



# FIT@HCMUS

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN, ĐHQG - HCM  
KHOA CÔNG NGHỆ THÔNG TIN



## LAB 4 - NHÓM

BỘ MÔN: BẢO MẬT CƠ SỞ DỮ LIỆU

Sinh viên thực hiện:

21120396 - Đào Thị Ngọc Giàu

21120419 - Vũ Thành Công

21120446 - Kiên Đình Mỹ Hạnh

TP. Hồ Chí Minh, tháng 5/2024

## **Mục lục**

<b>I. Các stored procedure .....</b>	<b>2</b>
<b>1. Store procedure SP_INS_PUBLIC_ENCRYPT_NHANVIEN.....</b>	<b>2</b>
<b>a. Cài đặt .....</b>	<b>2</b>
<b>b. Thực thi.....</b>	<b>2</b>
<b>2. Store procedure SP_SEL_PUBLIC_ENCRYPT_NHANVIEN.....</b>	<b>2</b>
<b>a. Cài đặt .....</b>	<b>2</b>
<b>b. Thực thi.....</b>	<b>2</b>
<b>II. Màn hình quản lý đăng nhập .....</b>	<b>3</b>
<b>III. Màn hình quản lý nhân viên.....</b>	<b>4</b>
<b>1. Thêm một nhân viên.....</b>	<b>5</b>
<b>2. Xem lương.....</b>	<b>7</b>
<b>IV. Màn hình quản lý lớp học.....</b>	<b>9</b>
<b>V. Màn hình quản lý sinh viên của từng lớp .....</b>	<b>9</b>
<b>1. Với lớp thuộc quyền quản lý của GV đã đăng nhập.....</b>	<b>9</b>
<b>2. Với lớp không thuộc quyền quản lý của GV đã đăng nhập .....</b>	<b>12</b>
<b>VI. Màn hình nhập bảng điểm.....</b>	<b>16</b>
<b>VII. Theo dõi thao tác nhập điểm bằng SQL Profile.....</b>	<b>18</b>

## I. Các stored procedure

### 1. Store procedure SP\_INS\_PUBLIC\_ENCRYPT\_NHANVIEN

#### a. Cài đặt

```

CREATE PROC SP_INS_PUBLIC_ENCRYPT_NHANVIEN
(
    @MANV VARCHAR(20),
    @HOTEN NVARCHAR(100),
    @EMAIL VARCHAR(20),
    @LUONG VARBINARY(MAX),
    @TENDN NVARCHAR(100),
    @MATKHAU VARBINARY(MAX),
    @PUB VARCHAR(MAX)
)
AS
INSERT INTO NHANVIEN(MANV, HOTEN, EMAIL, LUONG, TENDN, MATKHAU, PUBKEY)
VALUES (@MANV, @HOTEN, @EMAIL, @LUONG, @TENDN, @MATKHAU, @PUB);

```

#### b. Thực thi

```

150 EXEC SP_INS_PUBLIC_ENCRYPT_NHANVIEN 'NV12', N'Omega Tooth', 'omega@mail.com', 0x55E5E5DA35A9F7C881CEE6957EAA10FE52FE42A5FEFAC06340B0926EEFC9F0B68845...
151 -- manv: NV11
152 -- pass: omegaxxx
153 -- luong: 4500
154
155 SELECT * FROM NHANVIEN where MANV = 'NV12'
156

```

MANV	HOTEN	EMAIL	LUONG	TENDN	MATKHAU	PUBKEY
1	NV12	Omega Tooth	omega@mail.com	0x55E5E5DA35A9F7C881CEE6957EAA10FE52FE42A5FEFAC0...	omega	0x34C4EDC6C5364C6B11E8180A01162BADD1070CD7

### 2. Store procedure SP\_SEL\_PUBLIC\_ENCRYPT\_NHANVIEN

#### a. Cài đặt

```

CREATE PROC SP_SEL_PUBLIC_ENCRYPT_NHANVIEN
(
    @TENDN NVARCHAR(100),
    @MATKHAU VARBINARY(MAX)
)
AS
SELECT MANV, HOTEN, EMAIL, LUONG
FROM NHANVIEN
WHERE TENDN = @TENDN AND MATKHAU = @MATKHAU

```

#### b. Thực thi

```

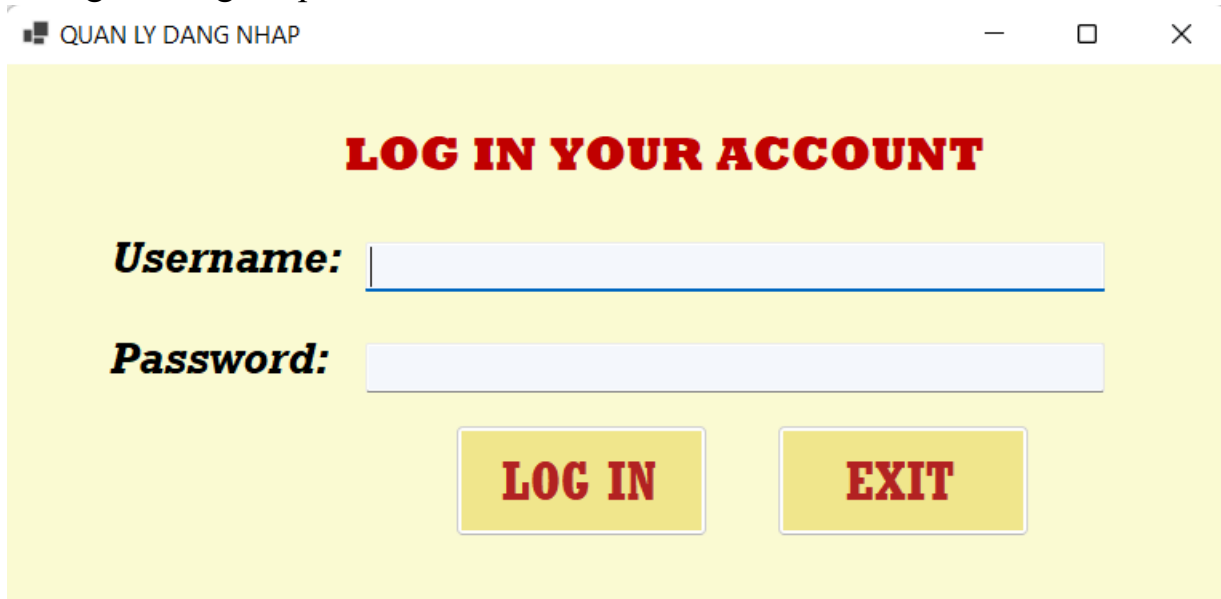
159
160 EXEC SP_SEL_PUBLIC_ENCRYPT_NHANVIEN N'omega', 0x34C4EDC6C5364C6B11E8180A01162BADD1070CD7
161

```

MANV	HOTEN	EMAIL	LUONG
1	NV12	Omega Tooth	omega@mail.com

## II. Màn hình quản lý đăng nhập

Thông tin đăng nhập là tài khoản nhân viên với MANV và MATKHAU



**LOG IN YOUR ACCOUNT**

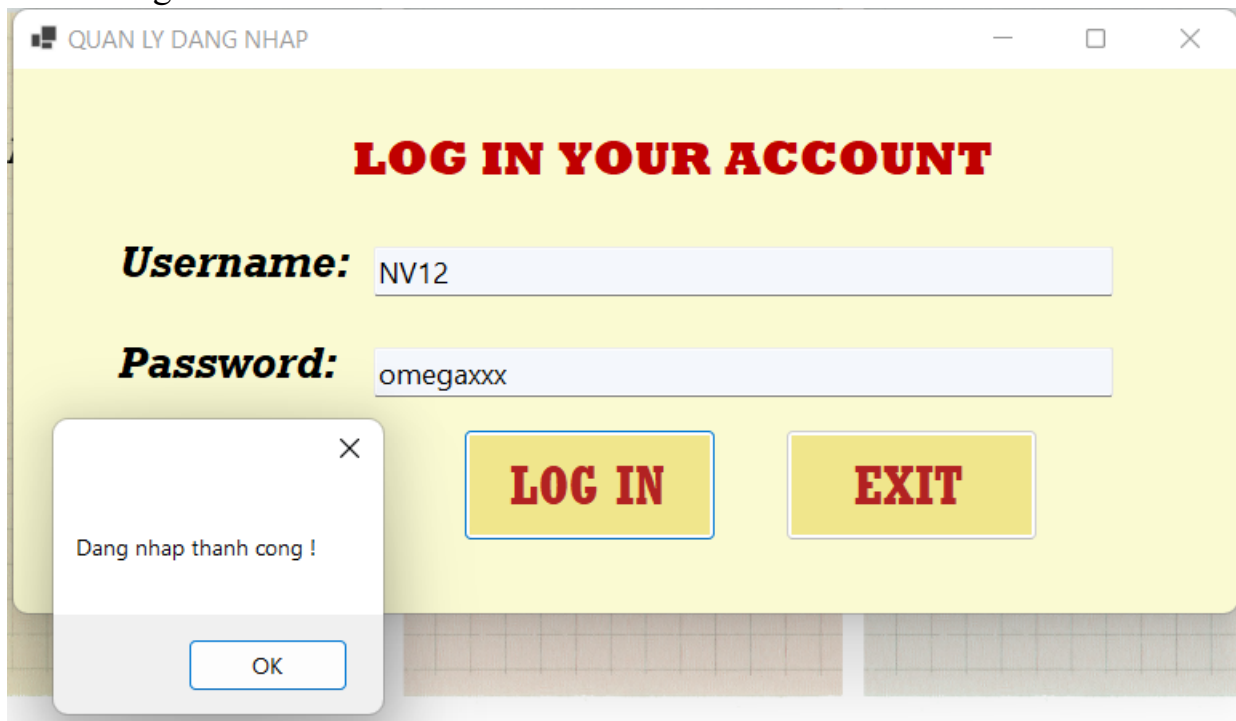
**Username:**

**Password:**

**LOG IN** **EXIT**

Màn hình đăng nhập

Sau khi nhập thông tin đăng nhập, ta sẽ được một thông báo hiện lên nếu đăng nhập thành công:



**LOG IN YOUR ACCOUNT**

**Username:** NV12

**Password:** omegaxxx

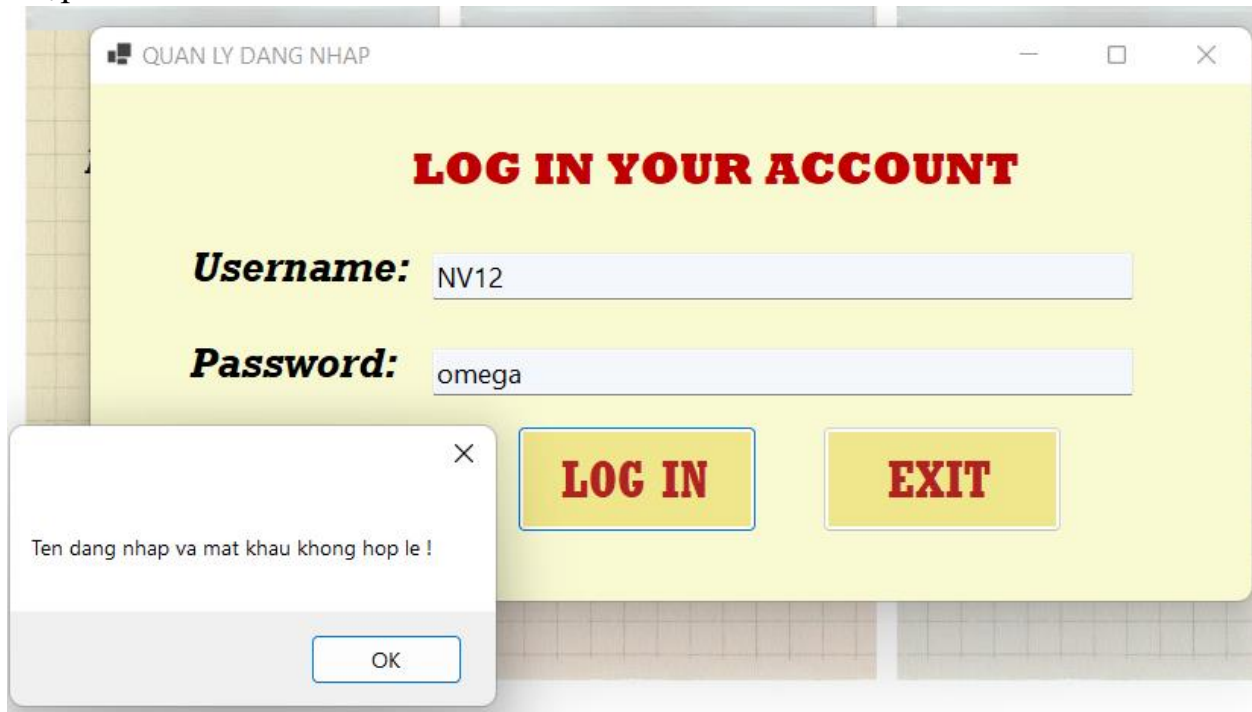
**LOG IN** **EXIT**

Đăng nhập thành công !

OK

Thông báo đăng nhập thành công

Ngược lại, với tên đăng nhập hoặc mật khẩu sai, sẽ hiện ra thông báo rằng tên đăng nhập đã sai:



*Thông báo đăng nhập thất bại*

### **III. Màn hình quản lý nhân viên**

Sau khi đã đăng nhập thành công, màn hình DANH SÁCH NHÂN VIÊN sẽ hiện ra:



*Màn hình danh sách nhân viên*

### 1. Thêm một nhân viên


Trước khi tạo 1 nhân viên, nhóm đã sử dụng Openssl để tạo ra cặp khóa public key và private key tương ứng với MANV được nhập vào.


Với cấu trúc lưu trữ khóa là:

MANV + priv.pem: đối với private key

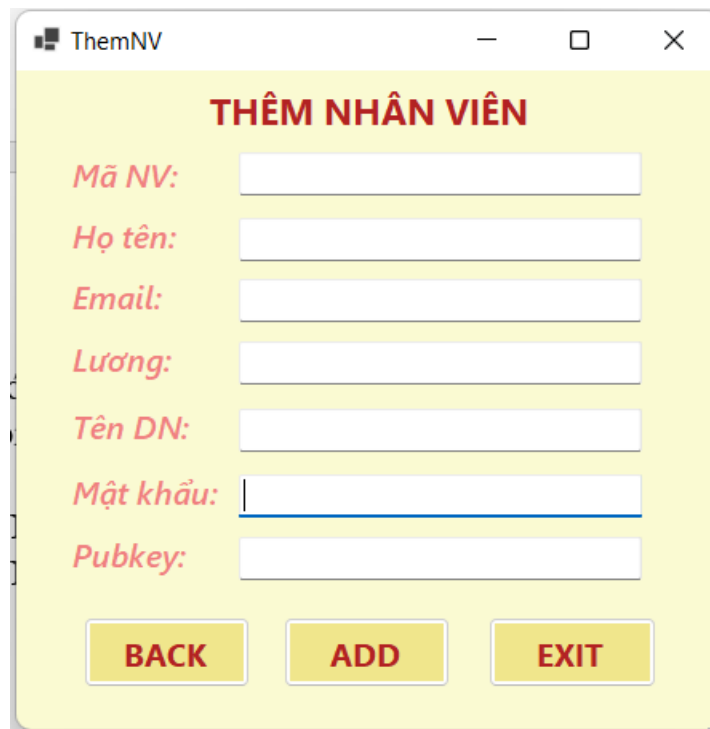
MANV + pub.pem: đối với public key

Ví dụ:

 NV12priv.pem

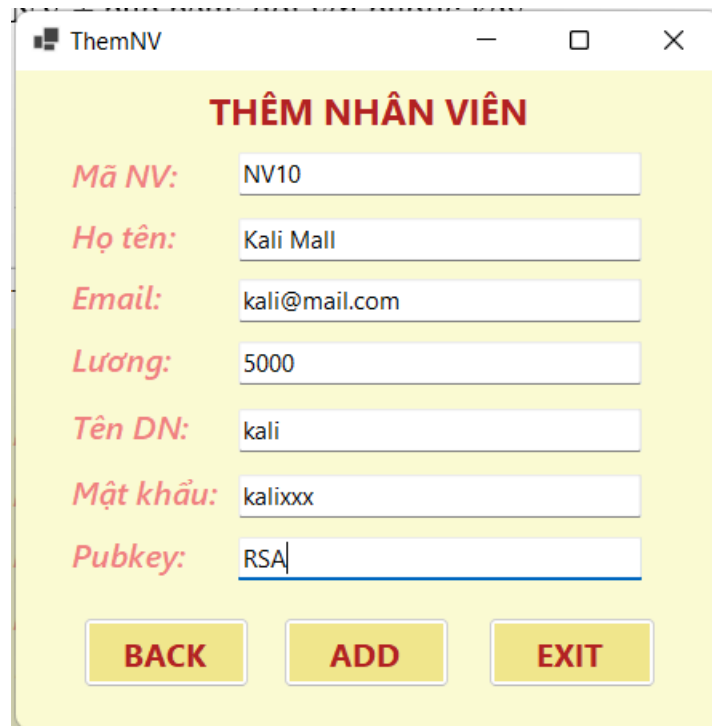
 NV12pub.pem

Khi nhấn vào button ADD NHÂN VIÊN, màn hình điền thông tin nhân viên sẽ hiện ra



*Màn hình thêm nhân viên*

Sau đó chỉ việc điền các thông tin vào:



**ThemNV**

**THÊM NHÂN VIÊN**

**Mã NV:** NV10

**Họ tên:** Kali Mall

**Email:** kali@mail.com

**Lương:** 5000

**Tên DN:** kali

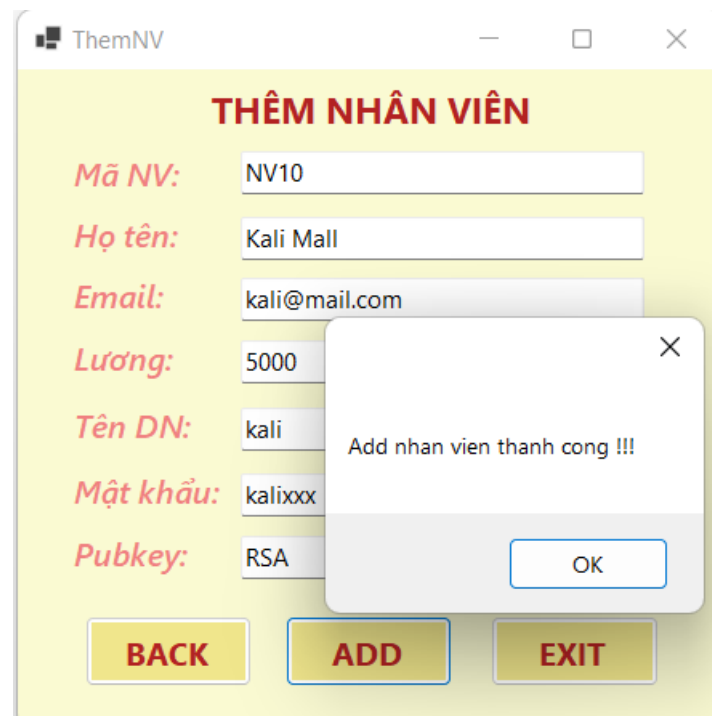
**Mật khẩu:** kalixxx

**Pubkey:** RSA

**BACK** **ADD** **EXIT**

*Nhập thông tin nhân viên*

Nếu đăng nhập thành công, một box sẽ hiện ra rằng bạn đã add thành công. Với khóa NV10pub.pem đã được generate từ Openssl từ trước, thì giá trị LUONG sẽ được mã hóa bằng khóa đó.



**ThemNV**

**THÊM NHÂN VIÊN**

**Mã NV:** NV10

**Họ tên:** Kali Mall

**Email:** kali@mail.com

**Lương:** 5000

**Tên DN:** kali

**Mật khẩu:** kalixxx

**Pubkey:** RSA

**BACK** **ADD** **EXIT**

**Add nhan vien thanh cong !!!**

**OK**

*Thêm nhân viên thành công*

Khi đó, nhân viên mới thêm vào có giá trị LUONG đã bị mã hóa bởi khóa public key.



	MÃ NV	HỌ TÊN	EMAIL	LƯƠNG	TÊN DN
▶	NV10	Kali Mall	kali@mail.com	System.Byte[]	kali
	NV11	Burp Suite	burp@mail.com	System.Byte[]	burp
	NV12	Omega Tooth	omega@mail.c...	System.Byte[]	omega
*					

*Giá trị cột LUONG của nhân viên mới đã được mã hóa*

## 2. Xem lương

Với cấu trúc lưu trữ khóa là:

MANV + priv.pem: đối với private key

MANV + pub.pem: đối với public key

Ví dụ:

- NV12priv.pem
- NV12pub.pem

Khi đó, với thông tin từ màn hình đăng nhập, ta có được MANV. Vì vậy khi muốn xem giá trị cột LUONG thì chỉ có thể xem được giá trị cột LUONG của nhân viên đã đăng nhập.

Để thuận tiện hơn, nhóm đã đặt cấu trúc file như trên và khi chọn XEM LƯƠNG, chương trình sẽ tự động đọc file NV12priv.pem để thực hiện decrypt cột LUONG. Và ta có kết quả như sau:



FormDSNhanVien

## DANH SÁCH NHÂN VIÊN

ADD NHÂN VIÊN
XEM LUONG

	MÃ NV	HỌ TÊN	EMAIL	LƯƠNG	TÊN DN
▶	NV10	Kali Mall	kali@mail.com	System.Byte[]	kali
	NV11	Burp Suite	burp@mail.com	System.Byte[]	burp
	NV12	Omega Tooth	omega@mail.c...	System.Byte[]	omega
*					

Chi xem duoc LUONG cua nhan vien da dang nhap !!!

OK

DANH SÁCH LỚP HỌC
EXIT

*Xem giá trị cột LUONG*

Sau khi nhấn “OK”, ta sẽ xem được cột LUONG của nhân viên đã đăng nhập

FormDSNhanVien

## DANH SÁCH NHÂN VIÊN

ADD NHÂN VIÊN
XEM LUONG

	MÃ NV	HỌ TÊN	EMAIL	LƯƠNG	TÊN DN
▶	NV12	Omega Tooth	omega@mail.c...	4500	omega
*					

DANH SÁCH LỚP HỌC
EXIT

*Giá trị cột LUONG của nhân viên đã đăng nhập*

#### IV. Màn hình quản lý lớp học

Màn hình quản lý lớp học hiển thị toàn bộ thông tin về các lớp học hiện đang có trong database.

	MÃ LỚP	TÊN LỚP	MÃ NV
▶	CNSH-K21	CÔNG NGHỆ SINH HỌC KHÓA 21	NV11
	CNTT-K21	CÔNG NGHỆ THÔNG TIN KHÓA 21	NV12
	CNTT-K35	CÔNG NGHỆ THÔNG TIN KHÓA 35	NV12
	CNTT-K46	CÔNG NGHỆ THÔNG TIN KHÓA 46	NV12
•			

Buttons: BACK, DS SINH VIÊN, EXIT

Màn hình quản lý lớp học

#### V. Màn hình quản lý sinh viên của từng lớp

Sau khi chọn lớp học mà muốn xem danh sách, ta nhấn vào button DS SINH VIÊN, sẽ thấy được danh sách toàn bộ sinh viên của lớp đó.

##### 1. Với lớp thuộc quyền quản lý của GV đã đăng nhập

Nhân viên đăng nhập với tài khoản của NV12, vì thế ta chọn 1 trong 3 lớp phía dưới để theo dõi. Màn hình danh sách sinh viên của lớp sẽ hiện ra, tuy nhiên dữ liệu ĐIỂM đã được mã hóa và không thể nhìn thấy.

FormDSSinhVien

## DANH SÁCH SINH VIÊN

**MÃ LỚP:**  **MÃ NV:**

**MÃ SV:**  **HỌ TÊN:**

	MÃ SV	HỌ TÊN	MÃ HP	TÊN HP	ĐIỂM
▶	21120419	VU THÀNH CÔNG	BMCS DL	DATABASE SECURITY	Byte...
	21120419	VU THÀNH CÔNG	QH TT	QUY HOACH TUYEN TINH	Byte...
*					

BACK
EDIT
XEM ĐIỂM
NHẬP ĐIỂM
EXIT

*Danh sách SV của GV có mã NV12 quản lý*

Trong màn hình này, ngoài 2 button BACK để quay lại trang trước, và EXIT để thoát khỏi chương trình, thì còn 3 button đáng lưu ý như sau:

- Button *EDIT*: dùng để thay đổi thông tin của sinh viên lớp đó

Trước hết nhấn vào dòng thông tin mà bạn muốn thay đổi, sau đó thay đổi các thông tin ở các thanh textbox phía trên.

Sau đó, nhấn vào button EDIT và ta được như sau:

FormDSSinhVien

## DANH SÁCH SINH VIÊN

**MÃ LỚP:** CNTT-K21 **MÃ NV:** NV12

**MÃ SV:** 21120419 **HỌ TÊN:** VU THÀNH CÔNG

	MÃ SV	HỌ TÊN	MÃ HP	TÊN HP	ĐIỂM
▶	21120419	VU THÀNH CÔNG	BMCS DL	DATABASE SECURITY	Byte...
	21120419	VU THÀNH CÔNG	QHTT	QUY HOACH TUYEN TINH	Byte...
*					

*Thông tin trước khi thay đổi*

FormDSSinhVien

## DANH SÁCH SINH VIÊN

**MÃ LỚP:** CNTT-K21 **MÃ NV:** NV12

**MÃ SV:** 21120419 **HỌ TÊN:** VU THÀNH THANH CÔNG

	MÃ SV	HỌ TÊN	MÃ HP	TÊN HP	ĐIỂM
▶	21120419	VU THÀNH THANH...	BMCS DL	DATABASE SECURITY	Byte...
	21120419	VU THÀNH THANH...	QHTT	QUY HOACH TUYEN TINH	Byte...
*					

*Thông tin sau khi đã thay đổi*

- *Button XEM ĐIỂM*: dùng để hiển thị cột điểm đã bị mã hóa  
Nhấn vào button XEM ĐIỂM và ta có kết quả trả về là cột điểm đã được giải mã.

FormDSSinhVien

## DANH SÁCH SINH VIÊN

**MÃ LỚP:** CNTT-K21 **MÃ NV:** NV12

**MÃ SV:**  **HỌ TÊN:**

	MÃ SV	HỌ TÊN	MÃ HP	TÊN HP	ĐIỂM
▶	21120419	VU THÀNH THANH...	BMCSDL	DATABASE SECURITY	8
	21120419	VU THÀNH THANH...	QHTT	QUY HOẠCH TUYỂN TÍNH	8
•					

*Điểm thi sau khi giải mã*

- *Button NHẬP ĐIỂM*: dùng để nhập điểm cho sinh viên trong lớp, sau khi nhấn button này sẽ chuyển qua màn hình nhập điểm (mục VI)

## 2. Với lớp không thuộc quyền quản lý của GV đã đăng nhập

Với thông tin đăng nhập của nhân viên có mã NV12, ta chọn lớp của nhân viên có mã NV11 để thực hiện.

Khi đó, màn hình chứa danh sách sinh viên của lớp vẫn hiện ra, tuy nhiên cột điểm đã bị mã hóa.

FormDSLop

## DANH SÁCH LỚP HỌC

**MÃ LỚP:** CNSH-K21

	MÃ LỚP	TÊN LỚP	MÃ NV
▶	CNSH-K21	CÔNG NGHỆ SINH HỌC KHÓA 21	NV11
	CNTT-K21	CÔNG NGHỆ THÔNG TIN KHÓA 21	NV12
	CNTT-K35	CÔNG NGHỆ THÔNG TIN KHÓA 35	NV12
	CNTT-K46	CÔNG NGHỆ THÔNG TIN KHÓA 46	NV12
*			

BACK
DS SINH VIÊN
EXIT

*Chọn lớp cần xem điểm*

FormDSSinhVien

## DANH SÁCH SINH VIÊN

**MÃ LỚP:** CNSH-K21      **MÃ NV:** NV11

**MÃ SV:**       **HỌ TÊN:**

	MÃ SV	HỌ TÊN	MÃ HP	TÊN HP	ĐIỂM
▶	21180888	ANTONIA PORSIL	SHGP	SINH HOC GIAI PHAU	Byte...
*					

BACK
EDIT
XEM ĐIỂM
NHẬP ĐIỂM
EXIT

*Màn hình danh sách sinh viên*

Thế nhưng, do không thuộc quyền quản lý của GV này, nên 3 button EDIT, XEM ĐIỂM và NHẬP ĐIỂM đều không thể thực hiện

**DANH SÁCH SINH VIÊN**

**MÃ LỚP:** CNSH-K21 **MÃ NV:** NV11

**MÃ SV:** 21180888 **HỌ TÊN:** ANTONIA PORSIL

	MÃ SV	HỌ TÊN	MÃ HP	TÊN HP	ĐIỂM
▶	21180888	ANTONIA PORSIL	SHGP	SINH HOC GIAI PHAU	Byte...
*					

Khong thuoc quyen quan ly cua GV !!!

OK

BACK EDIT XEM ĐIỂM NHẬP ĐIỂM EXIT

*Không thể EDIT*

FormDSSinhVien

## DANH SÁCH SINH VIÊN

**MÃ LỚP:** CNSH-K21 **MÃ NV:** NV11

**MÃ SV:** 21180888 **HỌ TÊN:** ANTONIA PORSIL

	MÃ SV	HỌ TÊN	MÃ HP	TÊN HP	ĐIỂM
▶	21180888	ANTONIA PORSIL	SHGP	SINH HOC GIAI PHAU	Byte...
*					

Không thuộc quyền quản lý của GV !!!

OK

BACKEDITXEM ĐIỂMNHẬP ĐIỂMEXIT

*Không thể XEM ĐIỂM*

FormDSSinhVien

## DANH SÁCH SINH VIÊN

**MÃ LỚP:** CNSH-K21 **MÃ NV:** NV11

**MÃ SV:** 21180888 **HỌ TÊN:** ANTONIA PORSIL

	MÃ SV	HỌ TÊN	MÃ HP	TÊN HP	ĐIỂM
▶	21180888	ANTONIA PORSIL	SHGP	SINH HOC GIAI PHAU	Byte...
*					

Không thuộc quyền GV quản lý !!!

OK

BACKEDITXEM ĐIỂMNHẬP ĐIỂMEXIT

*Không thể NHẬP ĐIỂM*



## VI. Màn hình nhập bảng điểm

Với GV có quyền nhập điểm, thì chương trình sẽ chuyển qua màn hình nhập điểm cho lớp học đó:

**NhapDiemSV**

**NHẬP ĐIỂM**

Mã lớp: CNTT-K21

Điểm: System.Byte[]

	MÃ SV	MÃ HP	ĐIỂM
	21120419	BMCS DL	System.Byte[]
▶	21120419	QHTT	System.Byte[]
*			

BACK INSERT EXIT

Màn hình nhập điểm

Chọn dòng cần nhập điểm, sau đó nhập điểm của môn học cần nhập

**NhapDiemSV**

**NHẬP ĐIỂM**

Mã lớp: CNTT-K21

Điểm: 10

	MÃ SV	MÃ HP	ĐIỂM
▶	21120419	BMCS DL	System.Byte[]
	21120419	QHTT	System.Byte[]
*			

BACK INSERT EXIT

Nhập điểm

The screenshot shows the 'NhapDiemSV' application window. At the top, it says 'NHẬP ĐIỂM' and 'Mã lớp: CNTT-K21'. Below this, there is a 'Điểm:' label and a text box containing '10'. A table with 4 columns (MÃ SV, MÃ HP, ĐIỂM) is visible. The first row has '21120419' in the first column, 'BMCSDL' in the second column, and 'System.Byte[]' in the third column. The second row has '21120419' in the first column, 'QHTT' in the second column, and 'System.Byte[]' in the third column. A confirmation dialog box is open in the foreground with the text 'Nhap diem thanh cong !!!' and an 'OK' button. At the bottom of the application window, there are three buttons: 'BACK', 'INSERT', and 'EXIT'.

	MÃ SV	MÃ HP	ĐIỂM
▶	21120419	BMCSDL	System.Byte[]
	21120419	QHTT	System.Byte[]
*			

*Nhập điểm thành công*

Sau khi nhập điểm xong, thông tin “Nhap diem thanh cong” sẽ được hiện ra thông báo bạn đã nhập điểm thành công.

The screenshot shows the 'NhapDiemSV' application window after the grade entry process. The 'Điểm:' text box still contains '10'. The table is the same as in the previous screenshot. The confirmation dialog box is no longer present. At the bottom of the application window, there are three buttons: 'BACK', 'INSERT', and 'EXIT'.

	MÃ SV	MÃ HP	ĐIỂM
▶	21120419	BMCSDL	System.Byte[]
	21120419	QHTT	System.Byte[]
*			

*Màn hình sau khi nhập điểm xong*

Tuy vậy, màn hình vẫn hiển thị cột điểm trong trạng thái đã bị encrypt. Để decrypt, có thể chọn BACK để quay trở lại màn hình DANH SÁCH SINH VIÊN và thực hiện chọn XEM ĐIỂM

**DANH SÁCH SINH VIÊN**

**MÃ LỚP:** CNTT-K21 **MÃ NV:** NV12

**MÃ SV:**  **HỌ TÊN:**

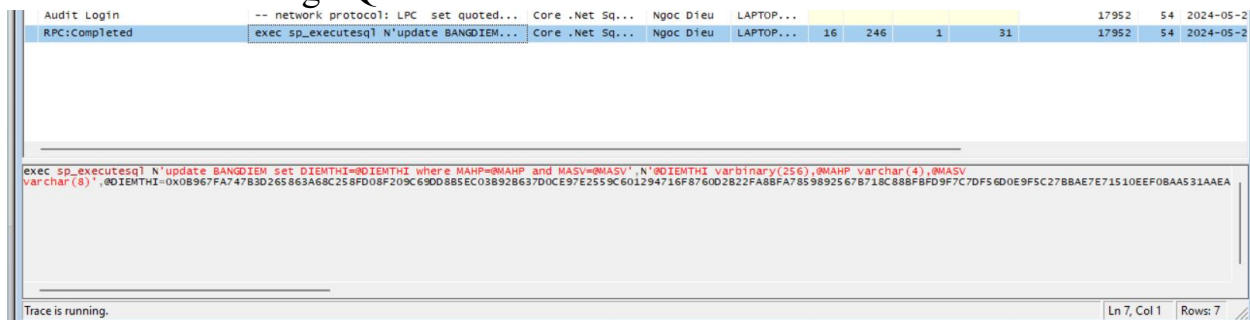
MÃ SV	HỌ TÊN	MÃ HP	TÊN HP	ĐIỂM
21120419	VU THÀNH THANH...	BMCS DL	DATABASE SECURITY	10
21120419	VU THÀNH THANH...	QHTT	QUY HOẠCH TUYỂN TINH	8

**BACK** **EDIT** **XEM ĐIỂM** **NHẬP ĐIỂM** **EXIT**

*Điểm 8 đã được update thành 10*

## VII. Theo dõi thao tác nhập điểm bằng SQL Profile

- Thao tác trong SQL Profile:



- Nhận xét:

- Các giá trị điểm đã được mã hóa bằng thuật toán RSA2048 trên Client, sau đó mới truyền giá trị xuống Database
- Điều này đảm bảo tính riêng tư và bảo mật vì ngoài chính bản thân thì bên trung gian hay là kẻ tấn công, và cả người quản lý Database (người

có quyền truy xuất SQL Profile) cũng không có khóa bí mật để có thể giải mã nội dung (điểm).

- Vì vậy dữ liệu được bảo mật tuyệt đối.
- Việc mã hóa ở Client rất phù hợp trong việc chia sẻ các gói tin bí mật hoặc lưu dữ liệu vào Cloud, cơ sở dữ liệu, ... mà phải truyền qua đường kết nối public.