

Lab 4

1. Stored dùng để thêm mới dữ liệu (Insert) vào table SINHVIEN trong đó giá trị cột mật khẩu đã được mã hóa sử dụng MD5 từ client.

```
CREATE PROCEDURE SP_INS_ENCRYPT SINHVIEN
@masv nvarchar(20), @hoten nvarchar(100), @ngaysinh datetime, @diachi nvarchar(200), @malop varchar(20),
@tendn nvarchar(100), @matkhau varchar(max)
AS
BEGIN
INSERT INTO SINHVIEN VALUES(@masv, @hoten, @ngaysinh, @diachi, @malop, @tendn, CONVERT(VARBINARY(MAX), @matkhau))
END
```

Việc mã hóa và insert sẽ được thực hiện phía client tại project MD5Hash.

	MASV	HOTEN	NGAYSINH	DIACHI	MALOP	TENDN	MATKHAU
▶	SV01	NGUYEN VAN A	1990-01-01 00:0...	280 AN DUONG...	CNTT-K42	SVA	<Binary data>
	SV02	NGUYEN VAN B	1990-01-01 00:0...	280 AN DUONG...	CNTT-K35	SVB	<Binary data>
	SV03	AAA	2019-03-29 00:0...	AAA	CNTT-K42	SV3	<Binary data>
	SV04	NGUYEN TI	2019-04-02 00:0...	243 Nguyen Va...	CNTT-K35	TI	<Binary data>

2. Stored dùng để thêm mới dữ liệu (Insert) vào table NHANVIEN, trong đó thuộc tính MATKHAU được mã hóa (HASH) sử dụng SHA1 và thuộc tính LUONG sẽ được mã hóa sử dụng thuật toán AES 256, với khóa mã hóa là mã số của sinh viên thực hiện bài Lab này.

```
CREATE MASTER KEY ENCRYPTION BY PASSWORD = '42.01.104.098'
CREATE CERTIFICATE MyCertificate0 ENCRYPTION BY PASSWORD = '42.01.104.098' WITH SUBJECT = 'ins_nv'
CREATE SYMMETRIC KEY SSN_Key_INS_NV WITH ALGORITHM = AES_256
ENCRYPTION BY CERTIFICATE MyCertificate0

ALTER PROCEDURE SP_INS_ENCRYPT NHANVIEN
@manv nvarchar(20), @hoten nvarchar(100), @email varchar(20), @luong varchar(max), @tendn nvarchar(100), @matkhau varchar(max)
AS
BEGIN
OPEN SYMMETRIC KEY SSN_Key_INS_NV
DECRYPTION BY CERTIFICATE MyCertificate0 WITH PASSWORD = '42.01.104.098'

INSERT INTO NHANVIEN VALUES(@manv, @hoten, @email, CONVERT(VARBINARY(MAX), @luong), @tendn, CONVERT(VARBINARY(MAX), @matkhau))
CLOSE SYMMETRIC KEY SSN_Key_INS_NV
END
```

Việc mã hóa và insert sẽ được thực hiện phía client tại project MD5Hash.

Khóa dùng để mã hóa sẽ được random tại client và lưu vào file để sử dụng cho việc giải mã lần sau.

This PC > Documents > BMCSDDL_Lab4 > MD5Hash > bin > Debug

Name	Date modified	Type	Size
MD5Hash	4/16/2019 7:57 PM	Application	18 KB
MD5Hash.exe.config	3/29/2019 10:03 PM	XML Configuratio...	1 KB
MD5Hash.pdb	4/16/2019 7:57 PM	Program Debug D...	42 KB
NV05	4/16/2019 8:00 PM	Rich Text Format	1 KB

MANV	HOTEN	EMAIL	LUONG	TENDN	MATKHAU
NV01	NGUYEN VAN A	NVA@	<Binary data>	NVA	<Binary data>
NV02	NGUYEN VAN B	NVB@	<Binary data>	NVB	<Binary data>
NV03	NGUYEN VAN C	NVC@	<Binary data>	NVC	<Binary data>
NV04	NGUYEN VAN D	NVD@	<Binary data>	NVD	<Binary data>
NV05	NGUYEN TEO	TEO@	<Binary data>	TEO	<Binary data>

3. Stored dùng để truy vấn dữ liệu nhân viên (NHANVIEN) với dữ liệu lương vẫn còn mã hóa.

```
ALTER PROCEDURE SP_SEL_ENCRYPT_NHANVIEN
AS
BEGIN
    OPEN SYMMETRIC KEY SSN_Key_INS_NV
    DECRYPTION BY CERTIFICATE MyCertificate0 WITH PASSWORD = '42.01.104.098'
    SELECT MANV, HOTEN, EMAIL, convert(varchar(max), LUONG) as LUONGCB
    FROM NHANVIEN
    CLOSE SYMMETRIC KEY SSN_Key_INS_NV
END

EXEC SP_SEL_ENCRYPT_NHANVIEN
```

4. Viết màn hình quản lý đăng nhập hệ thống (sử dụng C#)

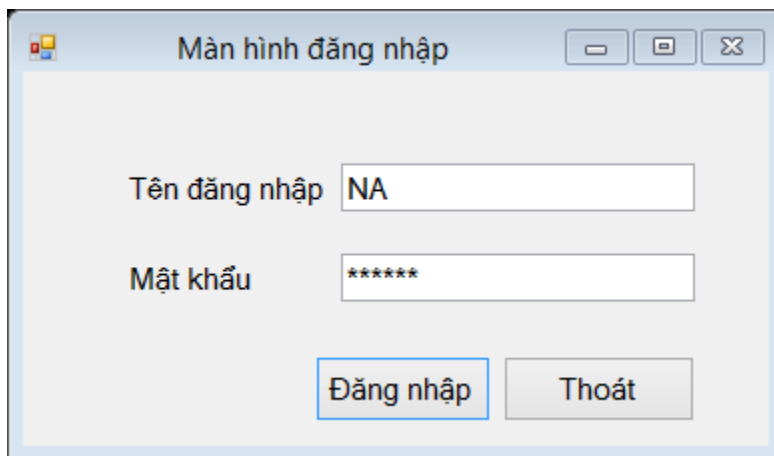
Sử dụng Project Lab4_DangNhap.

Store Procedure đăng nhập:

```
--LOGIN NHAN VIEN
CREATE PROCEDURE LoginNV(
    @UserName nvarchar(100),
    @Password varbinary(max)
)
AS
BEGIN
    SELECT COUNT(*)
    FROM NHANVIEN
    where TENDN = @UserName and MATKHAU = @Password
END
```

Đăng nhập bằng tài khoản nhân viên vừa tạo từ project MD5Hash (mã hóa mật khẩu tại client):

Tên DN: NA , mật khẩu: 123456.



The screenshot shows a standard Windows-style login dialog box. The title bar reads 'Màn hình đăng nhập'. Inside, there are two text boxes. The first is labeled 'Tên đăng nhập' and contains the text 'NA'. The second is labeled 'Mật khẩu' and contains seven asterisks '*****'. At the bottom of the dialog, there are two buttons: 'Đăng nhập' (Login) and 'Thoát' (Exit).

Thành công: hiển thị toàn bộ nhân viên với cột LUONG bị mã hóa.

Form2

DANH SÁCH NHÂN VIÊN

Thông tin nhân viên

Mã NV NV01	Họ tên NGUYEN VAN A
Email NVA@	Lương
Tên ĐN NA	Mật khẩu *****

	MANV	HOTEN	EMAIL	LUONGCB
▶	NV01	NGUYEN VAN A	NVA@	24jHoJ@ÚM%...
	NV02	NGUYEN VAN B	NVB@	24jHoJ@ÚM%...
	NV03	NGUYEN VAN C	NVC@	24jHoJ@ÚM%...
	NV04	NGUYEN VAN D	NVD@	7yZjXub9CiUxX/...
	NV05	NGUYEN TEO	TEO@	Pb6SVBnPDawf...
	NV06	NGUYEN A	A@	j6knMN9ru3Jqsa1...

Thất bại:

Thông báo

Tên đăng nhập và mật khẩu không hợp lệ!

5. Màn hình load danh sách nhân viên (sử dụng C#)

Gọi lại store SP_SEL_ENCRYPT_NHANVIEN với dữ liệu LUONG chưa giải mã.
Thực hiện giải mã phía client bằng cách chọn vào một dòng của nhân viên và mở khóa của nhân viên này để xem lương.

Form2

DANH SÁCH NHÂN VIÊN

Thông tin nhân viên

Mã NV NV06

Email A@

Tên ĐN NA

Họ tên NGUYEN A

Lương

Mật khẩu *****

	MANV	HOTEN	EMAIL	L
	NV04	NGUYEN VAN D	NVD@	7y
	NV05	NGUYEN TEO	TEO@	Pb
▶	NV06	NGUYEN A	A@	j6
	nv1	NGUYEN VAN L...	nv1@	qk
	nv2	REO	REO	WDTloneuMduU...
	nv4	BBB	BBBB	xWa20i10D7ZG9...

Thêm

Xóa

Sửa

Ghi/Lưu

Không

Thoát

Vui lòng mở khóa của nhân viên này để xem lương!

OK

Kết quả:

Form2

DANH SÁCH NHÂN VIÊN

Thông tin nhân viên

Mã NV NV06

Email A@

Tên ĐN NA

Họ tên NGUYEN A

Lương 3000000

Mật khẩu *****

	MANV	HOTEN	EMAIL	LUONGCB
	NV04	NGUYEN VAN D	NVD@	7yZjXub9CiUxX/...
	NV05	NGUYEN TEO	TEO@	Pb6SVBnPDawf...
▶	NV06	NGUYEN A	A@	3000000
	nv1	NGUYEN VAN L...	nv1@	qkEJ6ytT/uYAN...
	nv2	REO	REO	WDTloneuMduU...
	nv4	BBB	BBBB	xWa20i10D7ZG9...

Thêm

Xóa

Sửa

Ghi/Lưu

Không

Thoát

Nếu không có khóa thì không thể xem lương của nhân viên khác:

Form2

DANH SÁCH NHÂN VIÊN

Thông tin nhân viên

Mã NV: NV04 Họ tên: NGUYEN VAN D

Email: NVD@ Lương:

Tên ĐN: NA Mật khẩu: *****

	MANV	HOTEN	EMAIL	LUONGCB
	NV01	NGUYEN VAN A	NVA@	243HoJc
	NV02	NGUYEN VAN B	NVB@	243HoJc
	NV03	NGUYEN VAN C	NVC@	243HoJc
▶	NV04	NGUYEN VAN D	NVD@	7yZjXub9
	NV06	NGUYEN A	A@	j6knMNSn
	nv1	NGUYEN VAN L...	nv1@	qkEJ6ytT

Thêm Xóa Sửa Ghi/Lưu

Thông báo

Bạn không có quyền được xem lương của nhân viên này!

OK

- Thêm mới nhân viên
Nhấn nút thêm: hiển thị các textbox để điền thông tin nhân viên.

Form2

DANH SÁCH NHÂN VIÊN

Thông tin nhân viên

Mã NV: NV05 Họ tên: NGUYEN TEO

Email: TEO@ Lương: 3000000

Tên ĐN: NA Mật khẩu: *****

	MANV	HOTEN	EMAIL	LUONGCB
	NV04	NGUYEN VAN D	NVD@	7yZjXub9CiUxX/...
▶	NV05	NGUYEN TEO	TEO@	Pb6SVBnPDawf...
	NV06	NGUYEN A	A@	3000000
	nv1	NGUYEN VAN L...	nv1@	qkEJ6ytT/uYAN...
	nv2	REO	REO	WDTloneuMduU...
	nv4	BBB	BBBB	xWa20i10D7ZG9...

Thêm Xóa Sửa Ghi/Lưu Không Thoát

Điền thông tin vào các textbox sau đó chọn Ghi/Lưu. Màn hình sẽ tự động load lại nhân viên mới vừa được thêm.

Ví dụ thêm nhân viên có mã nv3:

Form2

DANH SÁCH NHÂN VIÊN

Thông tin nhân viên

Mã NV	<input type="text" value="nv3"/>	Họ tên	<input type="text" value="MY"/>
Email	<input type="text" value="MY@"/>	Lương	<input type="text" value="4000000"/>
Tên ĐN	<input type="text" value="MY"/>	Mật khẩu	<input type="password" value="*****"/>

	MANV	HOTEN	EMAIL	LUONGCB
	NV06	NGUYEN A	A@	3000000
	nv1	NGUYEN VAN L...	nv1@	qkEJ6ytT/uYAN...
	nv2	REO	REO	WDTloneuMduU...
	nv4	BBB	BBBB	xWa20i10D7ZG9...
	nv5	YYYYYY	yyy	346Ydr3a7gkuFZ...
	nv6	QQQQ	QQQ	1X+nbTaU3S8f...

Form2

DANH SÁCH NHÂN VIÊN

Thông tin nhân viên

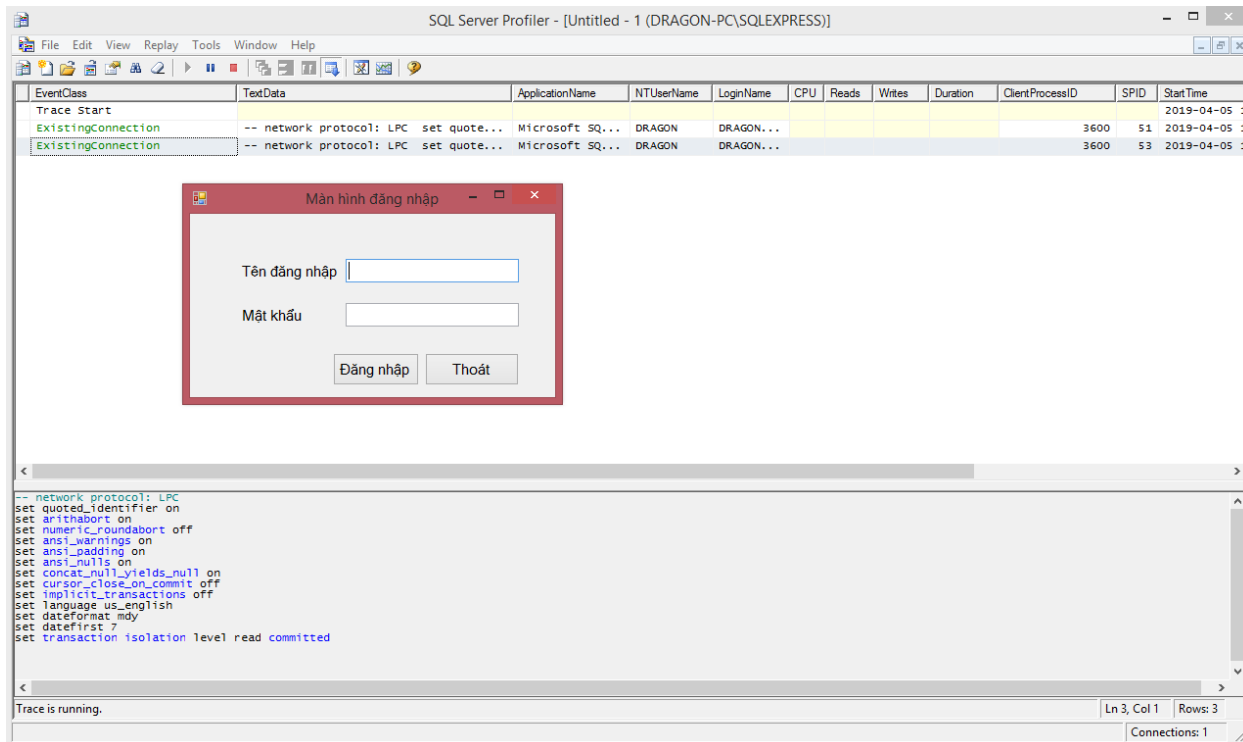
Mã NV	<input type="text" value="nv3"/>	Họ tên	<input type="text" value="MY"/>
Email	<input type="text" value="MY@"/>	Lương	<input type="text" value="4000000"/>
Tên ĐN	<input type="text" value="NA"/>	Mật khẩu	<input type="password" value="*****"/>

	MANV	HOTEN	EMAIL	LUONGCB
	NV06	NGUYEN A	A@	j6knMN9ru3Jqsa1...
	nv1	NGUYEN VAN L...	nv1@	qkEJ6ytT/uYAN...
	nv2	REO	REO	WDTloneuMduU...
▶	nv3	MY	MY@	4000000
	nv4	BBB	BBBB	xWa20i10D7ZG9...
	nv5	YYYYYY	yyy	346Ydr3a7gkuFZ...

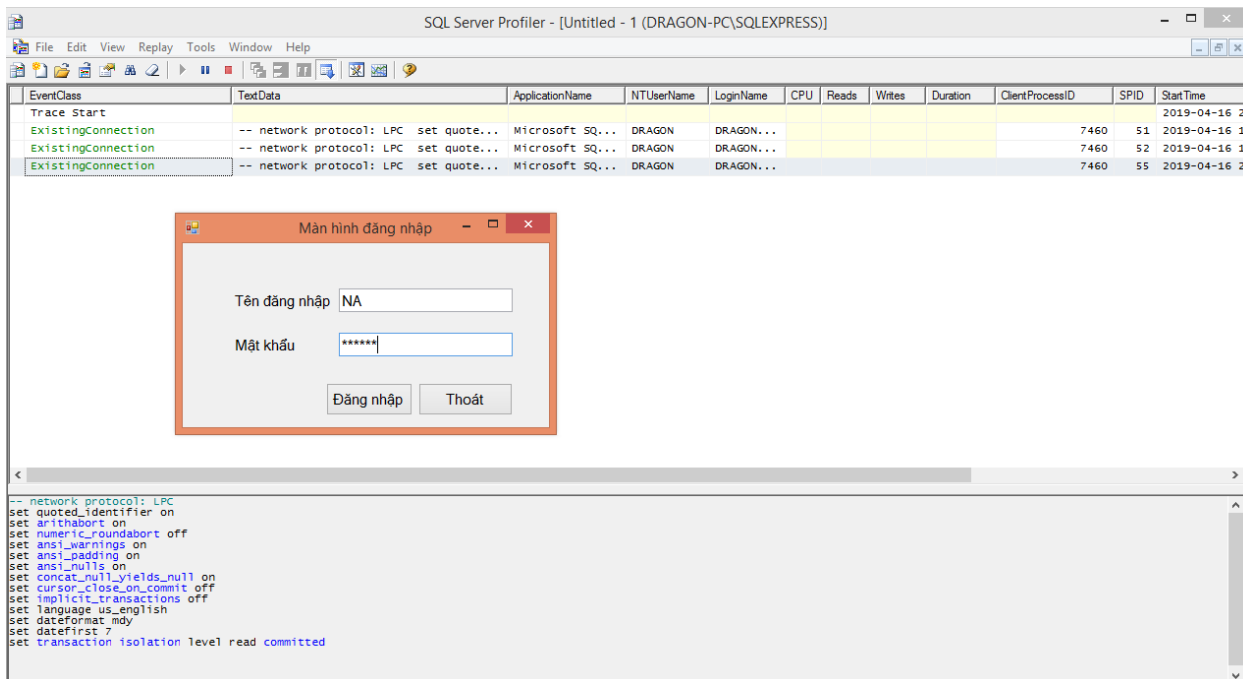
Ngoài ra có thể thực hiện chức năng Xóa, Lưu trên Form này (do đề bài không yêu cầu nên phần này sẽ không trình bày trong báo cáo).

6. Sử dụng công cụ SQL Profile để theo dõi thao tác đăng nhập

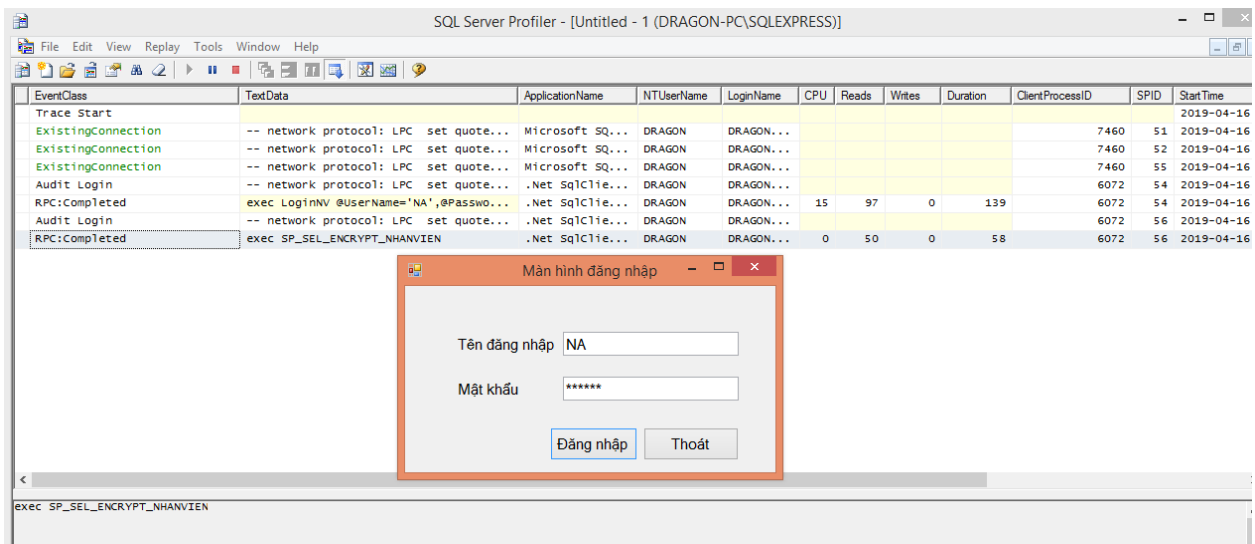
i) Mở màn hình quản lý đăng nhập



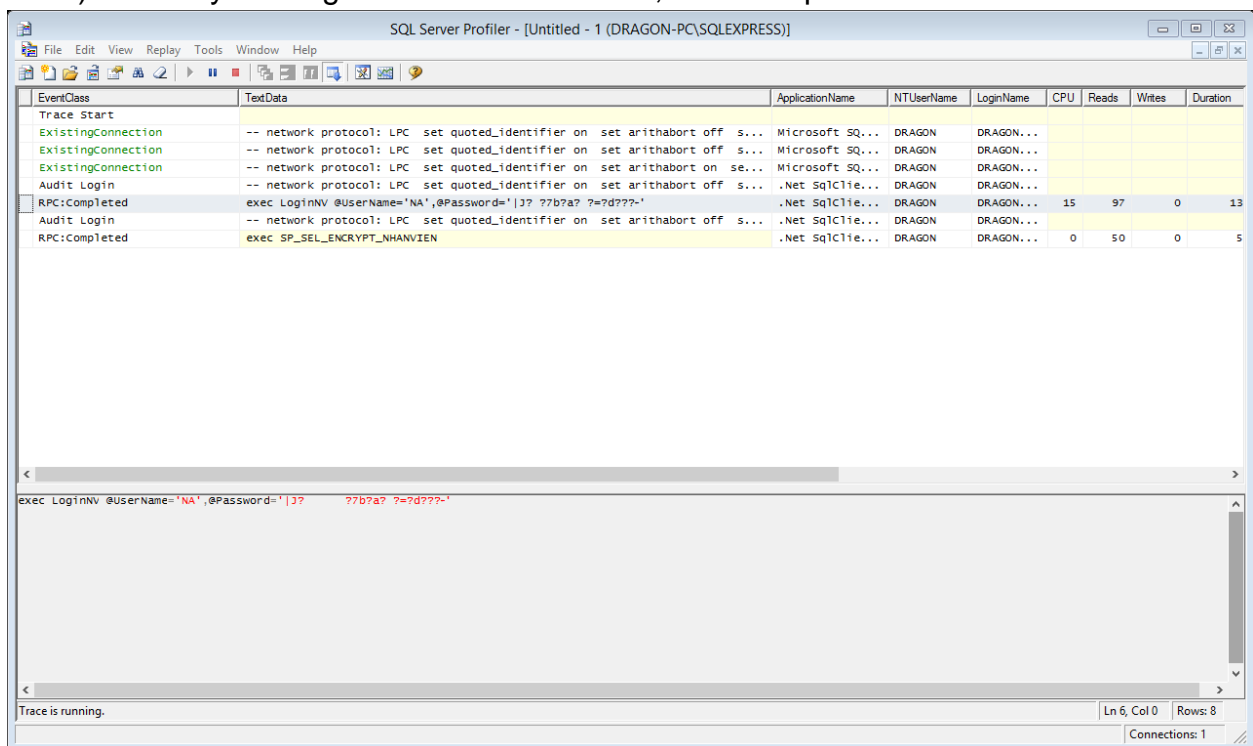
ii) Nhập tên đăng nhập và mật khẩu



iii) Nhấn nút đăng nhập



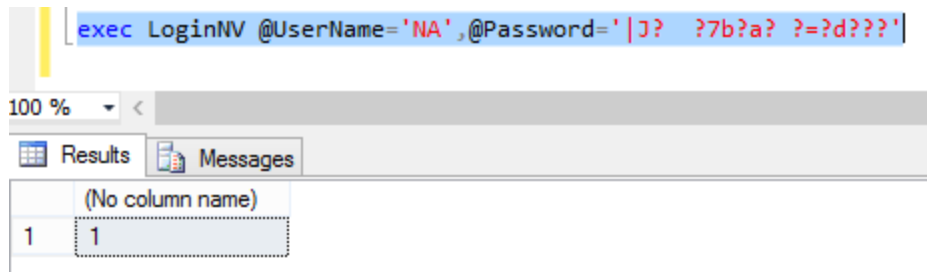
iv) Chuyển sang màn hình SQL Profile, xem kết quả



Tham số truyền vào store LoginNV là dữ liệu mật khẩu đã bị mã hóa bên client trước khi thực thi store bên server.

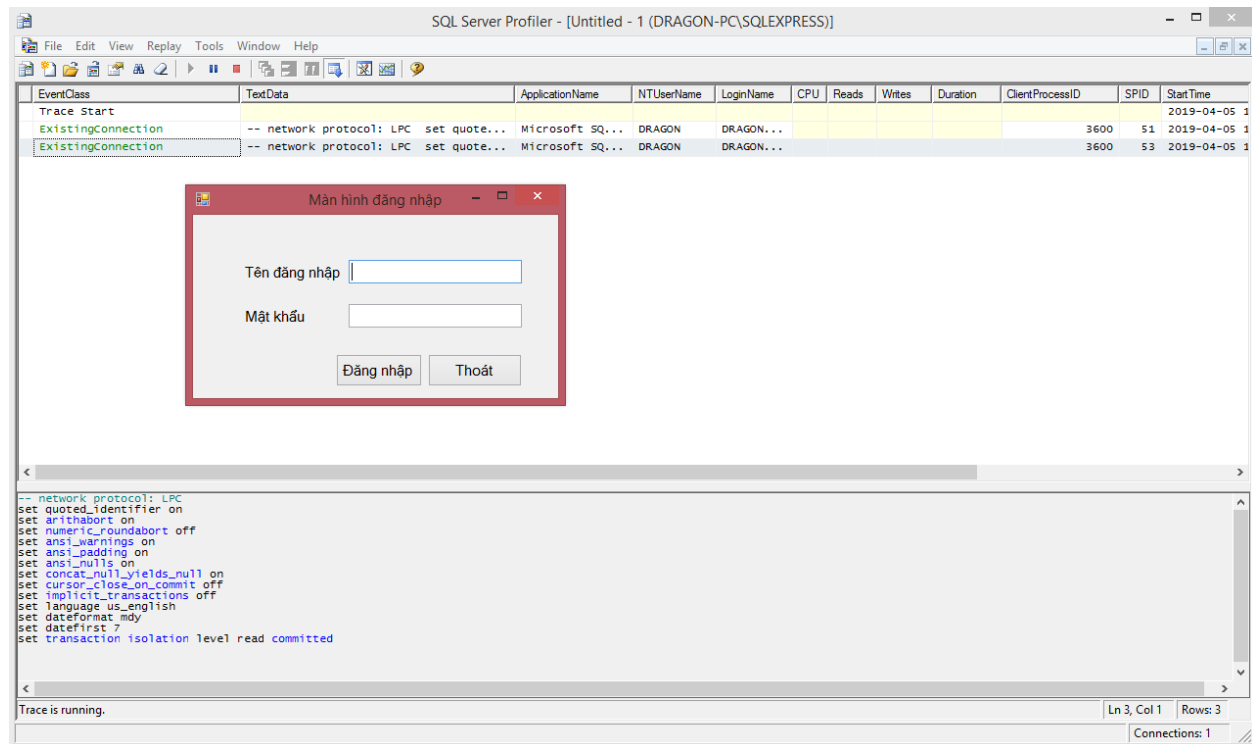
v) Thực thi câu lệnh truy vấn trong SQL Profile

Kết quả sẽ trả về đúng với yêu cầu store (nếu tên đăng nhập và mật khẩu trùng với database thì đếm số dòng chứa kết quả đó). Nếu kết quả trả về 1 thì đăng nhập thành công ngược lại trả về 0.

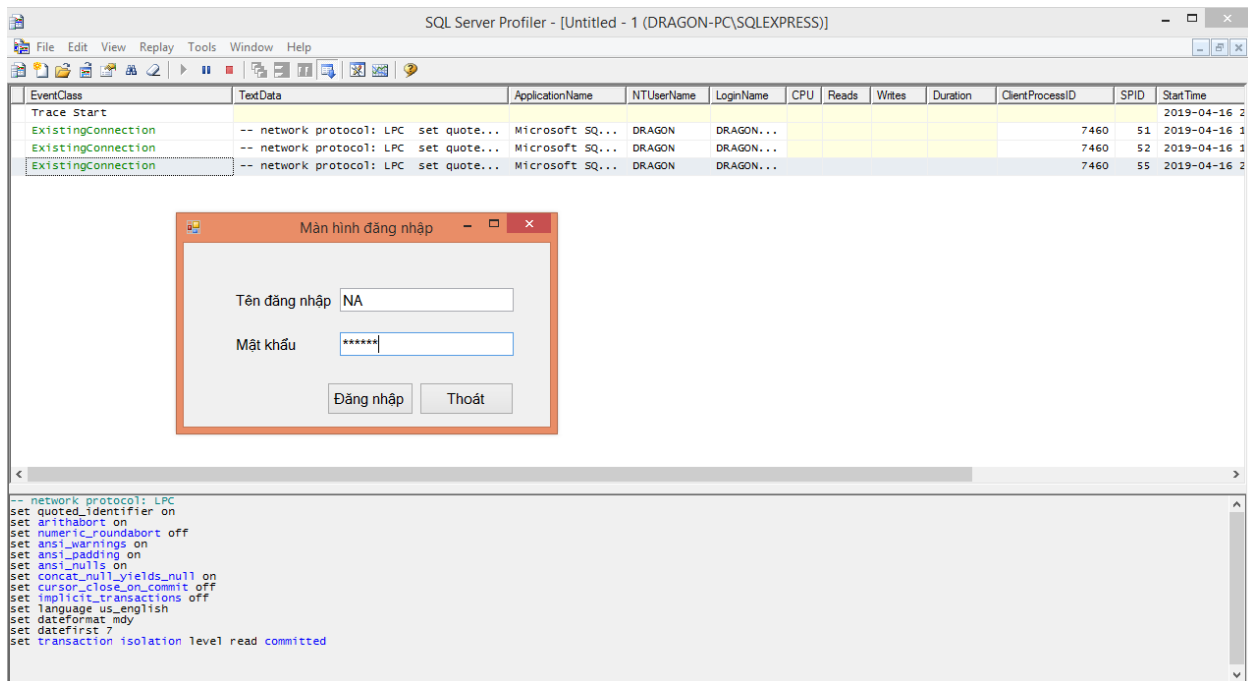


7. Sử dụng công cụ SQL Profile để theo dõi load màn hình danh sách nhân viên

i) Mở màn hình quản lý đăng nhập



ii) Nhập tên đăng nhập và mật khẩu đúng



- iii) Nhấn nút đăng nhập
- iv) Hiện thị màn hình danh sách nhân viên

Form2

DANH SÁCH NHÂN VIÊN

Thông tin nhân viên

Mã NV: NV01	Họ tên: NGUYEN VAN A
Email: NVA@	Lương:
Tên ĐN: NA	Mật khẩu: *****

MANV	HOTEN	EMAIL	LUONGCB
NV01	NGUYEN VAN A	NVA@	248HoJ@ÚM%...
NV02	NGUYEN VAN B	NVB@	248HoJ@ÚM%...
NV03	NGUYEN VAN C	NVC@	248HoJ@ÚM%...
NV04	NGUYEN VAN D	NVD@	7yZjXub9CiUx/...
NV05	NGUYEN TEO	TEO@	Pb6SVBnPDawf...
NV06	NGUYEN A	A@	j6knMN9ru3Jqsa1...

Thêm Xóa Sửa Ghi/Lưu Không Thoát

v) Chuyển sang màn hình SQL Profile, xem kết quả

EventClass	TextData	ApplicationName	NTUserName	LoginName	CPU	Reads	Writes	Duration	ClientProcessID
ExistingConnection	-- network protocol: LPC set quoted_identifier on set ...	Microsoft SQ...	DRAGON	DRAGON...					
ExistingConnection	-- network protocol: LPC set quoted_identifier on set ...	Microsoft SQ...	DRAGON	DRAGON...					
ExistingConnection	-- network protocol: LPC set quoted_identifier on set ...	Microsoft SQ...	DRAGON	DRAGON...					
ExistingConnection	-- network protocol: LPC set quoted_identifier on set ...	Microsoft SQ...	DRAGON	DRAGON...					
ExistingConnection	-- network protocol: LPC set quoted_identifier on set ...	Microsoft SQ...	DRAGON	DRAGON...					
Audit Login	-- network protocol: LPC set quoted_identifier on setNet SqlClie...	DRAGON	DRAGON...					
Audit Logout		.Net SqlClie...	DRAGON	DRAGON...	0	94	0	1763	
Audit Login	-- network protocol: LPC set quoted_identifier on setNet SqlClie...	DRAGON	DRAGON...					
RPC:Completed	exec LoginNV @UserName='NA',@Password=' j? 77b7a? 7=7d777?'	.Net SqlClie...	DRAGON	DRAGON...	0	97	0	1520	
Audit Login	-- network protocol: LPC set quoted_identifier on setNet SqlClie...	DRAGON	DRAGON...					
RPC:Completed	exec SP_SEL_ENCRYPT_NHANVIEN	.Net SqlClie...	DRAGON	DRAGON...	15	176	0	370	

vi) Copy câu lệnh truy vấn trong SQL Profile

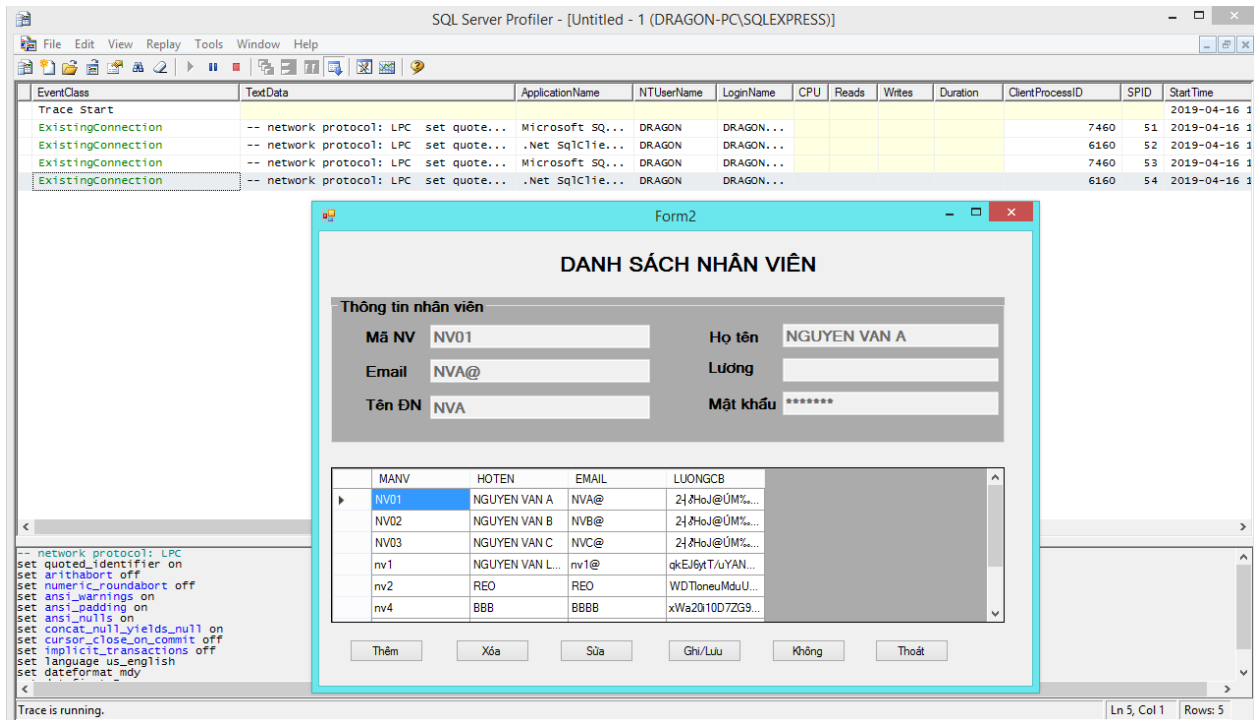
Câu lệnh đăng nhập tương tự phần 6.

Nếu đăng nhập thành công, Trace sẽ thực thi SP_SEL_ENCRYPT_NHANVIEN để hiển thị màn hình danh sách nhân viên. Lúc này LUONG vẫn bị mã hóa.

	MANV	HOTEN	EMAIL	LUONGCB
1	NV01	NGUYEN VAN A	NVA@	
2	NV02	NGUYEN VAN B	NVB@	
3	NV03	NGUYEN VAN C	NVC@	
4	nv1	NGUYEN VAN LUA	nv1@	qkEJ6ytT/uYANUgtRBYutFe37fWSqk20qQxO1UdCQcpFipbqY...
5	nv2	REO	REO	WDTloneuMduUSVhgzO57HsES0g+e2gj8vZM/XtfOALo=
6	nv4	BBB	BBBB	xWa20i10D7ZG9WoM11hwt24VcKAETqfzoERIZkK9Cul=
7	nv5	YYYYYYY	yyy	346Ydr3a7gkuFZQU3gHFwDUlpYg12ejOvRACyVce7HY=
8	nv6	QQQQ	QQQ	1X+nbTaU3S8IFPtpunyOSpmTv3+CiKwNVLnkXOo34=

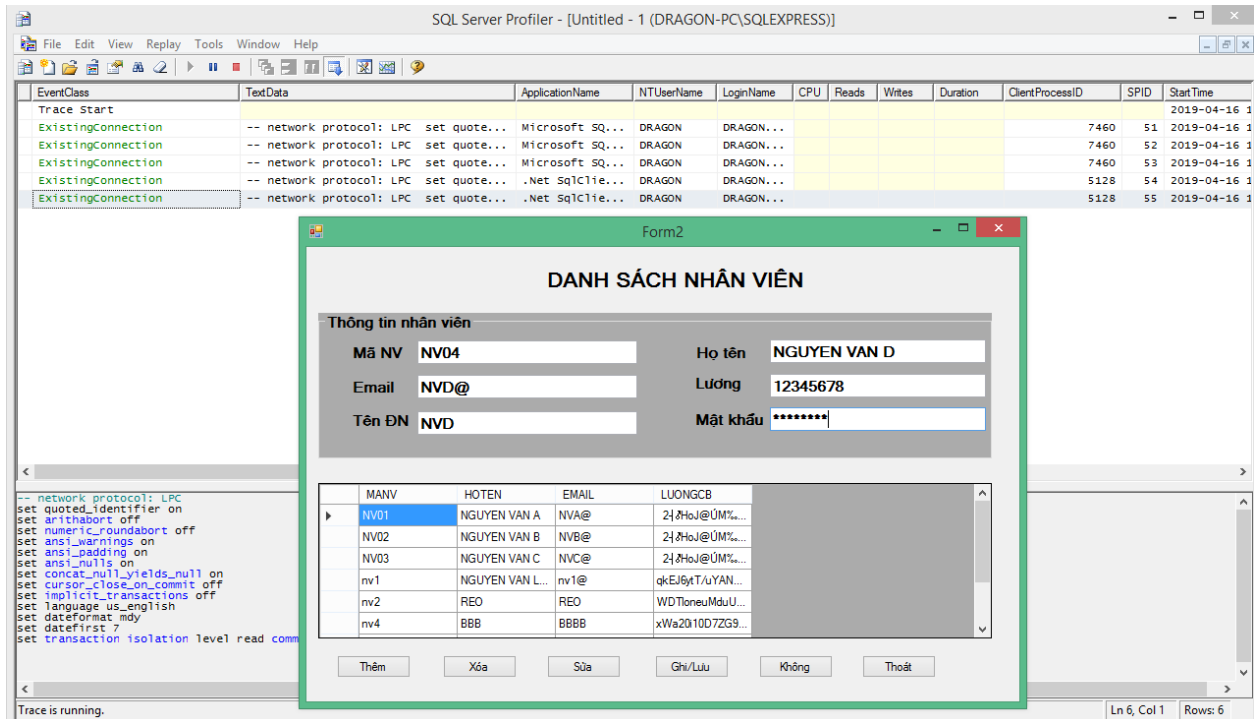
8. Sử dụng công cụ SQL Profile để theo dõi thao tác thêm mới nhân viên nhân viên.

i) Màn hình danh sách nhân viên



ii) Chọn chức năng thêm

iii) Nhập thông tin nhân viên mới



iv) Nhấn nút lưu để lưu thông tin nhân viên xuống CSDL

The screenshot shows the SQL Server Profiler interface with a trace running. The trace shows the execution of the command `exec SP_SEL_ENCRYPT_NHANVIEN`. Overlaid on this is a form titled "Form2" with the heading "DANH SÁCH NHÂN VIÊN".

Thông tin nhân viên

Mã NV	NV04	Họ tên	NGUYEN VAN D
Email	NVD@	Lương	7yZjXub9CiUxX/KTP5i7PekZ
Tên ĐN	NVA	Mật khẩu	*****

Below the form is a table listing employees:

MANV	HOTEN	EMAIL	LUONGCB
NV01	NGUYEN VAN A	NVA@	2i8Hsj@ÚM%...
NV02	NGUYEN VAN B	NVB@	2i8Hsj@ÚM%...
NV03	NGUYEN VAN C	NVC@	2i8Hsj@ÚM%...
NV04	NGUYEN VAN D	NVD@	7yZjXub9CiUxX/
nv1	NGUYEN VAN L...	nv1@	qkEJ6tT/úYAN...
nv2	REO	REO	WD1t0neuMáuU...

Buttons at the bottom of the form: Thêm, Xóa, Sửa, Ghi/Lưu, Không, Thoát.

v) Chuyển sang màn hình SQL Profile, xem kết quả

The screenshot shows the SQL Server Profiler interface with the trace stopped. The command `exec SP_SEL_ENCRYPT_NHANVIEN` is selected in the trace. The SQL Profile for this command is displayed below the trace.

SQL Profile for: exec SP_SEL_ENCRYPT_NHANVIEN

EventClass	TextData	ApplicationName	NTUserName	LoginName
Trace Start				
ExistingConnection	-- network protocol: LPC set quoted_identifier on set arithabort off set numeric_roundabort off s...	Microsoft SQ...	DRAGON	DRAGON...
ExistingConnection	-- network protocol: LPC set quoted_identifier on set arithabort off set numeric_roundabort off s...	Microsoft SQ...	DRAGON	DRAGON...
ExistingConnection	-- network protocol: LPC set quoted_identifier on set arithabort on set numeric_roundabort off se...	Microsoft SQ...	DRAGON	DRAGON...
ExistingConnection	-- network protocol: LPC set quoted_identifier on set arithabort off set numeric_roundabort off s...	.Net SqlClie...	DRAGON	DRAGON...
ExistingConnection	-- network protocol: LPC set quoted_identifier on set arithabort off set numeric_roundabort off s...	.Net SqlClie...	DRAGON	DRAGON...
Audit Logout		.Net SqlClie...	DRAGON	DRAGON...
Audit Logout		.Net SqlClie...	DRAGON	DRAGON...
RPC:Completed	exec sp_reset_connection	.Net SqlClie...	DRAGON	DRAGON...
Audit Login	-- network protocol: LPC set quoted_identifier on set arithabort off set numeric_roundabort off s...	.Net SqlClie...	DRAGON	DRAGON...
RPC:Completed	exec SP_INS_ENCRYPT_NHANVIEN @manv='NV04',@hoten='NGUYEN VAN D',@email='NVD@',@tendn='NVD',@matkhau='...	.Net SqlClie...	DRAGON	DRAGON...
Audit Login	-- network protocol: LPC set quoted_identifier on set arithabort off set numeric_roundabort off s...	.Net SqlClie...	DRAGON	DRAGON...
RPC:Completed	exec SP_SEL_ENCRYPT_NHANVIEN	.Net SqlClie...	DRAGON	DRAGON...

Trace is running. Status: Ln 13, Col 1 Rows: 13 Connections: 1

vi) Copy câu lệnh SP_INS_ENCRYPT_NHANVIEN trong SQL Profile

RPC:Completed	exec SP_INS_ENCRYPT_NHANVIEN @manv='NV04',@hoten='NGUYEN VAN D',@email='NVD@',@tendn='NVD',@matkhou='...' .Net SqlC1ie... DRAGON DRAGON..
Audit Login	-- network protocol: LPC set quoted_identifier on set arithabort off set numeric_roundabort off s... .Net SqlC1ie... DRAGON DRAGON..
RPC:Completed	exec SP_SEL_ENCRYPT_NHANVIEN .Net SqlC1ie... DRAGON DRAGON..
Audit Login	-- network protocol: LPC set quoted_identifier on set arithabort off set numeric_roundabort off s... Microsoft SQ... DRAGON DRAGON..
RPC:Completed	exec sp_executesql N'SELECT dtb.collation_name AS [Collation], dtb.name AS [DatabaseName2] FROM maste... Microsoft SQ... DRAGON DRAGON..
Audit Logout	Microsoft SQ... DRAGON DRAGON..
Audit Login	-- network protocol: LPC set quoted_identifier on set arithabort off set numeric_roundabort off s... Microsoft SQ... DRAGON DRAGON..
SQL:BatchStarting	SELECT dtb.name AS [Name], dtb.database_id AS [ID] FROM master.sys.databases AS dtb ORDER BY [Name] ASC Microsoft SQ... DRAGON DRAGON..
SQL:BatchCompleted	SELECT dtb.name AS [Name], dtb.database_id AS [ID] FROM master.sys.databases AS dtb ORDER BY [Name] ASC Microsoft SQ... DRAGON DRAGON..
Audit Logout	Microsoft SQ... DRAGON DRAGON..
Audit Login	-- network protocol: LPC set quoted_identifier on set arithabort off set numeric_roundabort off s... Microsoft SQ... DRAGON DRAGON..

< exec SP_INS_ENCRYPT_NHANVIEN @manv='NV04',@hoten='NGUYEN VAN D',@email='NVD@',@tendn='NVD',@matkhou='???t?YG?&???h?k??',@luong='7y2Jxub9C1uXX/KTP517PekZzqbYRVHfIy3g90tzoeY='

vii) Xem và viết nhận xét.

Câu lệnh này được gán với các biến tương ứng trong đó trước khi Insert vào bảng NHANVIEN thì giá trị cột MATKHAU và cột LUONG đã được mã hóa theo yêu cầu đề bài (mã hóa phía client) trước khi lưu vào CSDL phía server.