

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN TP.HCM
KHOA CÔNG NGHỆ THÔNG TIN

~0~



BÁO CÁO LAB NHÓM SỐ 3: MÃ HÓA DỮ LIỆU
SỬ DỤNG CÁC THUẬT TOÁN MÃ HÓA CÔNG KHAI

Nhóm thực hiện: 12

TP Hồ Chí Minh, ngày 16 tháng 4 năm 2023

Mục Lục

Mục Lục.....	2
I. PHÂN CÔNG NHÓM.....	3
1. Thành viên.....	3
2. Bảng phân công.....	3
II. BÀI LÀM.....	4
1. Stored dùng để thêm mới dữ liệu (Insert) vào table NHANVIEN.....	4
2. Stored dùng để truy vấn dữ liệu NHANVIEN.....	5
3. Xây dựng các màn hình quản lý sinh viên.....	5
a. Màn hình đăng nhập.....	5
b. Màn hình quản lý lớp.....	6
c. Màn hình quản lý sinh viên.....	8
d. Màn hình nhập điểm.....	10
4. Theo dõi thao tác nhập điểm trong SQL Profile.....	13

I. PHÂN CÔNG NHÓM

1. Thành viên

Tên	MSSV	Email
Nguyễn Quang Huy	20120297	20120297@student.hcmus.edu.vn
Nguyễn Thành Long	20120324	20120324@student.hcmus.edu.vn
Cái Hữu Nghĩa	20120335	20120335@student.hcmus.edu.vn
Phan Tấn Kiệt	20120313	20120313@student.hcmus.edu.vn

2. Bảng phân công

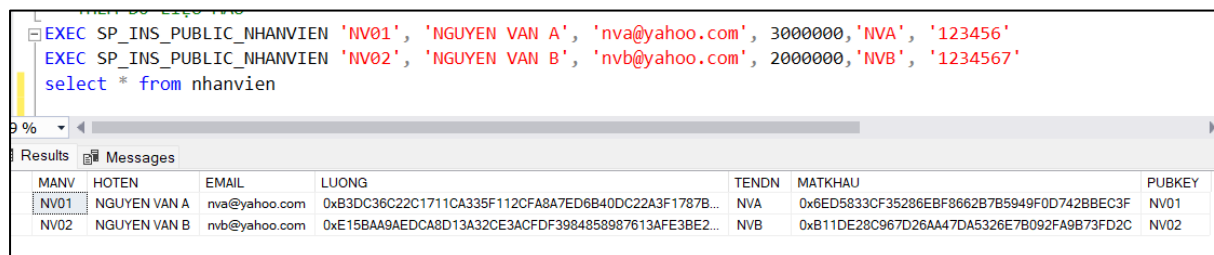
Tên	Câu	Tỷ lệ hoàn thành
Phan Tấn Kiệt	Câu i, ii: Tạo procedures. Màn hình đăng nhập	100%
Nguyễn Quang Huy	Màn hình thêm điểm	100%
Cái Hữu Nghĩa	Màn hình quản lý lớp Theo dõi thêm điểm bằng SQL Profile	100%
Nguyễn Thành Long	Màn hình quản lý sinh viên	100%

II. BÀI LÀM

1. Stored dùng để thêm mới dữ liệu (Insert) vào table NHANVIEN

```
IF OBJECT_ID('SP_INS_PUBLIC_NHANVIEN','P') IS NOT NULL
DROP PROCEDURE SP_INS_PUBLIC_NHANVIEN
GO
CREATE PROCEDURE SP_INS_PUBLIC_NHANVIEN
    @MANV VARCHAR(20),
    @HOTEN NVARCHAR(100),
    @EMAIL VARCHAR(20),
    @LUONG INT,
    @TENDN NVARCHAR(100),
    @MATKHAU NVARCHAR(100)
AS
BEGIN
    -- TẠO KHOÁ ASYMMETRIC ĐỂ MÃ HOÁ MẬT KHẨU
    IF NOT EXISTS(SELECT * FROM sys.asymmetric_keys WHERE name = @MANV)
    BEGIN
        DECLARE @Sql NVARCHAR(MAX)
        SET @Sql = N'CREATE ASYMMETRIC KEY ' + QUOTENAME(@MANV) + N'
        WITH ALGORITHM = RSA_2048
        ENCRYPTION BY PASSWORD = ''' + @MATKHAU + N''';'
        EXEC sp_executesql @Sql;
    END
    DECLARE @LUONG_VARBINARY VARBINARY(MAX) = CONVERT(VARBINARY(MAX), @LUONG)
    INSERT INTO NHANVIEN (MANV, HOTEN, EMAIL, LUONG, TENDN, MATKHAU, PUBKEY)
    VALUES (@MANV, @HOTEN, @EMAIL, ENCRYPTBYASYMKEY(ASYMKEY_ID(@MANV),
    @LUONG_VARBINARY), @TENDN, HASHBYTES('SHA1', @MATKHAU), @MANV);
END
```

Kết quả chạy:



The screenshot shows the execution of the stored procedure in SQL Server Enterprise Manager. The command window displays the execution of the procedure for two records: NV01 and NV02. Below the command window, the 'Results' pane shows the data inserted into the NHANVIEN table. The table has columns: MANV, HOTEN, EMAIL, LUONG, TENDN, MATKHAU, and PUBKEY. The data is as follows:

MANV	HOTEN	EMAIL	LUONG	TENDN	MATKHAU	PUBKEY
NV01	NGUYEN VAN A	nva@yahoo.com	3000000	NVA	0x6ED5833CF35286EBF8662B7B5949F0D742BBEC3F	NV01
NV02	NGUYEN VAN B	nvb@yahoo.com	2000000	NVB	0xB11DE28C967D26AA47DA5326E7B092FA9B73FD2C	NV02

2. Stored dùng để truy vấn dữ liệu NHANVIEN

```
IF OBJECT_ID('SP_SEL_PUBLIC_NHANVIEN','P') IS NOT NULL
DROP PROCEDURE SP_SEL_PUBLIC_NHANVIEN
GO
CREATE PROCEDURE SP_SEL_PUBLIC_NHANVIEN
    @MANV NVARCHAR(100),
    @MATKHAU NVARCHAR(100)
AS
BEGIN
    SELECT NV.MANV, NV.HOTEN, NV.EMAIL, CONVERT(INT,
    DECRYPTBYASYMKEY(ASYMKEY_ID(NV.MANV), NV.LUONG, @MATKHAU)) as LUONGCB
    FROM NHANVIEN AS NV
    where nv.TENDN = @MANV and NV.MATKHAU = HASHBYTES('SHA1', @MATKHAU)
END
```

Kết quả chạy:



The screenshot shows the SQL Server Enterprise Manager interface. The command window at the top displays two successful executions of the stored procedure: `exec SP_SEL_PUBLIC_NHANVIEN 'NVA', '123456'` and `exec SP_SEL_PUBLIC_NHANVIEN 'NVB', '1234567'`. Below the command window, the Results pane shows two rows of data. The first row corresponds to the first execution (MANV: NV01, HOTEN: NGUYEN VAN A, EMAIL: nva@yahoo.com, LUONGCB: 3000000). The second row corresponds to the second execution (MANV: NV02, HOTEN: NGUYEN VAN B, EMAIL: nvb@yahoo.com, LUONGCB: 2000000).

	MANV	HOTEN	EMAIL	LUONGCB
1	NV01	NGUYEN VAN A	nva@yahoo.com	3000000
1	NV02	NGUYEN VAN B	nvb@yahoo.com	2000000

3. Xây dựng các màn hình quản lý sinh viên

a. Màn hình đăng nhập

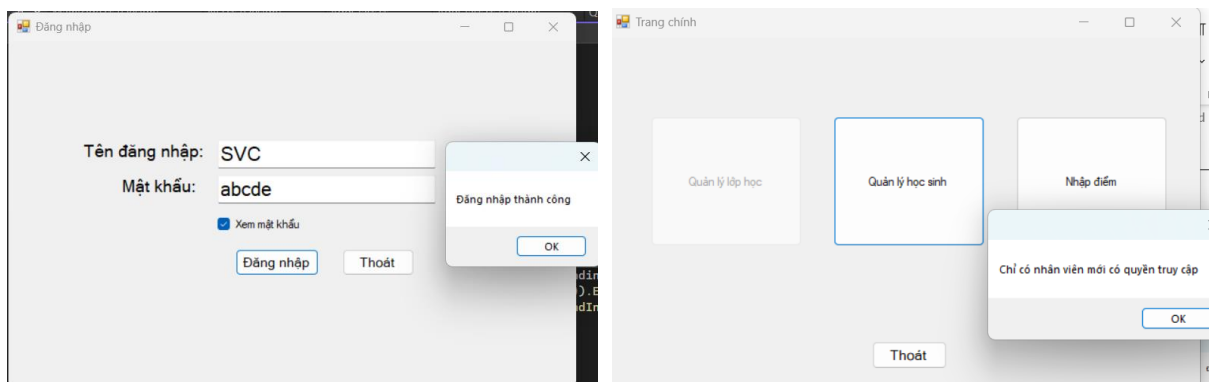
Màn hình đăng nhập có tính năng phân biệt giữa tài khoản của sinh viên và tài khoản của nhân viên. Với tài khoản của sinh viên sẽ bị chặn các tính năng, với nhân viên thì ngược lại.

```

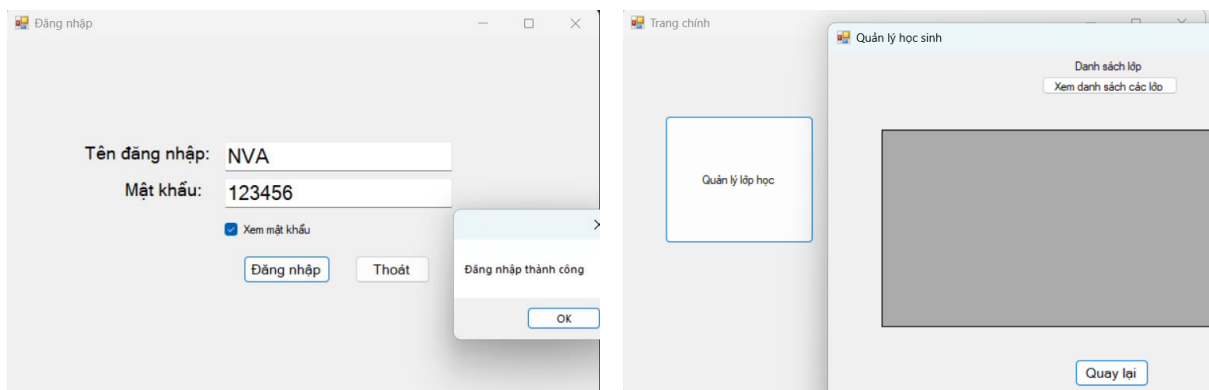
IF OBJECT_ID('LOG_IN', 'P') IS NOT NULL
DROP PROCEDURE LOG_IN
GO
CREATE PROCEDURE LOG_IN
    @MANV NVARCHAR(100),
    @MATKHAU NVARCHAR(100)
AS
BEGIN
    SELECT NV.MANV, NV.TENDN, SUBSTRING(NV.MANV, 1, 2) AS CHUCNANG
    FROM NHANVIEN AS NV
    where nv.TENDN = @MANV and NV.MATKHAU = HASHBYTES('SHA1', @MATKHAU)
    UNION
    SELECT sv.MASV, SV.TENDN, SUBSTRING(sv.MASV, 0, 2) AS CHUCNANG
    FROM SINHVIEN AS sv
    where sv.TENDN = @MANV and sv.MATKHAU = HASHBYTES('SHA1', @MATKHAU)
END
GO

```

Màn hình đăng nhập với 2 loại tài khoản:



Đăng nhập với tài khoản sinh viên

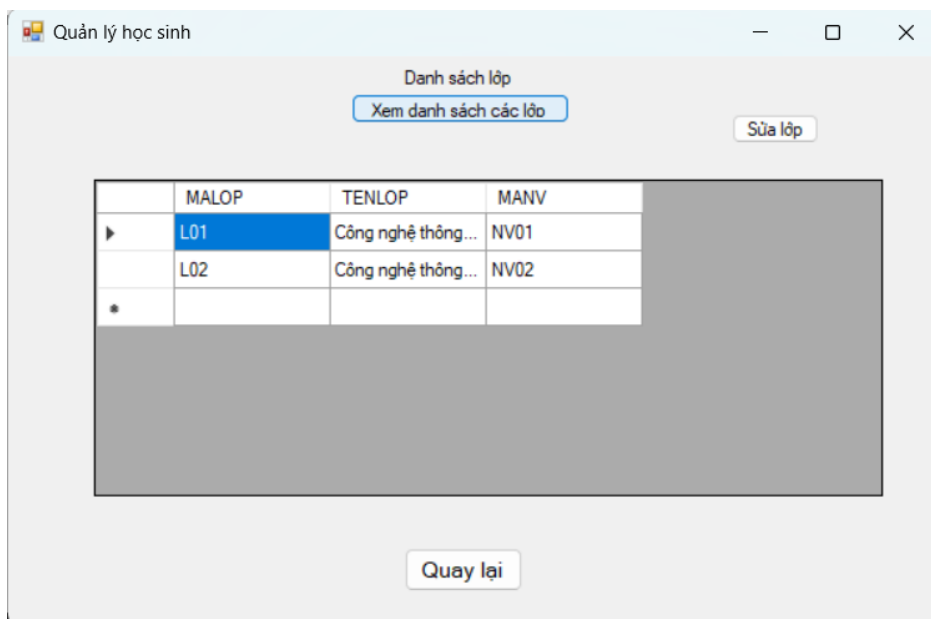


Đăng nhập với tài khoản nhân viên

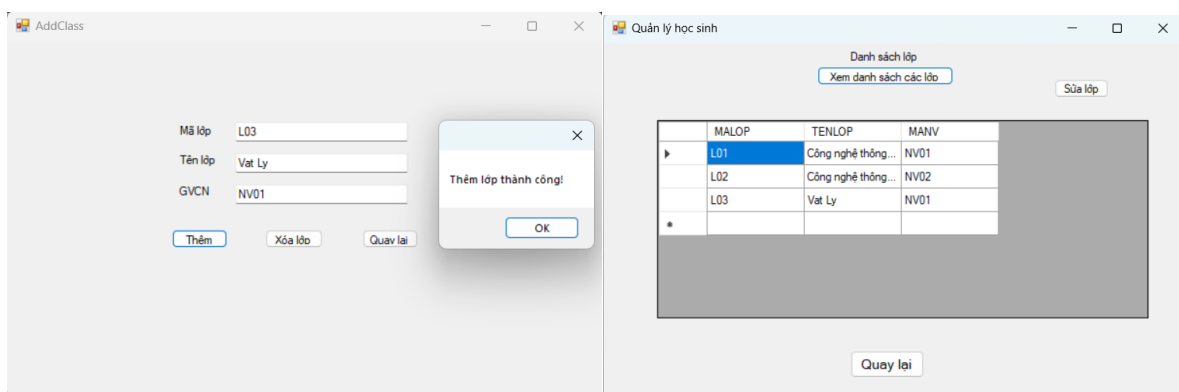
b. Màn hình quản lý lớp

Xem các lớp trong cơ sở dữ liệu (nút “Xem danh sách các lớp”):

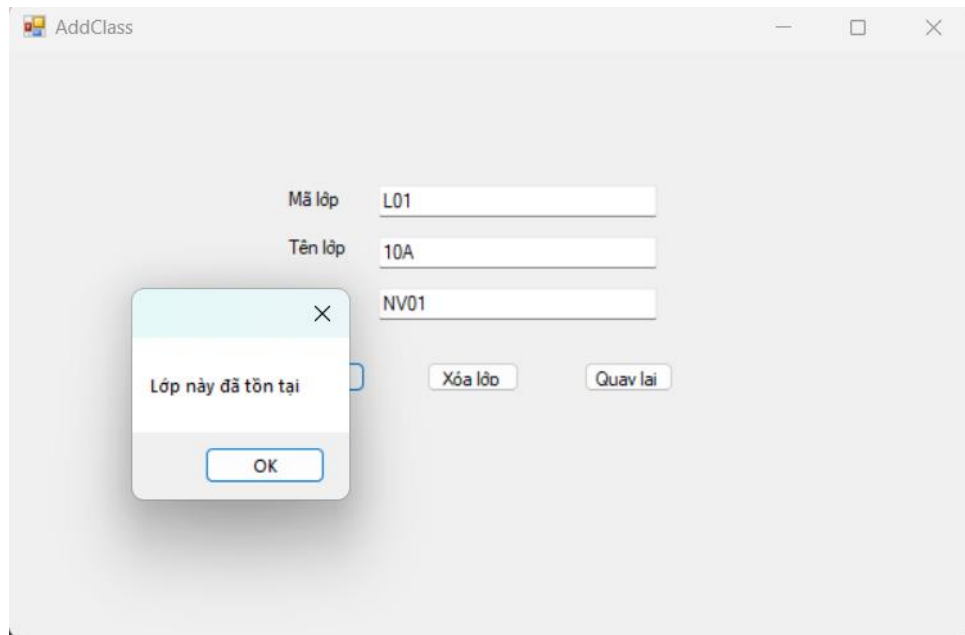
```
private void button2_Click(object sender, EventArgs e)
{
    con.Open();
    string query = "select * from LOP";
    SqlDataAdapter da = new SqlDataAdapter(query, con);
    DataTable table = new DataTable();
    da.Fill(table);
    dataGridView2.DataSource = table;
    con.Close();
}
```



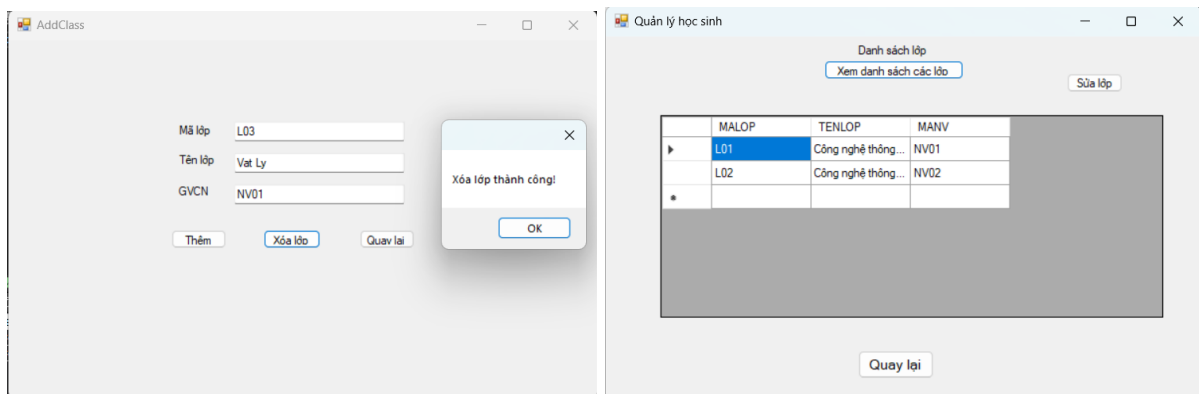
Thêm lớp học (nút “Sửa lớp”):



Khi thêm lớp có sẵn thì sẽ báo tồn tại lớp:



Xoá lớp học:



c. Màn hình quản lý sinh viên

Xem danh sách sinh viên (Nút “Xem danh sách sinh viên”):

```
string query = "select SV.MASV,SV.HOTEN,SV.NGAYSINH,SV.DIACHI,SV.MALOP from SINHVIEN as SV";
SqlDataAdapter da = new SqlDataAdapter(query, con);
DataTable table = new DataTable();
da.Fill(table);
dataGridView2.DataSource = table;
```


Thay đổi thông tin

MSSV

Họ Tên

Ngày Sinh

Địa chỉ

Mã lớp

OK

Quay lại

Xem danh sách sinh viên

MASV	HOTEN
SV01	Trần Văn C
SV02	Trần Văn D
*	

Cập nhật thông tin sinh viên (Màn hình bên trái):

```

IF OBJECT_ID('CAP_NHAT_SINH_VIEN', 'P') IS NOT NULL
DROP PROCEDURE CAP_NHAT_SINH_VIEN
GO
CREATE PROCEDURE CAP_NHAT_SINH_VIEN
    @MASV VARCHAR(20),
    @HOTEN NVARCHAR(100),
    @NGAYSINH DATETIME,
    @DIACHI NVARCHAR(200),
    @MALOP VARCHAR(20)
AS
BEGIN
    UPDATE SINHVIEN
    SET MASV=@MASV, HOTEN=@HOTEN, NGAYSINH=@NGAYSINH, DIACHI=@DIACHI, MALOP=@MALOP
    WHERE MASV = @MASV;
END

```

Thay đổi thông tin

MSSV

Họ Tên

Ngày Sinh

Địa chỉ

Mã lớp

OK

Quay lại

Xem danh sách sinh viên

Thay đổi thông tin thành công!

OK

MASV	HOTEN
SV01	C
SV02	Trần Văn D
*	

Ràng buộc chỉ nhân viên quản lý lớp sinh viên mới được thay đổi thông tin

```

IF OBJECT_ID('NHAN_VIEN_QL_SINH_VIEN', 'P') IS NOT NULL
DROP PROCEDURE NHAN_VIEN_QL_SINH_VIEN
GO
CREATE PROCEDURE NHAN_VIEN_QL_SINH_VIEN
    @MANV VARCHAR(20),
    @MASV VARCHAR(20)
AS
BEGIN
    SELECT *
    FROM SINHVIEN as sv
    INNER JOIN lop ON sv.MALOP = lop.MALOP
    INNER JOIN NHANVIEN as nv ON lop.MANV = nv.MANV
    where sv.MASV = @MASV and nv.MANV = @MANV
END

```

Vì SV01 đã được đổi sang lớp L02 nên nhân viên này không thể thay đổi thông tin của sinh viên.

	DIACHI	MALOP
▶	280 AN DUONG ...	L02
	280 TO VINH DI...	L01
*		

d. Màn hình nhập điểm

Stored procedure Nhap_Diem: giúp nhập điểm vào bảng BANGDIEM

Điểm thi được mã hóa bằng RSA 512 và khóa là MANV của người nhập

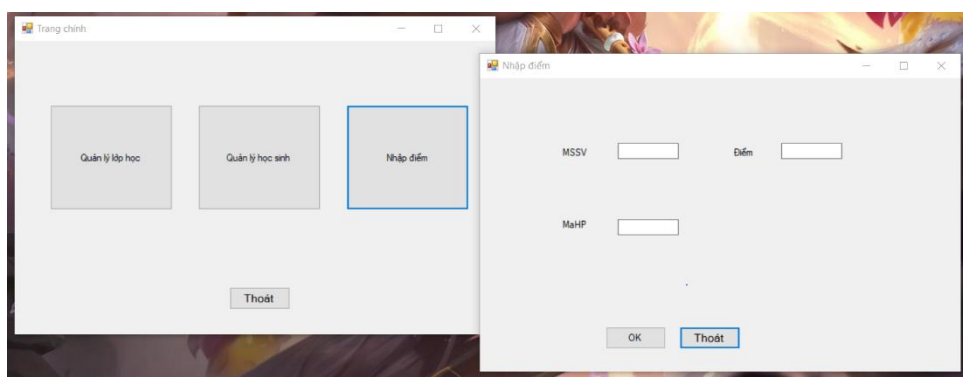
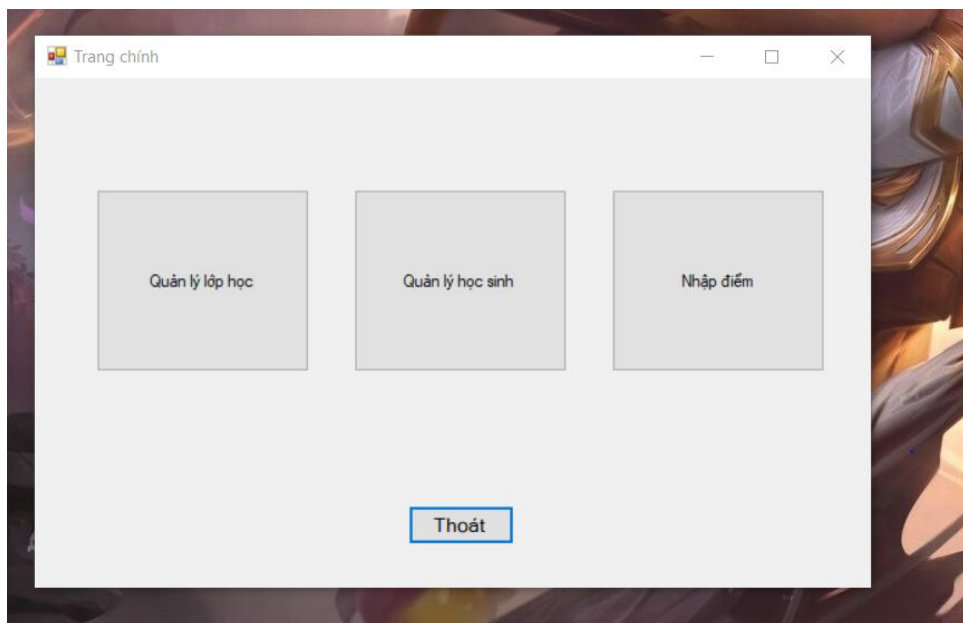
```

--Nhap diem
IF OBJECT_ID('Nhap_Diem','P') IS NOT NULL
DROP PROCEDURE Nhap_Diem
GO
CREATE PROCEDURE Nhap_Diem
    @MASV VARCHAR(20),
    @MAHP VARCHAR(20),
    @DIEMTHI VARCHAR(20),
    @MANV VARCHAR(20)
AS
BEGIN
    INSERT INTO BANGDIEM(MASV, MAHP, DIEMTHI)
    VALUES (@MASV, @MAHP, ENCRYPTBYASYMKEY(ASYMKEY_ID(@MANV), @DIEMTHI))
END
GO

--Exec Nhap_Diem 'SV02', 'HP01', '2', 'NV01'

```

Cấu hình

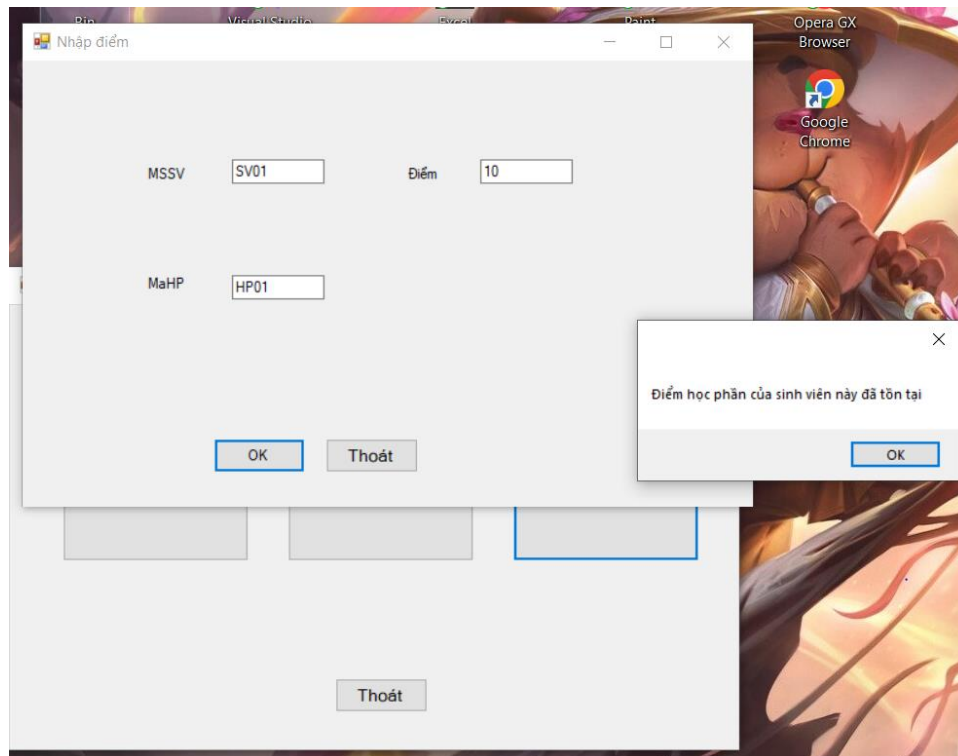


Kết quả: thông tin điểm của sinh viên đã được nhập, điểm thi đã được mã hóa

LAPTOP-U92LVGTP...m - dbo.BANGDIEM

	MASV	MAHP	DIEMTHI
▶	SV01	HP01	<Binary dat...
*	NULL	NULL	NULL

Nếu điểm học phần của sinh viên đó đã được nhập sẽ hiện thông báo điểm đã tồn tại



4. Theo dõi thao tác nhập điểm trong SQL Profile

Khi nhập điểm cho SV01 ứng với học phần 01, kết quả thành công:

EventClass	TextData	ApplicationName	NTUserName	LoginName	CPU	Reads	Writes	Duration	ClientProcessID	SPID	StartTime
SQL:BatchCompleted	SELECT target_data FROM sy...	SQLServerCEIP	SQLTELE...	NT SER...	16	651	0	93	11256	54	2023-0...
Audit Logout		SQLServerCEIP	SQLTELE...	NT SER...	16	2167	0	174	11256	54	2023-0...
RPC:Completed	exec sp_reset_connection	SQLServerCEIP	SQLTELE...	NT SER...	0	0	0	0	11256	54	2023-0...
Audit Login	-- network protocol: LPC set quoted...	SQLServerCEIP	SQLTELE...	NT SER...					11256	54	2023-0...
SQL:BatchStarting	SET DEADLOCK_PRIORITY -10	SQLServerCEIP	SQLTELE...	NT SER...					11256	54	2023-0...
SQL:BatchCompleted	SET DEADLOCK_PRIORITY -10	SQLServerCEIP	SQLTELE...	NT SER...	0	0	0	0	11256	54	2023-0...
SQL:BatchStarting	if not exists (select * from sys.dm...	SQLServerCEIP	SQLTELE...	NT SER...					11256	54	2023-0...
SQL:BatchCompleted	if not exists (select * from sys.dm...	SQLServerCEIP	SQLTELE...	NT SER...	0	20	0	1	11256	54	2023-0...
Audit Logout		.Net SqlClie...	Admin	DESKTO...	0	587	0	15793	13548	53	2023-0...
RPC:Completed	exec sp_reset_connection	.Net SqlClie...	Admin	DESKTO...	0	0	0	0	13548	53	2023-0...
Audit Login	-- network protocol: LPC set quoted...	.Net SqlClie...	Admin	DESKTO...					13548	53	2023-0...
RPC:Completed	exec sp_executesql N'exec Nhap_DiemNet SqlClie...	Admin	DESKTO...	0	170	1	6	13548	53	2023-0...


```

exec sp_executesql N'exec Nhap_Diem @MSSV,@MAHP,@DIENHI,@MANV' N'@MSSV nvarchar(4),@MAHP nvarchar(4),@DIENHI nvarchar(1),@MANV
nvarchar(4)',@MSSV=N'SV01',@MAHP=N'HP01',@DIENHI=N'5',@MANV=N'NV01'

```

Trace is running. Ln 29, Col 1 Rows: 29

Nhận xét:

- Đầu tiên, khi ta đăng nhập, sẽ có dữ liệu của client được đưa đến server báo có người dùng với username và password đăng nhập vào hệ thống.
- Sau khi ta nhập điểm, dữ liệu cũng được đưa đến server từ client dưới dạng bản rõ.
- Sau đó, dữ liệu sẽ được server lưu về, mã hóa rồi lưu vào database.
- Chỉ có những người nhân viên có chức năng quản lý sinh viên mới nhìn thấy được bản rõ của điểm sinh viên.