

## Lab: Data Encryption

- This is worth 5 points and it is due on Saturday at 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 **CISEncrypt** database, create it using this script: **CISEncrypt-Table-Crete (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. */
```

	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

```
-- 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 data type for encryption. */
```

	fname	lname	cardnumber_encrypt
1	Paul	Samuelson	0x010000001A84D43F599901C858FBE01A2873CB796419E37...
2	Adam	Smith	0x010000005896E08C16AF73FAFE01B83D6D942B1C3135B7A...
3	Milton	Friedman	0x010000006343333E888AAEA5BB90E3780CB5A9BE223D7A...
4	Gary	Becker	0x01000000277C485EBCEA84C4D32B428B940354223550339...
5	Daniel	Kahneman	0x0100000045943DD98207EB2243719AD4DC4303DE9F34AF...

We need to change the data type because column/cell level encryption requires the data type to be varbinary in order to encrypt it.

```
-- 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 after Task #2. \*/

	fname	lname	cardnumber_encrypt
1	Paul	Samuelson	0x006FA91963BA50448CE629F85BF114E801000000E2D79B5...
2	Adam	Smith	0x006FA91963BA50448CE629F85BF114E8010000005C8E600...
3	Milton	Friedman	0x006FA91963BA50448CE629F85BF114E8010000006B2AD13...
4	Gary	Becker	0x006FA91963BA50448CE629F85BF114E801000000FEE9AB5...
5	Daniel	Kahneman	0x006FA91963BA50448CE629F85BF114E801000000E0FFA66...

First, we create a certificate with the name BillingCert. Then we create a symmetric key and encrypt it using the BillingCert certificate. We empty the cust\_encrypt table, then we decrypt the symmetric key using the certificate so it can be used for encryption. Then, we enter the info back into the cust\_encrypt table, using the symmetric key to encrypt the cardnumber column.

-- Display the decrypted table

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

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

/\* Did you get the original data back? If not, what is going on? \*/

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

First, we decrypt the symmetric key using the certificate. Then, we convert the encrypted column back to varchar and decrypt it using the symmetric key. Yes, all the original data is there. Except for the customer ID, but only because it wasn't on the list of columns to display in the query.