



FIT@HCMUS

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



LAB 3 - MÃ HÓA DỮ LIỆU SỬ DỤNG CÁC THUẬT TOÁN MÃ HÓA ĐỐI XỨNG

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 4/2024

Mục lục

I. Các stored procedure (câu c).....	2
1. Stored procedure SP_INS_PUBLIC_NHANVIEN.....	2
a. Cài đặt.....	2
b. Thực thi.....	2
2. Stored procedure SP_SEL_PUBLIC_NHANVIEN.....	2
a. Cài đặt.....	2
b. Thực thi.....	2
II. Màn hình quản lý đăng nhập	3
III. Màn hình quản lý lớp học.....	3
IV. Màn hình sinh viên của từng lớp	4
V. Nhập điểm cho từng sinh viên	6
VI. Sử dụng SQL Profile theo dõi thao tác màn hình nhập điểm.....	8
1. Đăng nhập.....	8
2. Nhận xét.....	9

I. Các stored procedure (câu c)

1. Stored procedure SP_INS_PUBLIC_NHANVIEN

a. Cài đặt

```

89 GO
90 CREATE PROCEDURE SP_INS_PUBLIC_NHANVIEN @MANV VARCHAR(20), @HOTEN NVARCHAR(100),
91     @EMAIL VARCHAR(20), @LUONG INT,
92     @TENDN NVARCHAR(100), @MATKHAU VARCHAR(32)
93 AS
94 BEGIN
95     DECLARE @PUBKEY VARCHAR(20)
96     SET @PUBKEY = @MANV
97
98     DECLARE @AKEY NVARCHAR(MAX)
99     SET @AKEY = 'CREATE ASYMMETRIC KEY '+@MANV+' WITH ALGORITHM = RSA_2048 ENCRYPTION BY PASSWORD = '''+@MATKHAU+''''
100     EXEC(@AKEY)
101     INSERT INTO NHANVIEN(MANV, HOTEN, EMAIL, LUONG, TENDN, MATKHAU, PUBKEY)
102     VALUES (@MANV, @HOTEN, @EMAIL,
103         ENCRYPTBYASYMKEY(ASYMKEY_ID(@PUBKEY), CONVERT(VARBINARY(MAX), @LUONG)),
104         @TENDN, CONVERT(VARBINARY, HASHBYTES('SHA1', @MATKHAU)),
105         @PUBKEY)
106 END
107

```

b. Thực thi

108
109 EXEC SP_INS_PUBLIC_NHANVIEN 'NV04', N'NGUYEN VAN A', 'NVd@', 3000000, 'NV04', 'abcd12'

132 %
Messages
(1 row affected)

108
109 EXEC SP_INS_PUBLIC_NHANVIEN 'NV04', N'NGUYEN VAN A', 'NVd@', 3000000, 'NV04', 'abcd12'

110
111 SELECT* FROM NHANVIEN
112
113 --ii)

109 %
Results Messages

	MANV	HOTEN	EMAIL	LUONG	TENDN	MATKHAU	PUBKEY
1	NV04	NGUYEN VAN A	NVd@	0x2645323DF7AD25DA97C60DE5682EFE8E27E0246C4752930...	NV04	0xC35A37F0BCA08AFA583247CC461CAD9C8082A47C	NV04

2. Stored procedure SP_SEL_PUBLIC_NHANVIEN

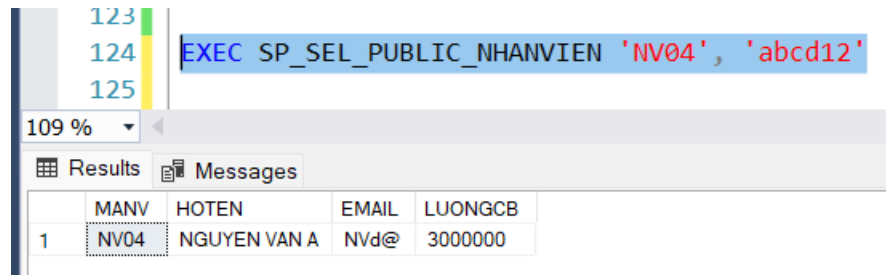
a. Cài đặt

```

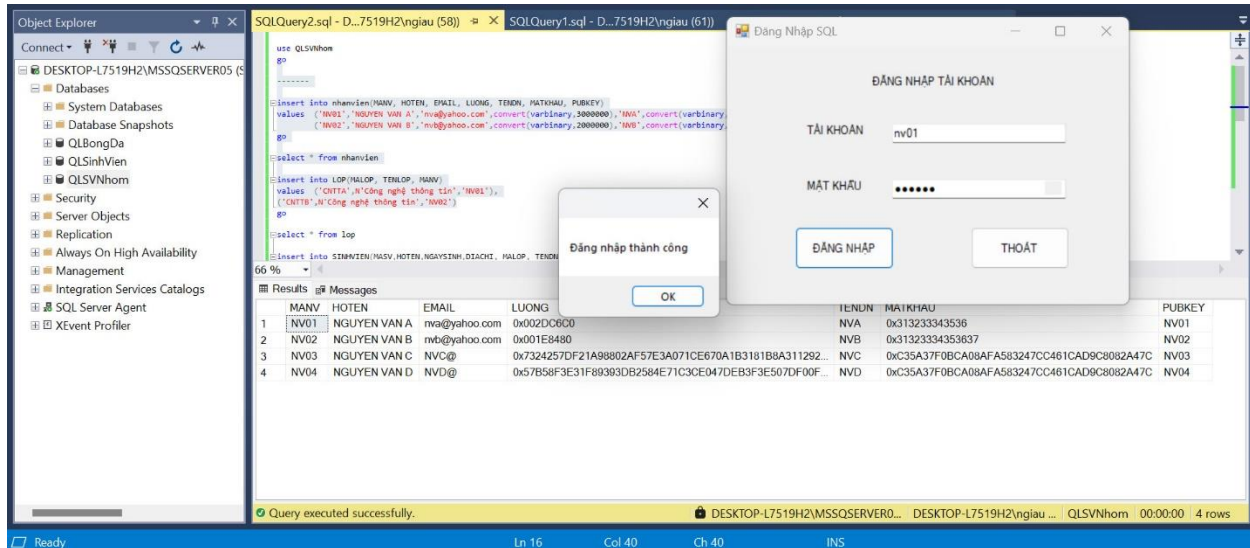
114 GO
115 CREATE PROCEDURE SP_SEL_PUBLIC_NHANVIEN @TENDN NVARCHAR(100), @MATKHAU VARCHAR(100)
116 AS
117 BEGIN
118     SELECT MANV, HOTEN, EMAIL,
119         LUONGCB = CONVERT(INT, DECRYPTBYASYMKEY(ASYMKEY_ID(MANV), LUONG, CONVERT(NVARCHAR, @MATKHAU)))
120     FROM NHANVIEN
121     WHERE CONVERT(NVARCHAR, @TENDN) = TENDN AND MATKHAU = HASHBYTES('SHA1', @MATKHAU)
122 END

```

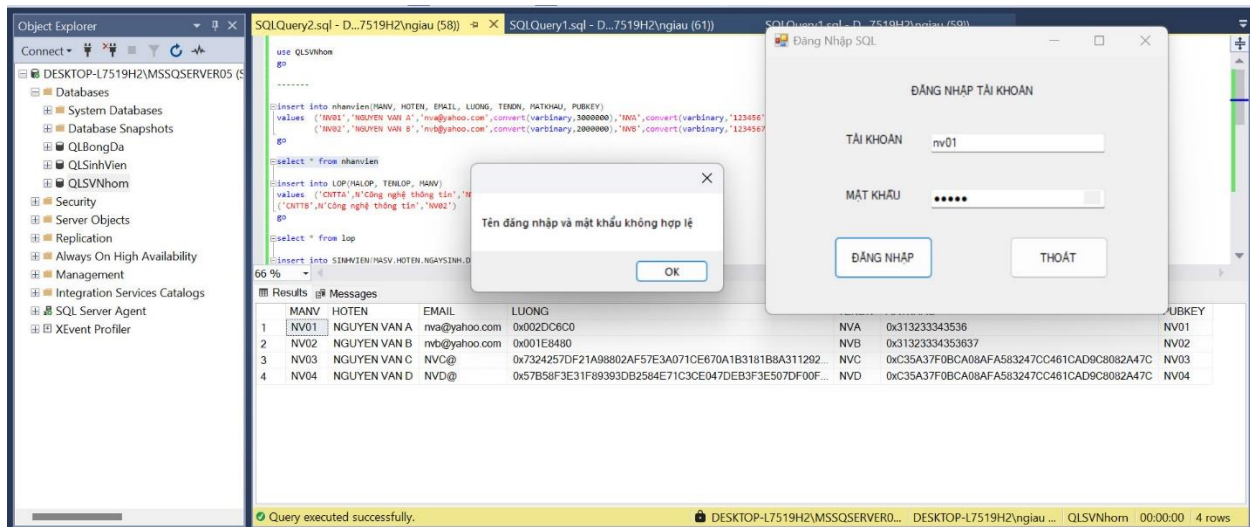
b. Thực thi



II. Màn hình quản lý đăng nhập



Đăng nhập thành công



Đăng nhập không thành công

III. Màn hình quản lý lớp học

The screenshot shows a web application window titled "FormThaoTac". It contains a form for adding or editing student information. The form fields are: Mã Sinh Viên, Họ Tên, Ngày Sinh, Mã Lớp, Tên Đăng Nhập, and Mật Khẩu. There are buttons for "Thêm", "Sửa", and "Xoá". Below the form is a table with columns: Mã SV, Họ Tên, Ngày Sinh, Địa Chỉ, and Mã Lớp. The table contains two rows of data.

Mã SV	Họ Tên	Ngày Sinh	Địa Chỉ	Mã Lớp
21120396	Đào Thị Ngọc Giàu	1/1/1999	HCM	CNTTA
21120419	Vũ Thành Công	9/3/2003	LAM DONG	CNTTA

Sau khi đăng nhập, nhân viên chỉ có thể theo dõi những sinh viên thuộc mã lớp do nhân viên quản lý.

IV. Màn hình sinh viên của từng lớp

The screenshot shows the same web application window "FormThaoTac" but with different data entered in the form fields. The form fields are: Mã Sinh Viên, Họ Tên, Ngày Sinh, Mã Lớp, Tên Đăng Nhập, and Mật Khẩu. There are buttons for "Thêm", "Sửa", and "Xoá". Below the form is a table with columns: Mã SV, Họ Tên, Ngày Sinh, Địa Chỉ, and Mã Lớp. The table contains three rows of data.

Mã SV	Họ Tên	Ngày Sinh	Địa Chỉ	Mã Lớp
21120396	Đào Thị Ngọc Giàu	1/1/1999	HCM	CNTTA
21120419	Vũ Thành Công	9/3/2003	LAM DONG	CNTTA
21120446	Kiên Định Mỹ Hạnh	4/27/2003	Trà Vinh	CNTTA

Thêm sinh viên

The screenshot shows the 'FormThaoTac' application window. It contains a form for adding, editing, or deleting a student record. The form fields are: Mã Sinh Viên (21120446), Địa Chỉ (Trà Vinh), Họ Tên (Kiên Đình Mỹ Hạnh), Ngày Sinh (27/04/2003), Mã Lớp (CNTTA), Tên Đăng Nhập (nv01), and Mật Khẩu (masked). Below the form is a table of student records. A confirmation dialog box titled 'Cảnh báo' (Warning) is displayed over the table, asking 'Bạn có muốn xóa hay không?' (Do you want to delete or not?). The dialog has 'Yes' and 'No' buttons.

Mã SV	Họ Tên	Mã Lớp
21120396	Đào Thị Ngọc Giàu	CNTTA
21120419	Vũ Thành Công	CNTTA
21120446	Kiên Đình Mỹ Hạnh	CNTTA

Xóa một sinh viên

The screenshot shows the 'FormThaoTac' application window with the search functionality. The search bar is labeled 'Tìm kiếm với Mã Sinh Viên, Họ Tên hoặc Mã Lớp' (Search by Student ID, Name, or Class Code). The search results table shows the following data:

Mã SV	Họ Tên	Ngày Sinh	Địa Chỉ	Mã Lớp
21120396	Đào Thị Ngọc Giàu	1/1/1999	HCM	CNTTA

Tìm kiếm thông tin một sinh viên

Nhân viên quản lý sinh viên của một lớp có các quyền thêm, xóa, sửa, hoặc tìm kiếm bất kỳ một sinh viên nào.

V. Nhập điểm cho từng sinh viên

Bước 1: Chọn sinh viên cần nhập điểm bằng cách nhấn vào phần sửa.

The screenshot shows a window titled "FormThaoTac" with the following fields and controls:

- Mã Sinh Viên: 21120419
- Họ Tên: Vũ Thành Công
- Ngày Sinh: 03/09/2003
- Mã Lớp: CNTT
- Tên Đăng Nhập: NV01
- Mật Khẩu: •••••
- Địa Chỉ: Đồng Tháp
- Buttons: Thêm, Sửa (highlighted), Xóa
- Search: Tìm kiếm với Mã Sinh Viên, Họ Tên hoặc Mã Lớp

Below the form is a table with the following data:

	Mã SV	Họ Tên	Ngày Sinh	Địa Chỉ	Mã Lớp
▶	21120396	Đào Thị Ngọc Giàu	1/1/1999	HCM	CNTTA
	21120419	Vũ Thành Công	9/3/2003	Đồng Tháp	CNTTA
	21120446	Kiên Đình Mỹ Hạnh	4/27/2003	Trà Vinh	CNTTA
•					

Bước 2: Màn hình giao diện thông tin sinh viên cần nhập điểm sẽ được hiện lên

The screenshot shows a Windows application window titled "FormSuaDiem". On the left is a form with the following fields: "Mã Sinh Viên:" with value "21120396", "Họ Tên:" with value "Đào Thị Ngọc Giàu", "Mã HP:" with value "CTDL", and "Điểm:" with an empty text box. Below these are three buttons: "Thêm", "Xoá", and "Sửa". On the right is a table with two columns: "Học Phần" and "Điểm Thi". The first row has "CTDL" under "Học Phần" and "Byte[] Array" under "Điểm Thi". A second row is partially visible with an asterisk in the first column.

	Học Phần	Điểm Thi
▶	CTDL	Byte[] Array
*		

Giao diện nhập điểm

Bước 3: Thao tác với điểm số: Có thể xóa điểm đó đi, hoặc nhập thêm điểm vào

This screenshot shows the same "FormSuaDiem" window as before, but with a modal dialog box in the foreground. The dialog box is titled "Cảnh báo" (Warning) and contains a yellow warning icon and the text "Bạn có muốn xoá hay không?" (Do you want to delete or not?). At the bottom of the dialog are two buttons: "Yes" and "No". In the background, the "Xoá" button on the main form is highlighted with a blue border.

Xóa điểm

Học Phần	Điểm Thi
CTDL	Byte[] Array
KTLT	Byte[] Array

Nhập điểm

Do ngay từ đầu, nhóm em đã xây dựng app theo cách đăng nhập của nhân viên và chỉ có nhân viên có thể đăng nhập. Và đồng thời, nhân viên chỉ có thể nhìn thấy lớp mà mình quản lý, do đó không thể sửa đổi điểm của lớp khác.

VI. Sử dụng SQL Profile theo dõi thao tác màn hình nhập điểm

1. Đăng nhập

2. Nhận xét

- Trong bài này, người dùng SQL Profiler nhận thấy nhân viên chỉ chỉnh sửa được điểm của sinh viên thuộc lớp do nhân viên đó quản lý.
- Người có quyền truy cập tới tool SQL Profiler hoặc nghe trộm liên lạc giữa ứng dụng và Database hoàn toàn có thể biết được mật khẩu người lần điểm số đã nhập.
- Do đó, thông tin điểm số sẽ bị lộ