5FC4C9E3983C1D517D46801000000D1707F7...
4	Gary	Becker	0x00A96902E1B5FC4C9E3983C1D517D46801000000980A37D...
5	Daniel	Kahneman	0x00A96902E1B5FC4C9E3983C1D517D468010000007765F49...

```
select fname,
       lname,
       cardnumber = convert(nvarchar(25), DecryptByKey(cardnumber_encrypt))
from dbo.cust_encrypt
go
-- Screen shot required (#4) --
-- Did you get the original data back? If not, what's wrong? Explain how to
get the original data back.
```

```

Oldhouse-Table-Cre...dministrator (59)* Encryption-Cert (La...Administrator (58))
select * from dbo.cust_encrypt
go
-- Screen shot required (#3) --
-- Now, an authorized user can retrieve the data
USE Oldhouse;
OPEN SYMMETRIC KEY BillingSymKey
    DECRYPTION BY CERTIFICATE BillingCert
select fname,
       lname,
       cardnumber = convert(nvarchar(25), DecryptByKey(cardnumber_encrypt))
from dbo.cust_encrypt
go
-- Screen shot required (#4) --
-- Answer this question: Did you get the original data back? If not, what's wrong?
CLOSE SYMMETRIC KEY BillingSymKey

```

	fname	lname	cardnumber
1	Paul	Samuelson	ררררר
2	Adam	Smith	ררררררררר
3	Milton	Friedman	ררררררררר
4	Gary	Becker	ררררררר
5	Daniel	Kahneman	רררררר

We did not get the original data back because the data type is nvarchar which converts the numbers into Unicode symbols. To get the original data back we would just change nvarchar(25) to varchar(25) in the query like so:

```

select fname,
       lname,
       cardnumber = convert(varchar(25), DecryptByKey(cardnumber_encrypt))
from dbo.cust_encrypt
go

```

```

Oldhouse-Table-Cre...dministrator (59)* Encryption-Cert (La...Administrator (58))
select * from dbo.cust_encrypt
go
-- Screen shot required (#3) --
-- Now, an authorized user can retrieve the data
USE Oldhouse;
OPEN SYMMETRIC KEY BillingSymKey
    DECRYPTION BY CERTIFICATE BillingCert
select fname,
       lname,
       cardnumber = convert(varchar(25), DecryptByKey(cardnumber_encrypt))
from dbo.cust_encrypt
go
-- Screen shot required (#4) --
-- Answer this question: Did you get the original data back? If not, what's wrong?
CLOSE SYMMETRIC KEY BillingSymKey

```

	fname	lname	cardnumber
1	Paul	Samuelson	1111111111
2	Adam	Smith	2222222222
3	Milton	Friedman	3333333333
4	Gary	Becker	4444444444
5	Daniel	Kahneman	5555555555