# 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**.

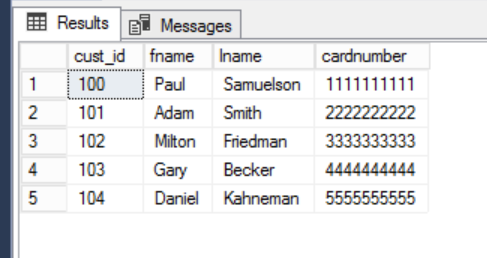
## 2. Deliverables

-- Display the original table

select \* from dbo.cust

go

/\* Task #1: Show the original table in a screen shot. \*/

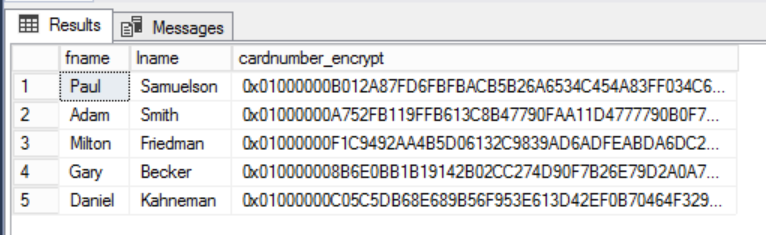


-- Display the encrypted table

select \* from dbo.cust\_encrypt

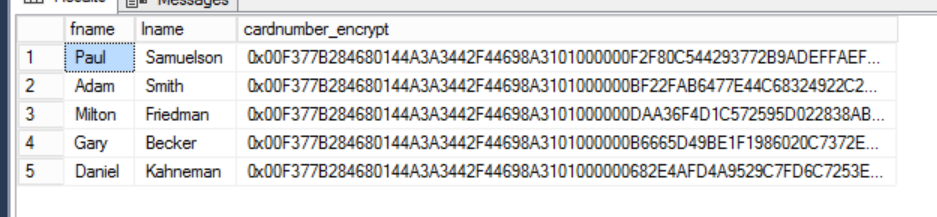
go

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



The datatype of VARBINARY is essentially a file in and of itself, and stores byte strings instead of character strings. This enables by-character encryption in SQL server to work like standard file encryption. The VARINARY data type can be converted back to a VARCHAR data type.

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



The card numbers were decrypted and then encrypted using a certificate in this instance.

-- Display the decrypted table

select fname,

lname,

cardnumber = convert(nvarchar(25), DecryptByKey(cardnumber\_encrypt))

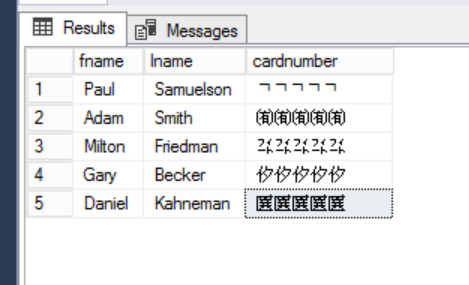
from dbo.cust\_encrypt

go

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

/\* 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 \*/



The issue here is that the VARCHAR data that was originally encrypted was not converted to VARCHAR but rather to NVARCHAR, and the characters are all Chinese characters from Unicode. If we convert the datatype to varchar instead, we get the original credit card numbers back.

