

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

~0~



BÁO CÁO LAB NHÓM SỐ 4:
MÃ HÓA DỮ LIỆU PHÍA CLIENT

Nhóm thực hiện: 12

TP Hồ Chí Minh, ngày 30 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.....	4
3. Xây dựng các màn hình quản lý sinh viên.....	5
a. Màn hình đăng nhập.....	5
b. Màn hình quản lý nhân viên.....	6
c. Màn hình quản lý lớp.....	12
d. Màn hình quản lý sinh viên.....	13
e. Màn hình nhập điểm.....	15
4. Theo dõi thao tác nhập điểm trong SQL Profile.....	17

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	Màn hình đăng nhập, màn hình quản lý nhân viên, lớp RSA	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_ENCRYPT_NHANVIEN','P') IS NOT NULL
DROP PROCEDURE SP_INS_PUBLIC_ENCRYPT_NHANVIEN
GO
CREATE PROCEDURE SP_INS_PUBLIC_ENCRYPT_NHANVIEN
    @MANV VARCHAR(20),
    @HOTEN NVARCHAR(100),
    @EMAIL VARCHAR(20),
    @LUONG varbinary(max),
    @TENDN NVARCHAR(100),
    @MATKHAU varbinary(max),
    @PUBKEY varchar(MAX)
AS
BEGIN
    INSERT INTO NHANVIEN (MANV, HOTEN, EMAIL, LUONG, TENDN, MATKHAU,PUBKEY)
    VALUES (@MANV, @HOTEN, @EMAIL, @LUONG, @TENDN, @MATKHAU, @PUBKEY);
END
GO
```

2. Stored dùng để truy vấn dữ liệu NHANVIEN

```
IF OBJECT_ID('SP_SEL_PUBLIC_ENCRYPT_NHANVIEN','P') IS NOT NULL
DROP PROCEDURE SP_SEL_PUBLIC_ENCRYPT_NHANVIEN
GO
CREATE PROCEDURE SP_SEL_PUBLIC_ENCRYPT_NHANVIEN
    @MANV NVARCHAR(100),
    @MATKHAU varbinary(max)
AS
BEGIN
    SELECT NV.MANV, NV.HOTEN, NV.EMAIL, NV.LUONG
    FROM NHANVIEN AS NV
    where nv.TENDN = @MANV and NV.MATKHAU = @MATKHAU
END
GO
```

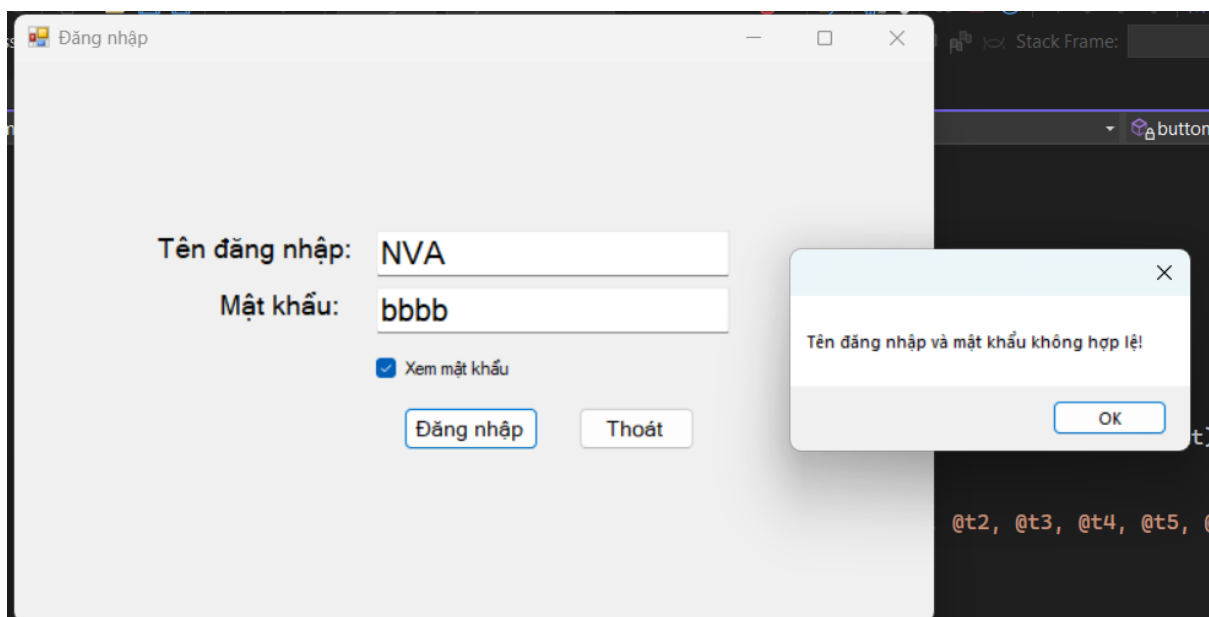
3. Xây dựng các màn hình quản lý sinh viên

a. Màn hình đăng nhập

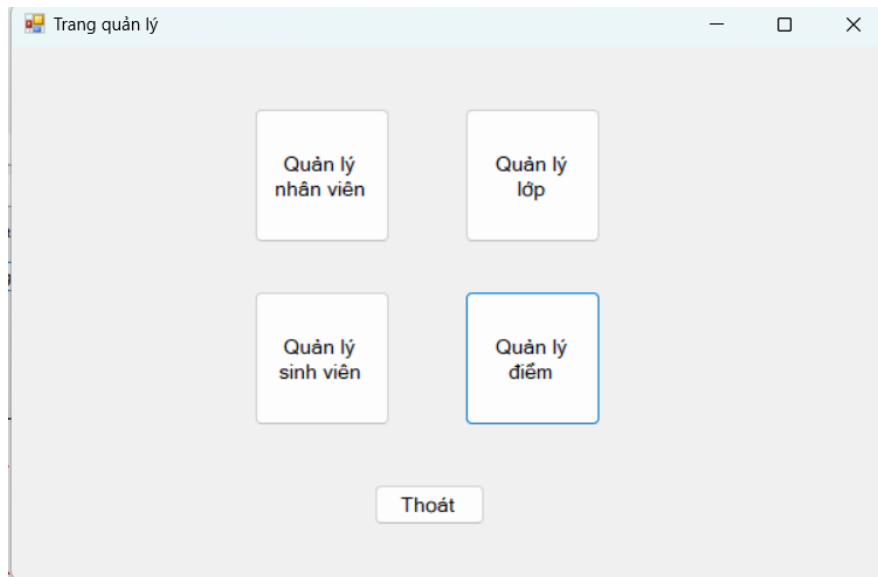
stored cho đăng nhập

```
IF OBJECT_ID('SP_SEL_LOG_IN', 'P') IS NOT NULL
DROP PROCEDURE SP_SEL_LOG_IN
GO
CREATE PROCEDURE SP_SEL_LOG_IN
    @TENDN NVARCHAR(100),
    @MATKHAU varbinary(max)
AS
BEGIN
    SELECT NV.MANV
    FROM NHANVIEN AS NV
    where nv.TENDN = @TENDN and NV.MATKHAU = @MATKHAU
END
GO
```

Màn hình ứng dụng:



Hình 1: Nhập sai thông tin đăng nhập



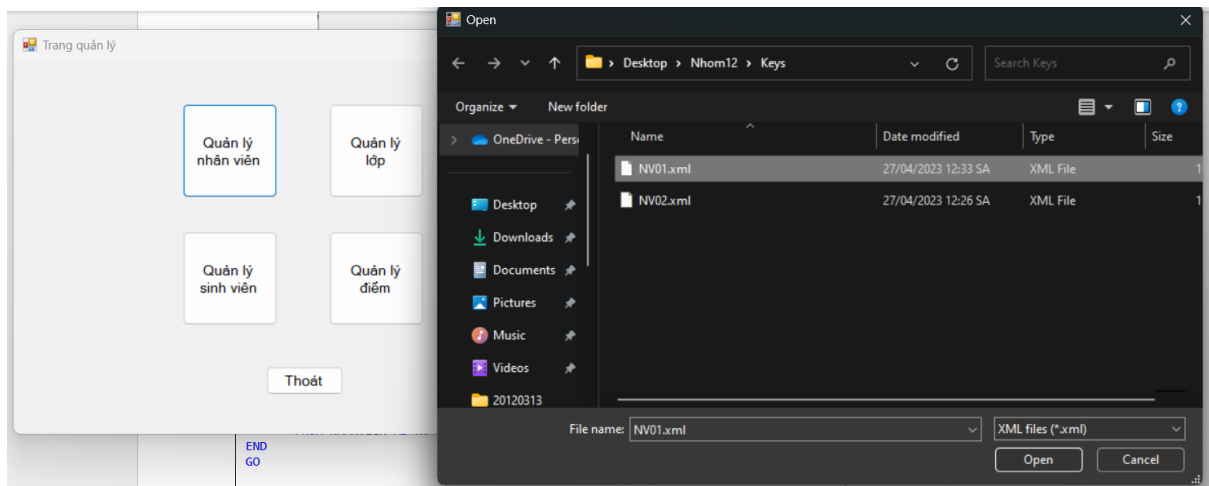
Hình 2: Chuyển sang trang quản lý khi nhập đúng

b. Màn hình quản lý nhân viên

Stored 1: Xem thông tin nhân viên

```
IF OBJECT_ID('SP_SEL_NHANVIEN', 'P') IS NOT NULL
DROP PROCEDURE SP_SEL_NHANVIEN
GO
CREATE PROCEDURE SP_SEL_NHANVIEN
AS
BEGIN
    SELECT NV.MANV, NV.HOTEN, NV.EMAIL, NV.LUONG, NV.PUBKEY
    FROM NHANVIEN AS NV
END
GO
```

Khi chọn chức năng quản lý nhân viên. Ứng dụng yêu cầu người dùng nhập file chứa các khoá của mình. Chỉ giải mã giá trị lương khi đúng khoá, các giá trị còn lại hiện Encrypted



Hình 3: Khóa của NV01

NhanVien

DANH MỤC NHÂN VIÊN

Thông tin nhân viên

Mã NV Họ tên

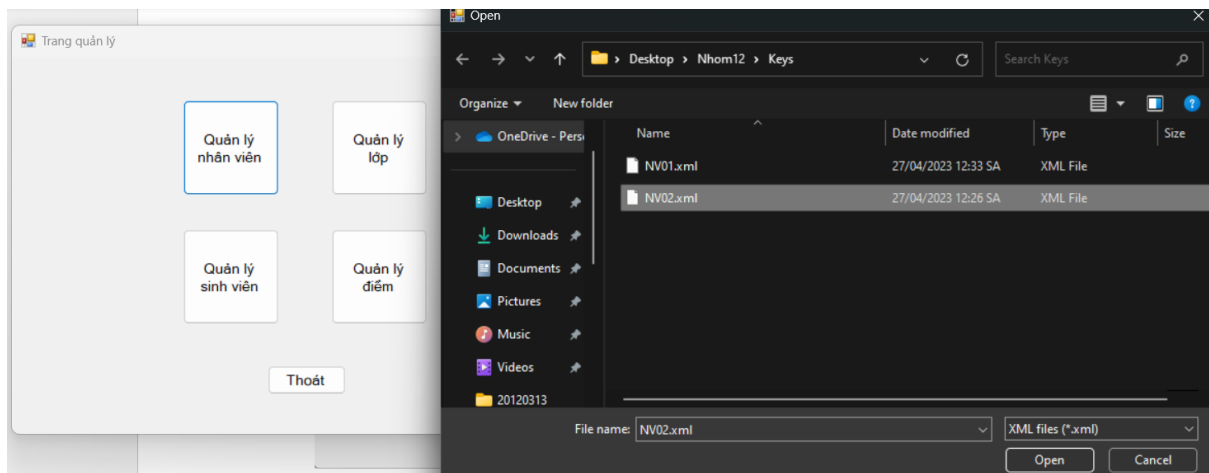
Email Lương

Tên DN Mật khẩu

	MANV	HOTEN	EMAIL	PUBKEY	LUONGNV
▶	NV01	NGUYEN VAN A	NVA@	3M/1oMYt3U2kk...	4000000
	NV02	NGUYEN VAN B	NVB@	38HRX3boONsvf...	Encrypted
*					

Thêm Xóa Sửa Ghi/Lưu Không Thoát

Hình 4: Giải mã lương NV01 là 4000000



Hình 5: Khoá của NV02

NhanVien

DANH MỤC NHÂN VIÊN

Thông tin nhân viên

Mã NV Họ tên

Email Lương

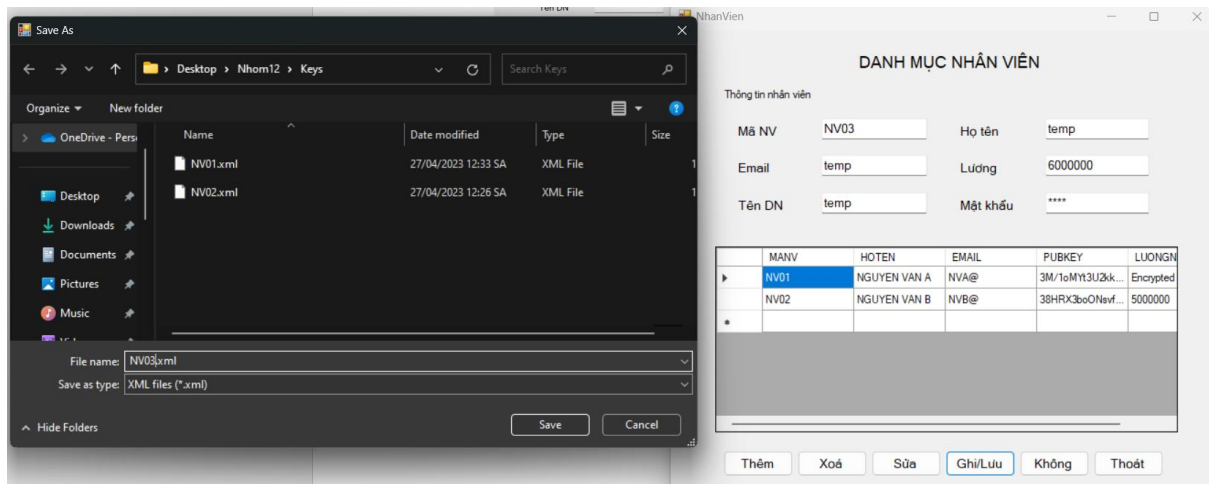
Tên DN Mật khẩu

	MANV	HOTEN	EMAIL	PUBKEY	LUONGNV
▶	NV01	NGUYEN VAN A	NVA@	3M/1oMYt3U2kk...	Encrypted
	NV02	NGUYEN VAN B	NVB@	38HRX3boONsvf...	5000000
*					

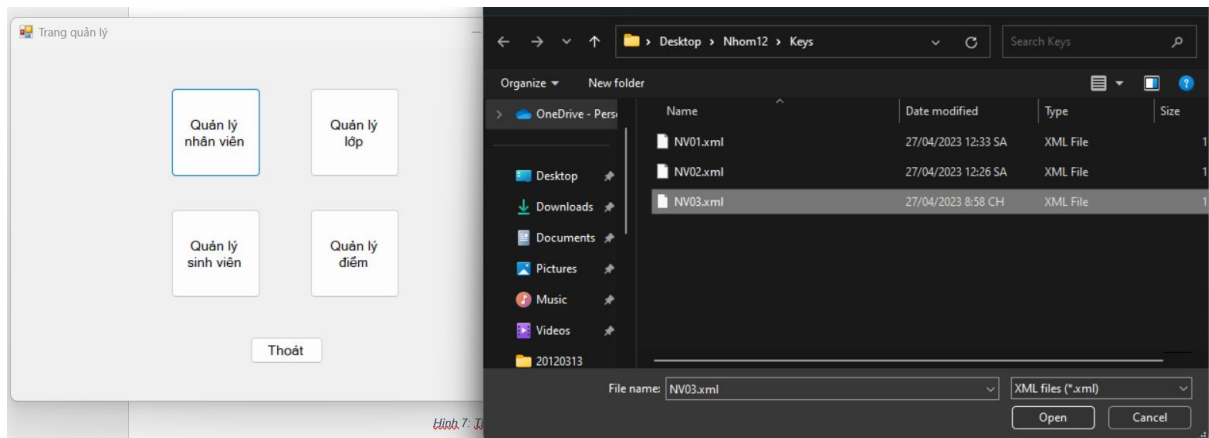
Thêm Xoá Sửa Ghi/Lưu Không Thoát

Hình 6: Giải mã lương NV02 là 5000000

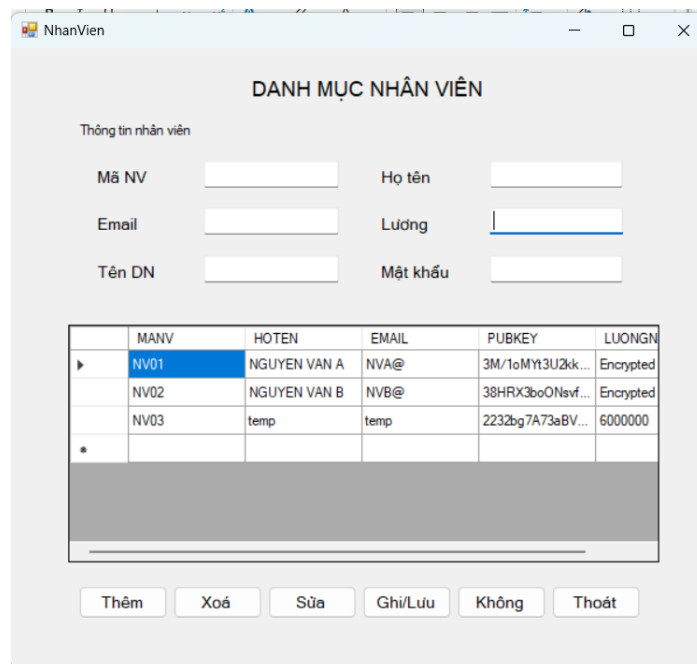
Chức năng thêm nhân viên: Yêu cầu người dùng lưu khoá của NV mới được thêm.



Hình 7: Thêm nhân viên NV03



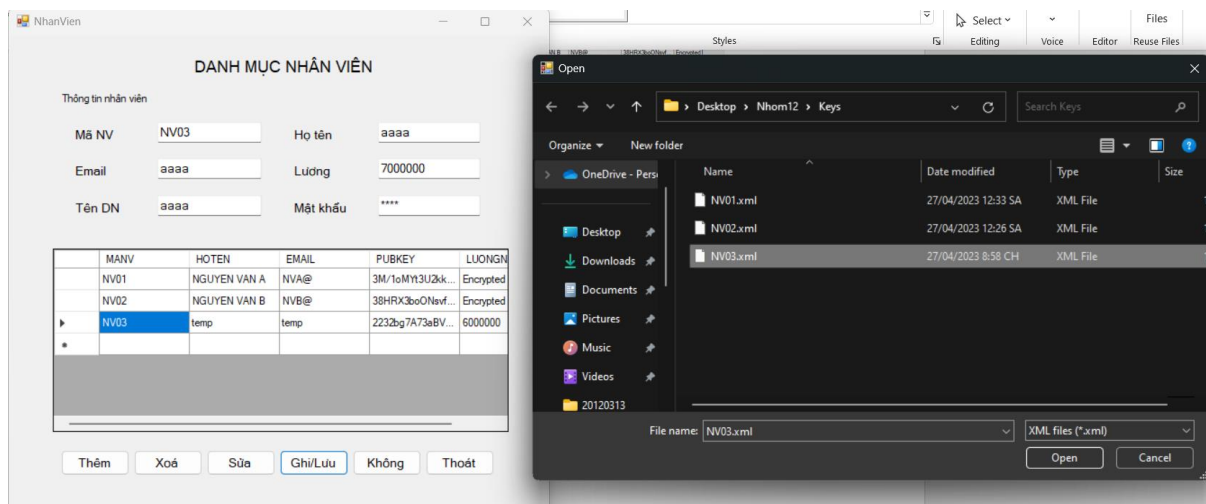
Hình 8: Dùng khóa NV03 để giải mã



Hình 9: Kết quả thấy lương của NV03 là 6000000

Chức năng chỉnh sửa thông tin nhân viên: Yêu cầu chọn file khoá của NV ấy

```
IF OBJECT_ID('SP_UPD_PUBLIC_ENCRYPT_NHANVIEN','P') IS NOT NULL
DROP PROCEDURE SP_UPD_PUBLIC_ENCRYPT_NHANVIEN
GO
CREATE PROCEDURE SP_UPD_PUBLIC_ENCRYPT_NHANVIEN
    @MANV VARCHAR(20),
    @HOTEN NVARCHAR(100),
    @EMAIL VARCHAR(20),
    @LUONG varbinary(max),
    @TENDN NVARCHAR(100),
    @MATKHAU varbinary(max)
AS
BEGIN
    UPDATE NHANVIEN
    set HOTEN = @HOTEN, EMAIL = @EMAIL, LUONG = @LUONG, TENDN = @TENDN, MATKHAU =
    @MATKHAU
    where MANV = @MANV
END
GO
```



Hình 10: Chỉnh sửa thông tin NV03

NhanVien

DANH MỤC NHÂN VIÊN

Thông tin nhân viên

Mã NV: NV03 Họ tên: aaaa

Email: aaaa Lương: 7000000

Tên DN: aaaa Mật khẩu: ****

	MANV	HOTEN	EMAIL	PUBKEY	LUONGN
▶	NV01	NGUYEN VAN A	NVA@	3M/1oMYt3U2kk...	Encrypted
	NV02	NGUYEN VAN B	NVB@	38HRX3boONsvf...	Encrypted
	NV03	aaaa	aaaa	223Zbg7A73aBV...	7000000
*					

Thêm Xóa Sửa Ghi/Lưu Không Thoát

Hình 11: Cập nhật thông tin NV03

Chức năng xoá nhân viên: Chọn nút xoá và nhập mã NV

NhanVien

DANH MỤC NHÂN VIÊN

Thông tin nhân viên

Mã NV: NV03 Họ tên: aaaa

Email: aaaa Lương: 7000000

Tên DN: aaaa Mật khẩu: ****

	MANV	HOTEN	EMAIL	PUBKEY	LUONGN
▶	NV01	NGUYEN VAN A	NVA@	3M/1oMYt3U2kk...	Encrypted
	NV02	NGUYEN VAN B	NVB@	38HRX3boONsvf...	Encrypted
*					

Thêm Xóa Sửa Ghi/Lưu Không Thoát

Hình 12: Xoá NV03

c. Màn hình quản lý lớp

Chức năng xem lớp:

	MALOP	TENLOP	MANV
▶	L01	Công nghệ thông...	NV01
	L02	Công nghệ thông...	NV02
	L03	ABC	NV02
*			

Chức năng chỉnh sửa lớp

Chỉnh sửa thông tin lớp học

Mã lớp: L04

Tên lớp: AAA

GVCN: NV01

Thêm lớp

Xóa lớp

Quay lại

Thêm lớp thành công!!

OK

Lop

Danh sách lớp học

Xem danh sách Sửa danh sách lớp

	MALOP	TENLOP	MANV
▶	L01	Công nghệ thông...	NV01
	L02	Công nghệ thông...	NV02
	L03	ABC	NV02
	L04	AAA	NV01
*			

Quay lại Thoát

d. Màn hình quản lý sinh viên

Chức năng quản lý sinh viên: Người dùng nhập lớp và chọn tra cứu

SinhVien

Danh sách sinh viên

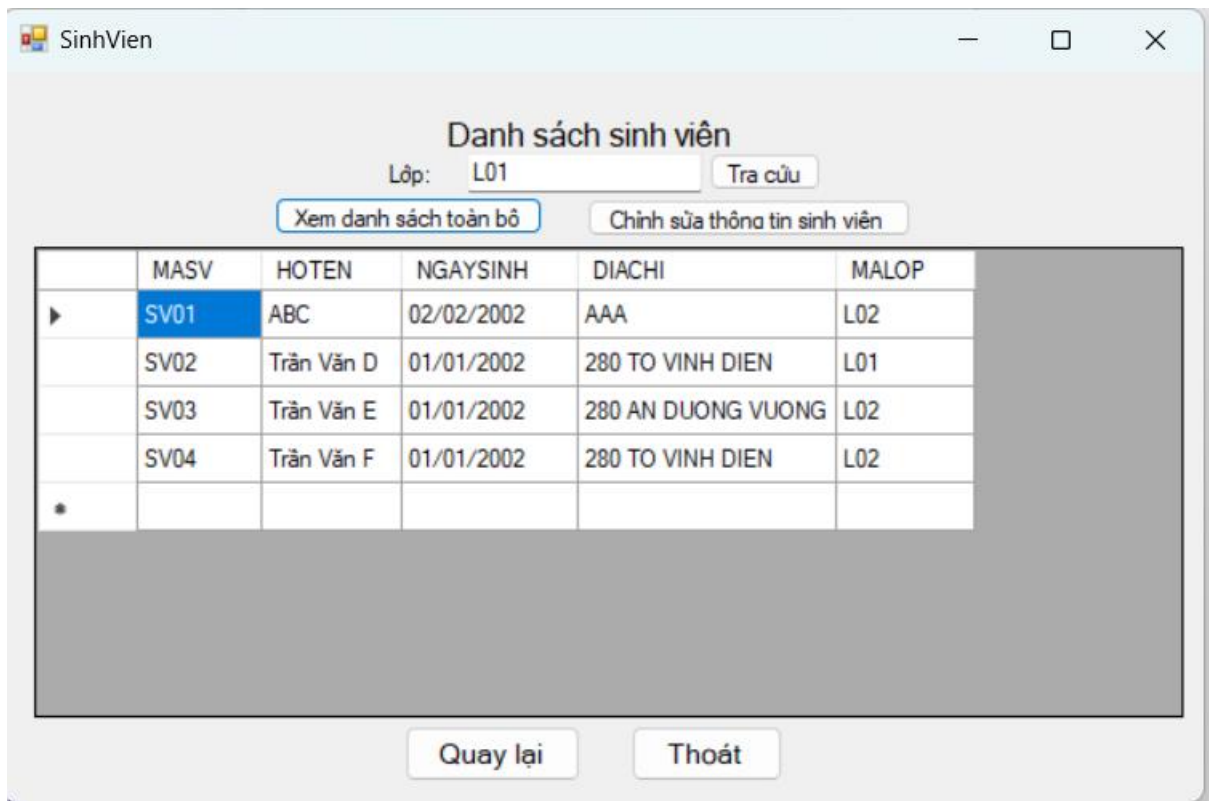
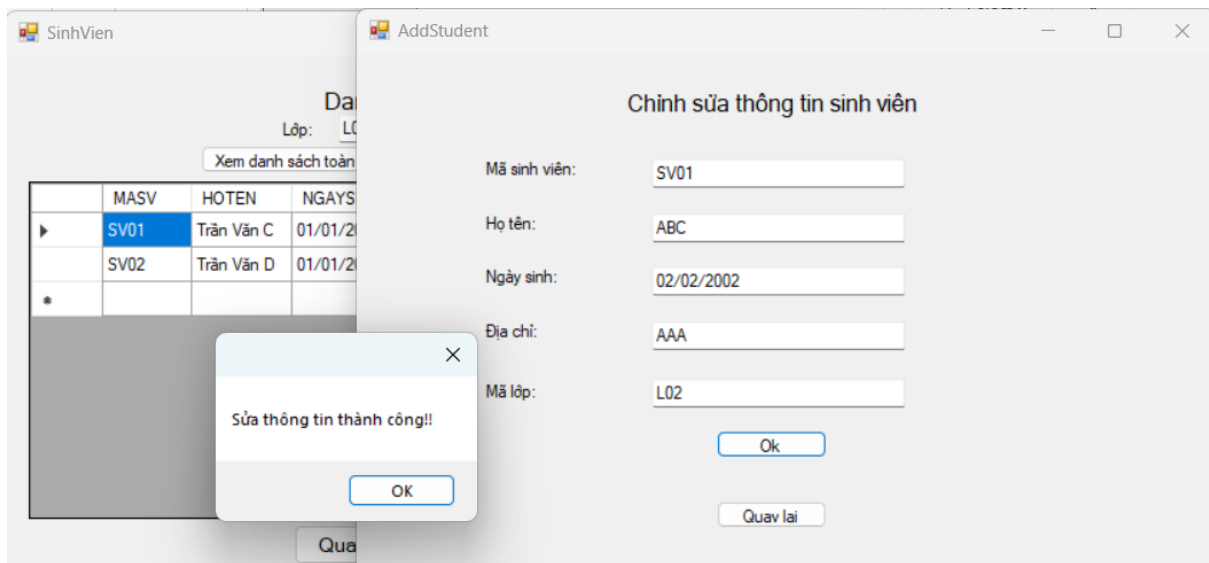
Lớp: L01 Tra cứu

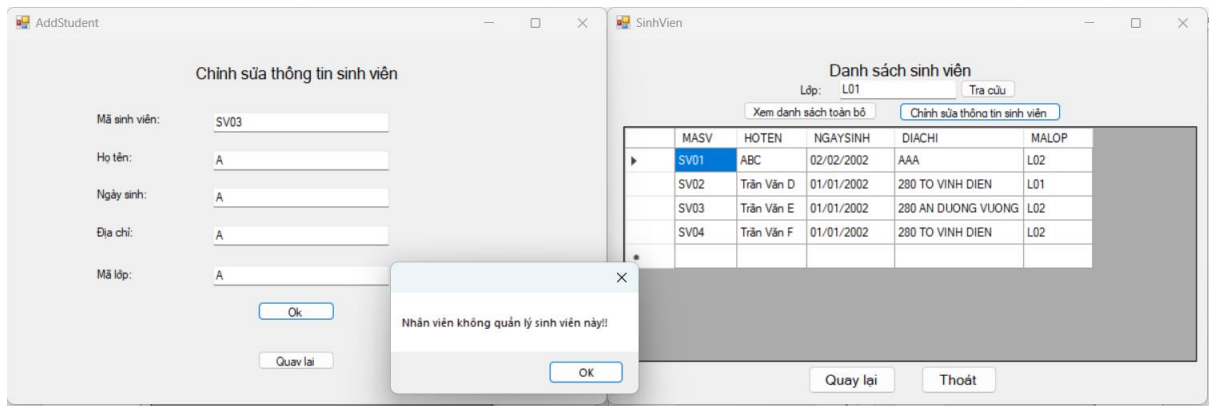
Xem danh sách toàn bộ Chỉnh sửa thông tin sinh viên

	MASV	HOTEN	NGAYSINH	DIACHI	MALOP
▶	SV01	Trần Văn C	01/01/2002	280 AN DUONG VUONG	L01
	SV02	Trần Văn D	01/01/2002	280 TO VINH DIEN	L01
*					

Quay lại Thoát

Chức năng chỉnh sửa sinh viên: chỉ có giáo viên quản lý sinh viên này mới có thể chỉnh sửa.



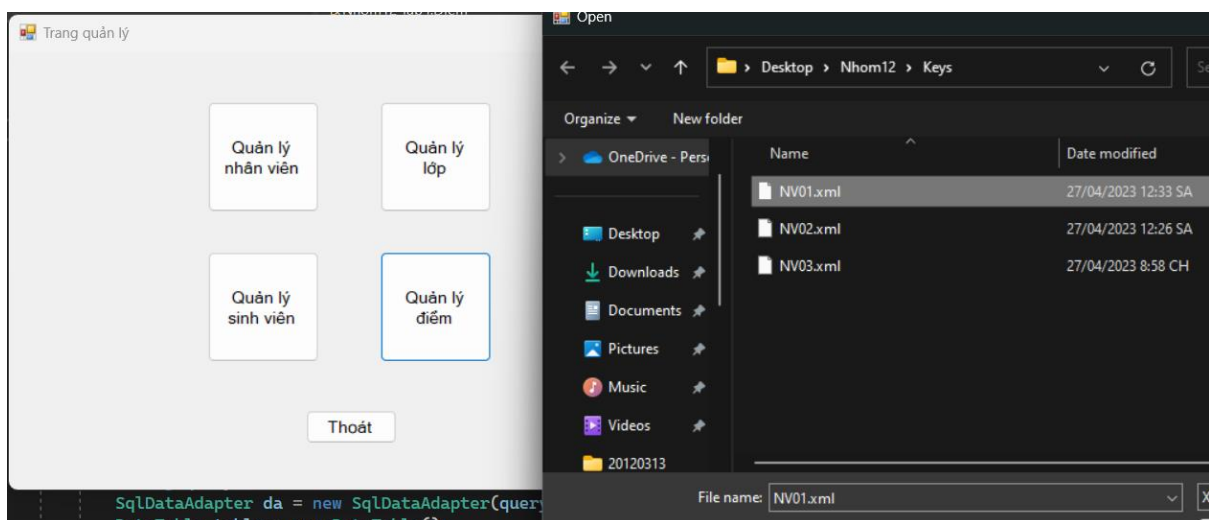


e. Màn hình nhập điểm

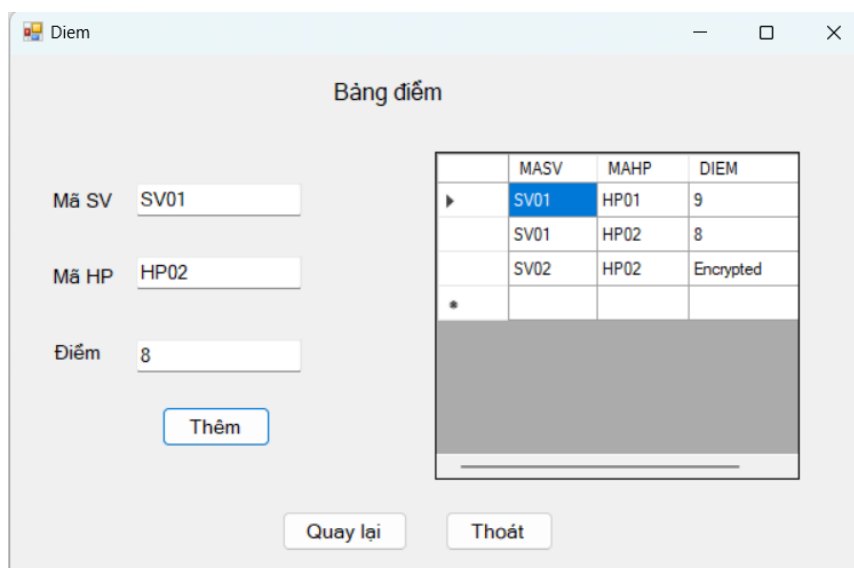
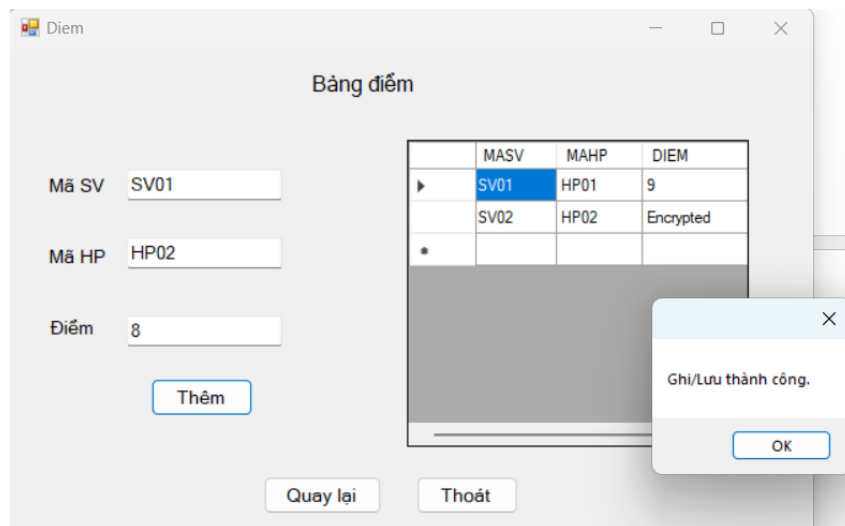
Chức năng nhập điểm:

```
IF OBJECT_ID('SP_INS_PUBLIC_ENCRYPT_BANGDIEM', 'P') IS NOT NULL
DROP PROCEDURE SP_INS_PUBLIC_ENCRYPT_BANGDIEM
GO
CREATE PROCEDURE SP_INS_PUBLIC_ENCRYPT_BANGDIEM
    @MASV VARCHAR(20),
    @MAHP VARCHAR(20),
    @DIEMTHI varbinary(max)
AS
BEGIN
    INSERT INTO BANGDIEM (MASV, MAHP, DIEMTHI)
    VALUES (@MASV, @MAHP, @DIEMTHI);
END
GO
```

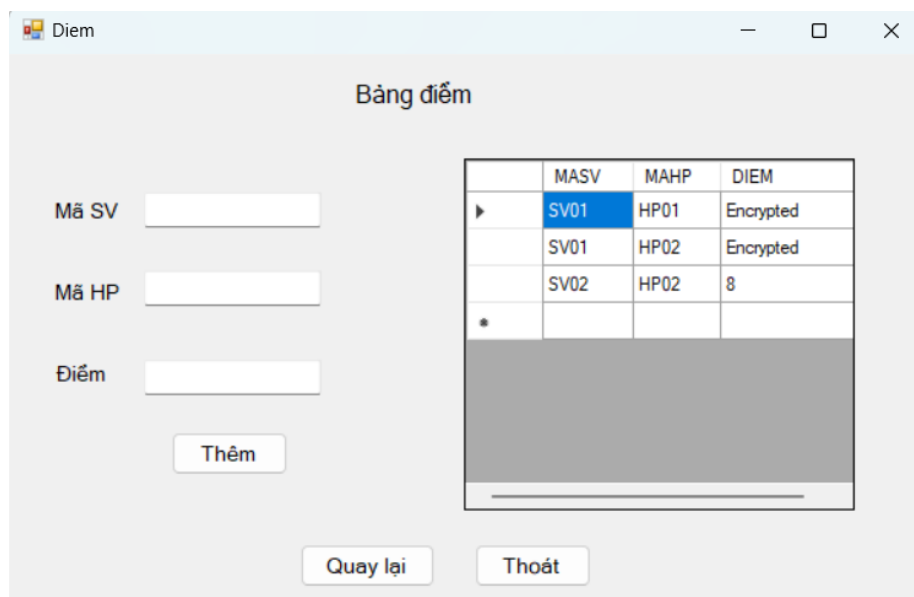
Màn hình thêm điểm: Khi người dùng chọn chức năng quản lý điểm, ứng dụng sẽ yêu cầu nhập file khoá.



Nhập điểm ở khung bên trái, khoá của nhân viên nào thì chỉ hiện điểm do nhân viên đó nhập

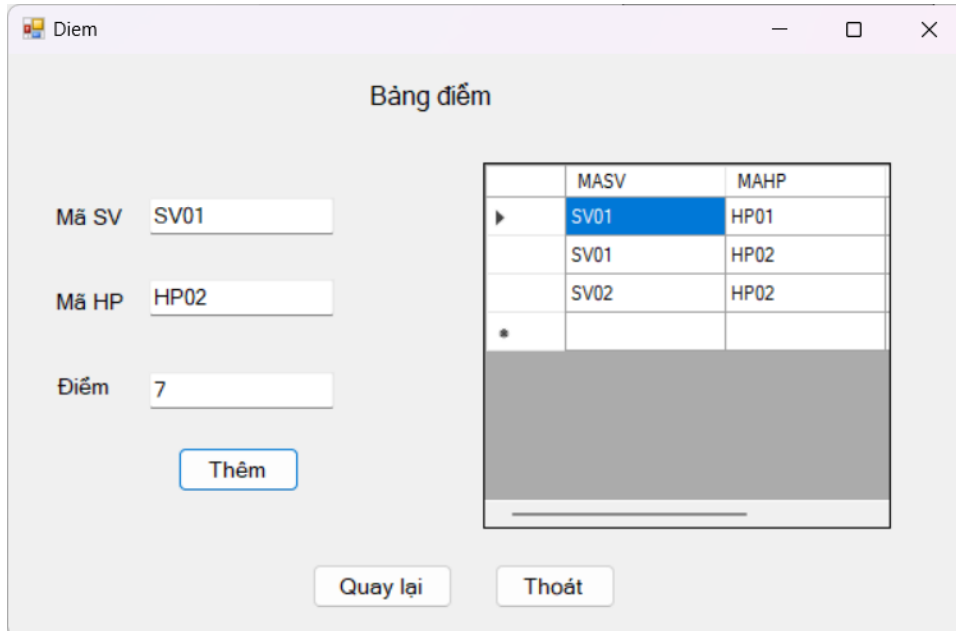


Khi chọn khoá của **nhân viên 2**



4. Theo dõi thao tác nhập điểm trong SQL Profile

Sau khi đăng nhập vào tài khoản NVA, password: bbbbbbbb và nhập điểm của SV01, HP01, điểm là 7, điểm được nhập được chấp nhận và lưu thành công, sau đó lưu vào database.



The screenshot shows a window titled "Diem" with a subtitle "Bảng điểm". On the left, there is a form with three input fields: "Mã SV" (Student ID) with the value "SV01", "Mã HP" (Homework ID) with the value "HP02", and "Điểm" (Score) with the value "7". Below these fields is a blue button labeled "Thêm" (Add). On the right, there is a table with two columns: "MASV" and "MAHP". The table contains three rows of data: (SV01, HP01), (SV01, HP02), and (SV02, HP02). The first row is highlighted in blue. Below the table is a grey rectangular area. At the bottom of the window, there are two buttons: "Quay lại" (Go back) and "Thoát" (Exit).

MASV	MAHP
SV01	HP01
SV01	HP02
SV02	HP02

Trong SQL Profiler cho ta biết được có user đã insert dữ liệu điểm vào database.

Câu truy vấn:

```
exec sp_executesql N'SP_INS_PUBLIC_ENCRYPT_BANGDIEM @t1,
@t2, @t3',N'@t1 nvarchar(4),@t2 nvarchar(4),@t3
varbinary(128)',@t1=N'SV01',@t2=N'HP02',@t3=0x419DBAD5C5D4F
04EB1D7B4B2EBF6F616D3B212823B305C212F18FD4214F2F6CCCF6E60
D8C1406EE0E269A9A4CF620AF7B93DCE52D93172BAD0A5071E3778CC
191C8D9605758D27379031FBE17A06BB4108E8098D098E09D9C51056A4
28166FD0191388BCC0538EF2EF524586136F4E7FAA0C5CBCF09DB1759
38550A3B0A378C9.
```

SQL Server Profiler - [Untitled - 1 (DESKTOP-A79AAA6\MSSQLSERVER01)]												
File Edit View Replay Tools Window Help												
EventClass	TextData	ApplicationName	NTUserName	LoginName	CPU	Reads	Writes	Duration	ClientProcessID	SPID	StartTime	EndTime
Trace Start											2023-04-30 15:51:02...	
ExistingConnection	-- network protocol: LPC set quoted...	Microsoft SQL...	Admin	DESKTO...					22412	65	2023-04-30 15:40:06...	
ExistingConnection	-- network protocol: LPC set quoted...	Microsoft SQL...	Admin	DESKTO...					22412	67	2023-04-30 15:40:07...	
ExistingConnection	-- network protocol: LPC set quoted...	SQLServerCEIP	SQLTELE...	NT SER...					14016	68	2023-04-30 15:49:20...	
ExistingConnection	-- network protocol: LPC set quoted...	.Net SqlClie...	Admin	DESKTO...					25568	76	2023-04-30 15:50:53...	
Audit Login	-- network protocol: LPC set quoted...	.Net SqlClie...	Admin	DESKTO...					16504	77	2023-04-30 15:51:10...	
RPC:Completed	exec sp_executesql N'EXEC SP_SEL_LOG...	.Net SqlClie...	Admin	DESKTO...	0	148	3	6	16504	77	2023-04-30 15:51:10...	2023-04-30 15:51:10...
Audit Logout		.Net SqlClie...	Admin	DESKTO...	0	148	3	3854	16504	77	2023-04-30 15:51:10...	
RPC:Completed	exec sp_reset_connection	.Net SqlClie...	Admin	DESKTO...	0	0	0	0	16504	77	2023-04-30 15:51:14...	2023-04-30 15:51:14...
Audit Login	-- network protocol: LPC set quoted...	.Net SqlClie...	Admin	DESKTO...					16504	77	2023-04-30 15:51:14...	
SQL:BatchStarting	exec SP_SEL_PUBLIC_ENCRYPT_BANDIS...	.Net SqlClie...	Admin	DESKTO...					16504	77	2023-04-30 15:51:14...	
SQL:BatchCompleted	exec SP_SEL_PUBLIC_ENCRYPT_BANDIS...	.Net SqlClie...	Admin	DESKTO...	0	22	0	1	16504	77	2023-04-30 15:51:14...	2023-04-30 15:51:14...
Audit Logout		.Net SqlClie...	Admin	DESKTO...	0	170	3	13286	16504	77	2023-04-30 15:51:14...	2023-04-30 15:51:14...
RPC:Completed	exec sp_reset_connection	.Net SqlClie...	Admin	DESKTO...	0	0	0	0	16504	77	2023-04-30 15:51:27...	2023-04-30 15:51:27...
Audit Login	-- network protocol: LPC set quoted...	.Net SqlClie...	Admin	DESKTO...					16504	77	2023-04-30 15:51:27...	
RPC:Completed	exec sp_executesql N'SP_TNS_PUBLIC_E...	.Net SqlClie...	Admin	DESKTO...	0	473	0	4	16504	77	2023-04-30 15:51:27...	2023-04-30 15:51:27...
Audit Logout		.Net SqlClie...	Admin	DESKTO...	0	643	3	19476	16504	77	2023-04-30 15:51:27...	2023-04-30 15:51:27...
RPC:Completed	exec sp_reset_connection	.Net SqlClie...	Admin	DESKTO...	0	0	0	0	16504	77	2023-04-30 15:51:46...	2023-04-30 15:51:46...
Audit Login	-- network protocol: LPC set quoted...	.Net SqlClie...	Admin	DESKTO...					16504	77	2023-04-30 15:51:46...	
SQL:BatchStarting	exec SP_SEL_PUBLIC_ENCRYPT_BANDIS...	.Net SqlClie...	Admin	DESKTO...					16504	77	2023-04-30 15:51:46...	
SQL:BatchCompleted	exec SP_SEL_PUBLIC_ENCRYPT_BANDIS...	.Net SqlClie...	Admin	DESKTO...	0	44	0	1	16504	77	2023-04-30 15:51:46...	2023-04-30 15:51:46...
Trace Pause											2023-04-30 15:52:07...	
exec sp_executesql N'SP_TNS_PUBLIC_ENCRYPT_BANDIS @E1, @E2, @E3' N'E1 nvarchar(4),@E2 nvarchar(4),@E3 varbinary(128)',@E1=N'SV02',@E2=N'HP02',@E3=0x419DBAD5C5D4F04EB1D7B4B2EBF6F616D3B212823B305C212F18FD4214F2 F6CCCF6E60D8C1406EE0E269A9A4CF620AF7B93DCE52D93172BAD0A5071E3 778CC191C8D9605758D27379031FBE17A06BB4108E8098D098E09D9C51056A4 28166FD0191388BCC0538EF2EF524586136F4E7FAA0C5CBCF09DB175938550A 3B0A378C9)												
Trace is paused.												Ln 16, Col 2 Rows: 22
												Connections: 1

Nhận xét: Điểm được nhập từ client dưới dạng bản rõ, khi nhấn lưu, dữ liệu điểm sẽ được mã hóa RSA ngay trên client với khoá được nhập khi người dùng chọn chức năng “Quản lý điểm” sau đó mới được gửi đến và lưu vào database dưới dạng bản mã (điểm = 0x419DBAD5C5D4F04EB1D7B4B2EBF6F616D3B212823B305C212F18FD4214F2F6CCCF6E60D8C1406EE0E269A9A4CF620AF7B93DCE52D93172BAD0A5071E3778CC191C8D9605758D27379031FBE17A06BB4108E8098D098E09D9C51056A428166FD0191388BCC0538EF2EF524586136F4E7FAA0C5CBCF09DB175938550A3B0A378C9)