**BẢO MẬT CƠ SỞ DỮ LIỆU**

**Lab04 – Nhóm**

**Mã hóa dữ liệu từ client trước khi lưu xuống CSDL**

**Giải mã dữ liệu ở client sau khi truy vấn dữ liệu từ CSDL**

Sinh viên:

**Đỗ Trọng Nghĩa – 18120477**

**Vũ Trọng Nghĩa – 18120481**

**Lê Danh Lưu – 18120460**

C:\Users\tdqua_000\Dropbox\SS-Slides\DeCuong-CDIO\Template CDIO v4.2\Templates\Hinh anh\LogoTruong.png

Khoa Công nghệ Thông tin

Đại học Khoa học Tự nhiên TP HCM

[I. Tạo cơ sở dữ liệu 3](#_Toc74442146)

[I.1. Mô hình CSDL 3](#_Toc74442147)

[I.2. Các Stored Procedure chính 4](#_Toc74442148)

[II. Mã hóa dữ liệu ở phía Client 10](#_Toc74442149)

[II.1. Class RSA512 10](#_Toc74442150)

[II.2. Class MD5 12](#_Toc74442151)

[II.3. Class SHA1 13](#_Toc74442152)

[III. Sử dụng công cụ SQL Profile để theo dõi các màn hình Error! Bookmark not defined.](#_Toc74442153)

[III.1. Theo dõi màn hình đăng nhập 14](#_Toc74442154)

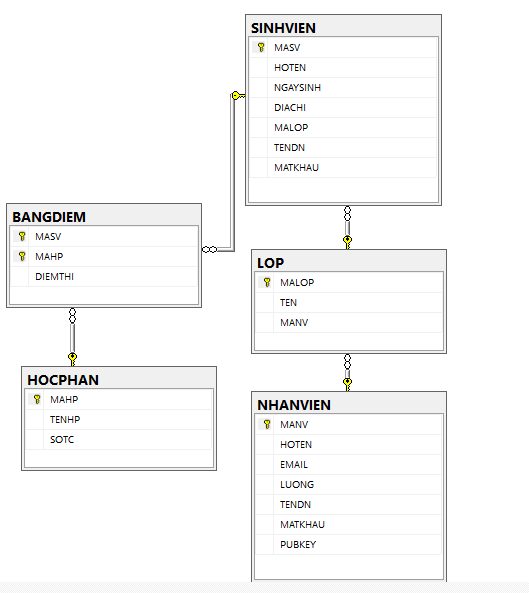
[III.2. Theo dõi màn hình load danh sách nhân viên 17](#_Toc74442155)

[III.3. Theo dõi màn hình thêm nhân viên **Error! Bookmark not defined.**](#_Toc74442156)

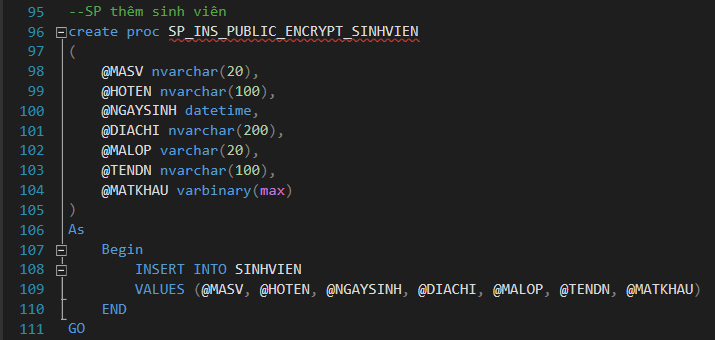
[III.4. Theo dõi thêm các thao tác xóa và chỉnh sửa nhân viên **Error! Bookmark not defined.**](#_Toc74442157)

1. Tạo cơ sở dữ liệu
   1. Mô hình CSDL

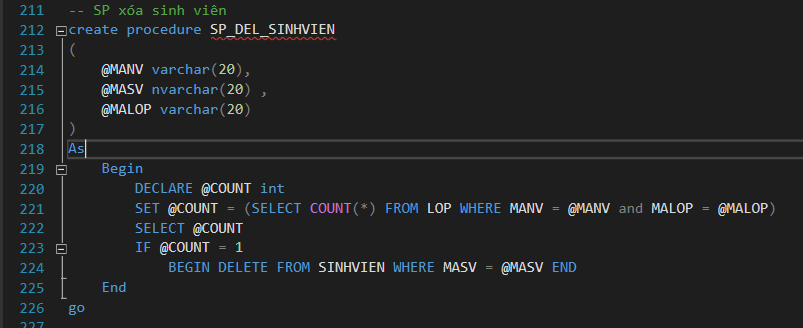
* Thiết lập CSDL có mô hình như sau



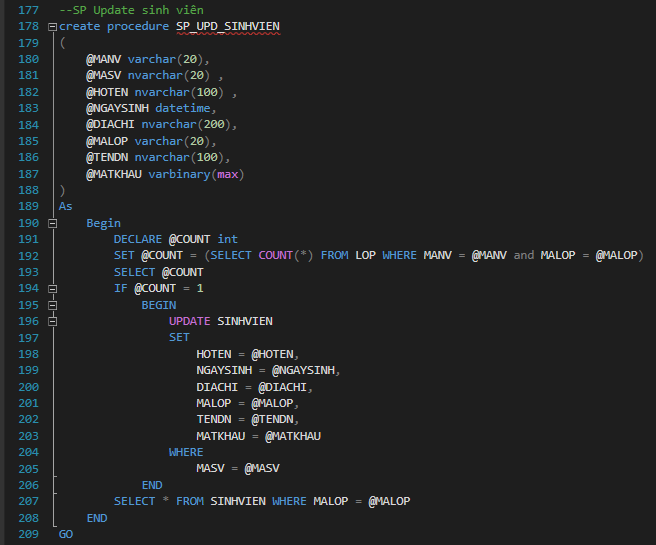
* 1. Các Stored Procedure chính
     1. SP\_INS\_PUBLIC\_ ENCRYPT \_SINHVIEN



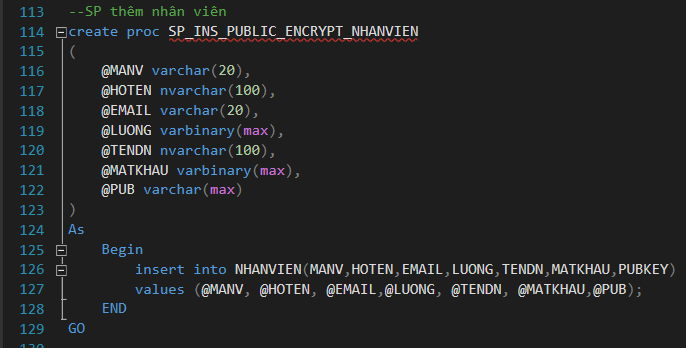
* + 1. SP\_DEL\_SINHVIEN



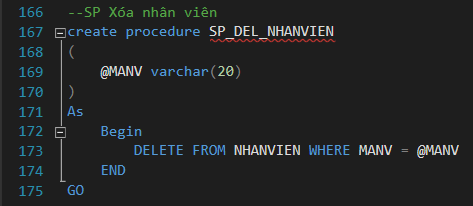
* + 1. SP\_UPD\_SINHVIEN



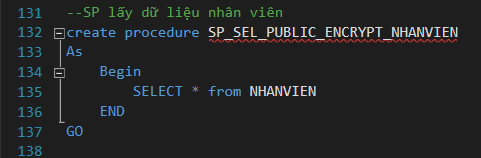
* + 1. SP\_INS\_ ENCRYPT \_NHANVIEN



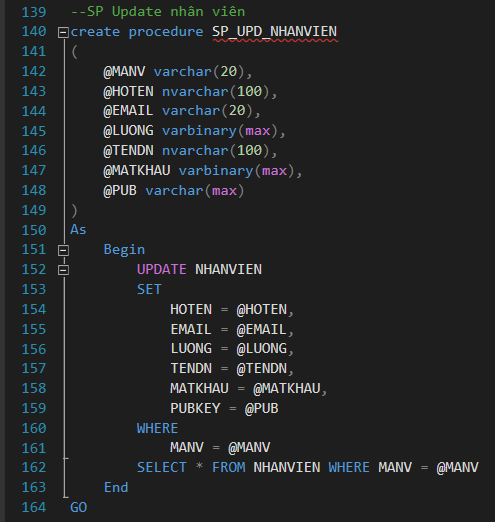
* + 1. SP\_DEL\_NHANVIEN



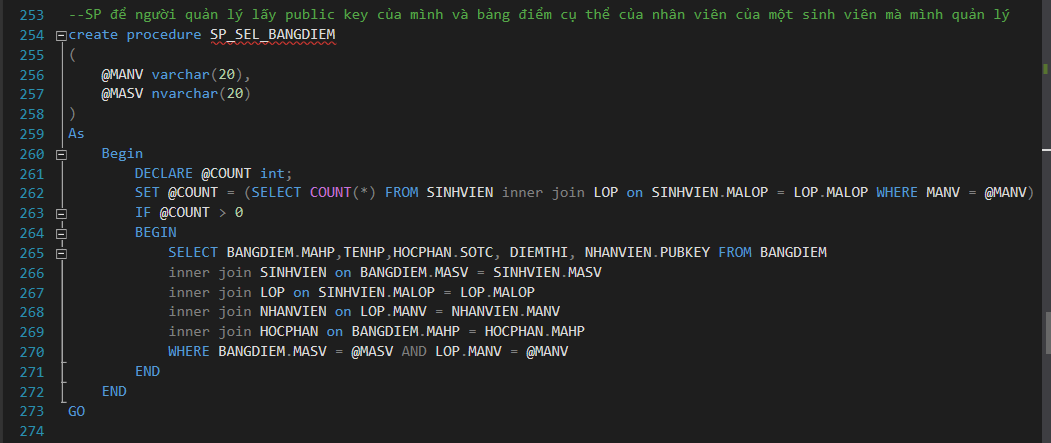
* + 1. SP\_SEL\_ ENCRYPT \_NHANVIEN



* + 1. SP\_UPD\_NHANVIEN



* + 1. SP\_SEL\_BANGDIEM



* + 1. SP\_UPD\_BANGDIEM

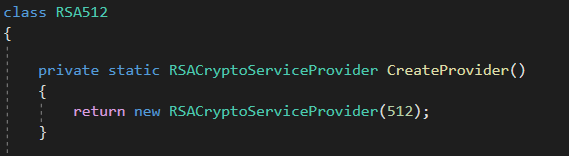


* + 1. SP\_LOG\_IN
* Với mỗi tên đăng nhập, nhận mật khẩu mã hóa dưới 2 dạng MD5 và SHA1 (cách mã hóa mật khẩu của sinh viên và nhân viên). Tiến hành select, cột đầu tiên là 1 – Nếu có tồn tại tài khoản, 0 – Nếu không tồn tại tài khoản. Cột thứ hai là 0 – Nếu là tài khoản sinh viên, mã nhân viên – Nếu là của nhân viên đó đăng nhập.

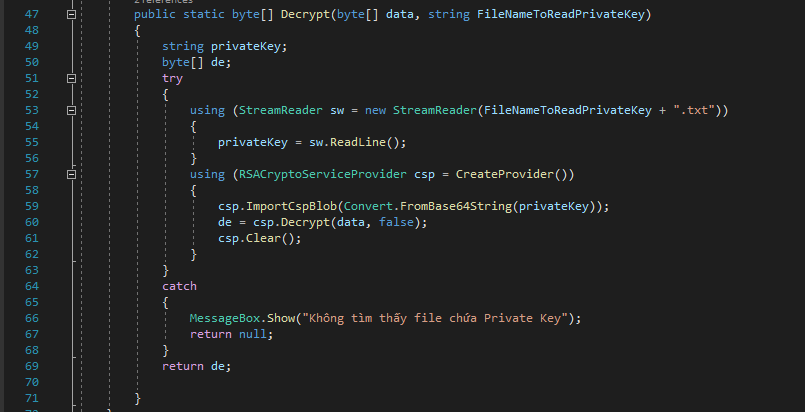


1. Mã hóa dữ liệu ở phía Client
   1. Class RSA512
      1. Thiết lập các thuộc tính

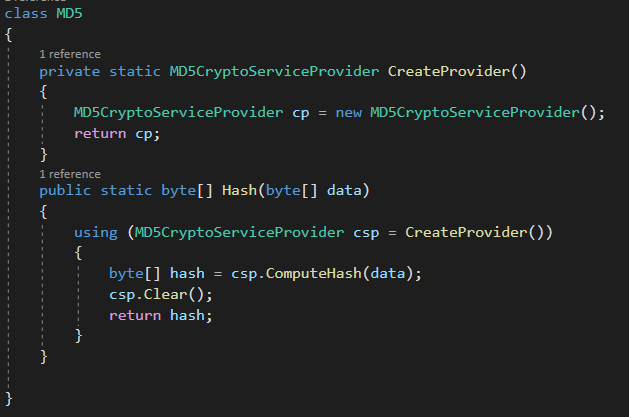
* Sử dụng thư viện **RSACryptoServiceProvider** và tạo phương thức CreateProvider() để tạo hệ mã với độ dài khóa là 512 bit. Vì vậy, việc thêm dữ liệu ban đầu cần phải mã hóa theo public key và giải mã theo private key (có các file: MaNV\_PrivateKey.txt đính kèm, trong đó MaNV là mã các nhân viên trong bảng NHANVIEN).



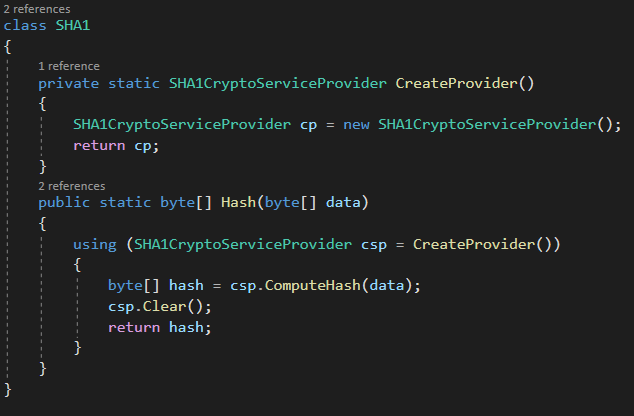
* + 1. Mã hóa
* Dựa vào phương thức CreateProvider() và sinh khóa
  + 1. Giải mã
* Dựa vào phương thức CreateProvider()



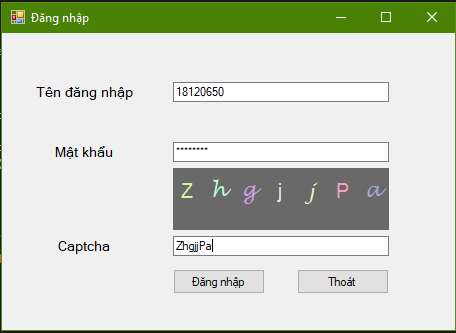
* 1. Class MD5
* Dùng để mã hóa mật khẩu của sinh viên



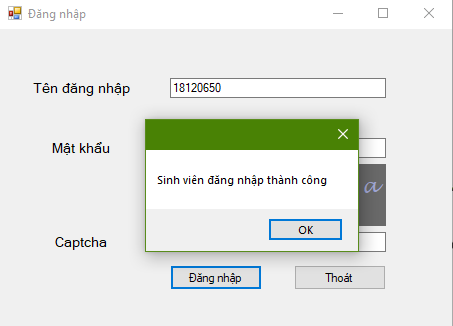
* 1. Class SHA1
* Dùng để mã hóa mật khẩu nhân viên



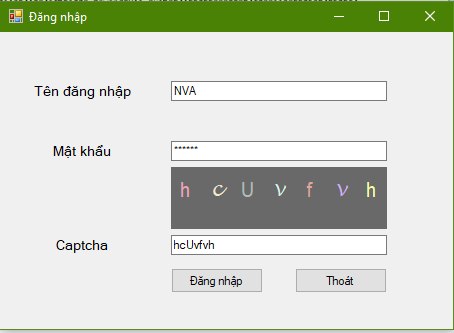
1. Các màn hình và sử dụng SQL Profile để theo dõi màn hình nhập điểm
   1. Màn hình đăng nhập
      1. Đối với tài khoản trong bảng SINHVIEN

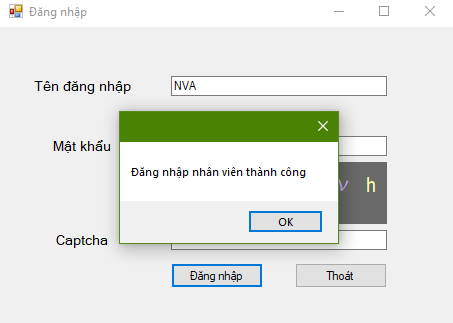


* Đối với tài khoản thuộc table SINHVIEN thì chỉ có thông báo đăng nhập thành công, không có phần xử lý đăng nhập

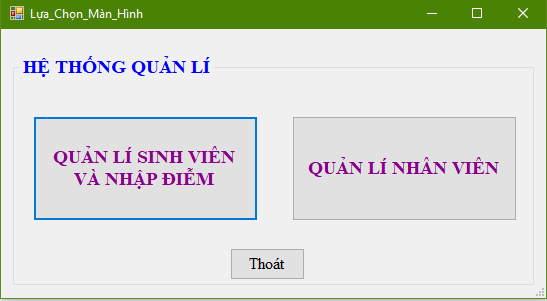


* + 1. Đối với tài khoản trong bảng NHANVIEN

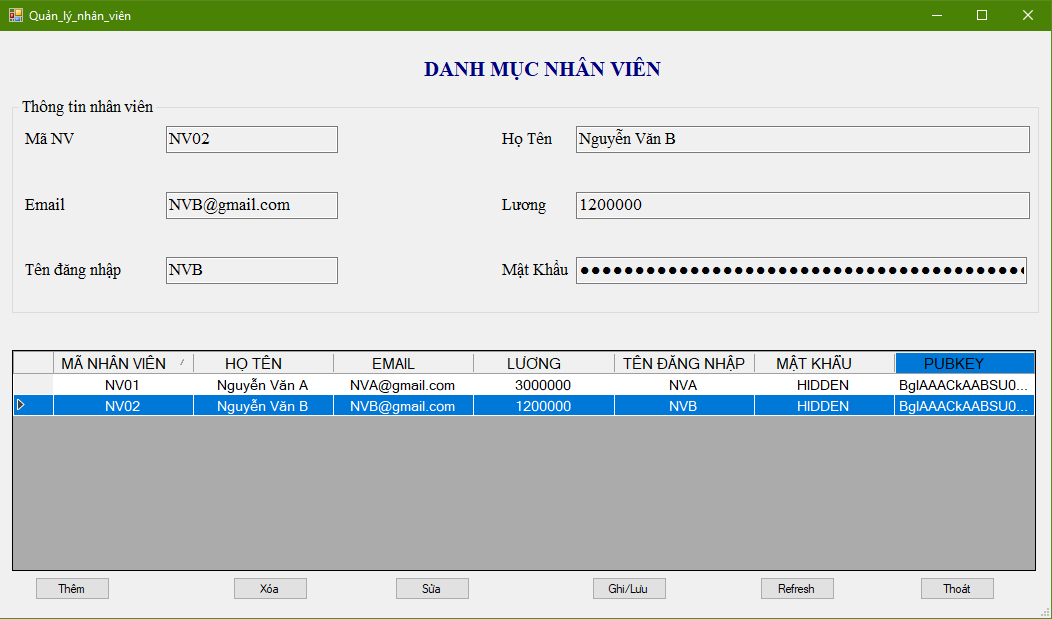




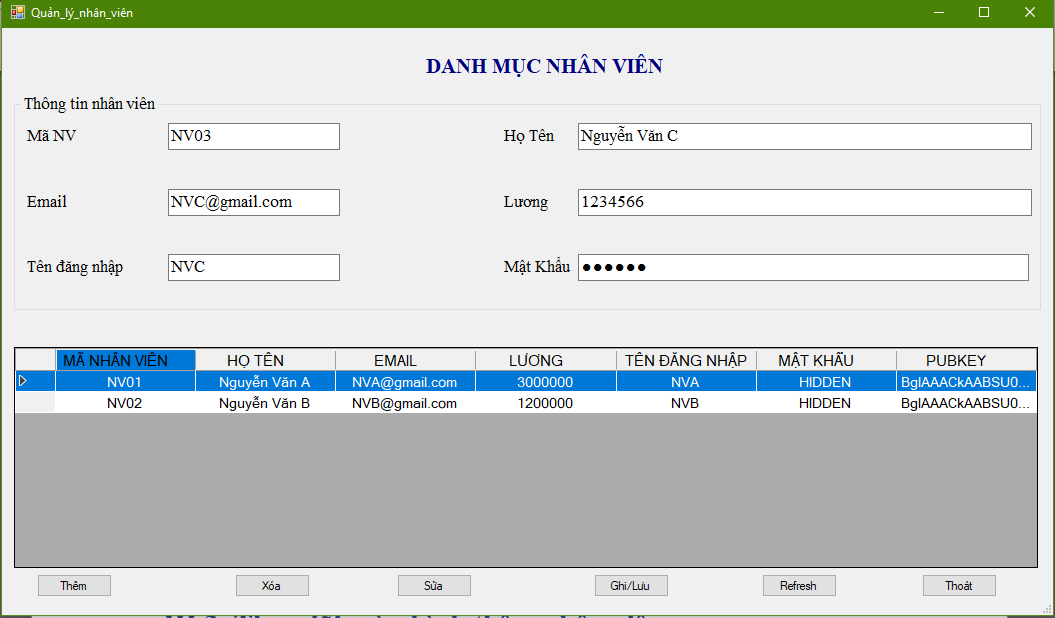
* + 1. Màn hình lựa chọn
* Sau khi đăng nhập với tài khoản nhân viên thì sẽ có màn hình lựa chọn cho người dùng quản lí nhân viên hoặc sinh viên



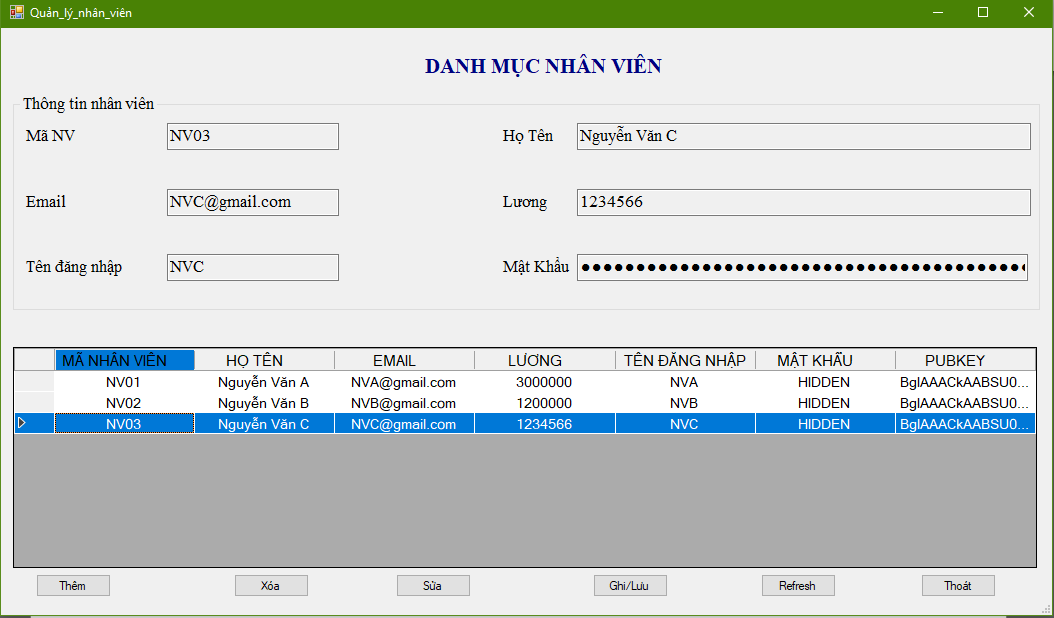
* 1. Màn hình quản lí nhân viên
     1. Thêm nhân viên
* Vì mật khẩu được mã hóa bằng SHA1, không decrypt được nên textbox mật khẩu chỉ là chuỗi hash.
* Lương của nhân viên sẽ được mã hóa bằng thuật toán RSA512 và Private Key sẽ được lưu ở file MANV\_PrivateKey.txt (trong đó MANV là mã nhân viên)



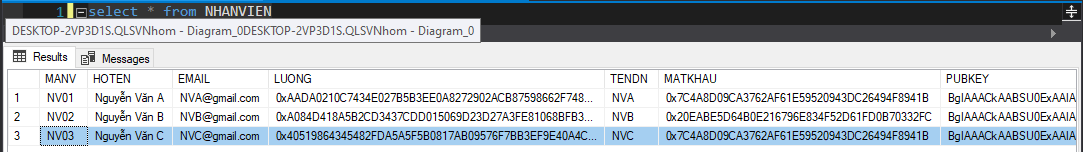
* Khi thêm nhân viên, ta cần bấm nút “Thêm” để mở khóa các textbox, sau đó nhập các thông tin vào (không được để trống các trường)



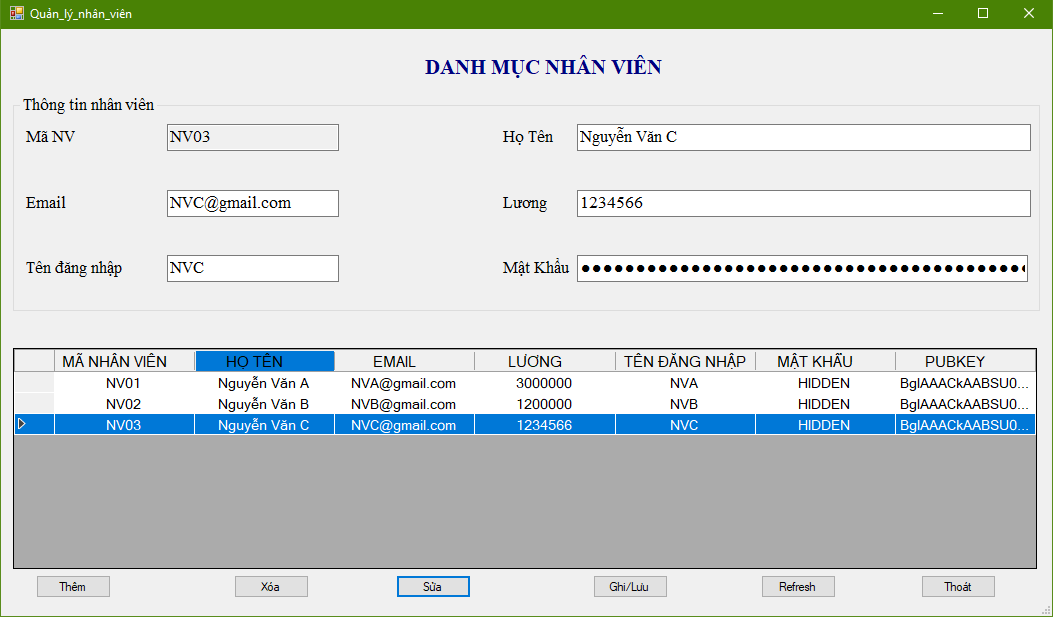
* Sau đó chọn “Ghi/Lưu” để lưu lại nhân viên



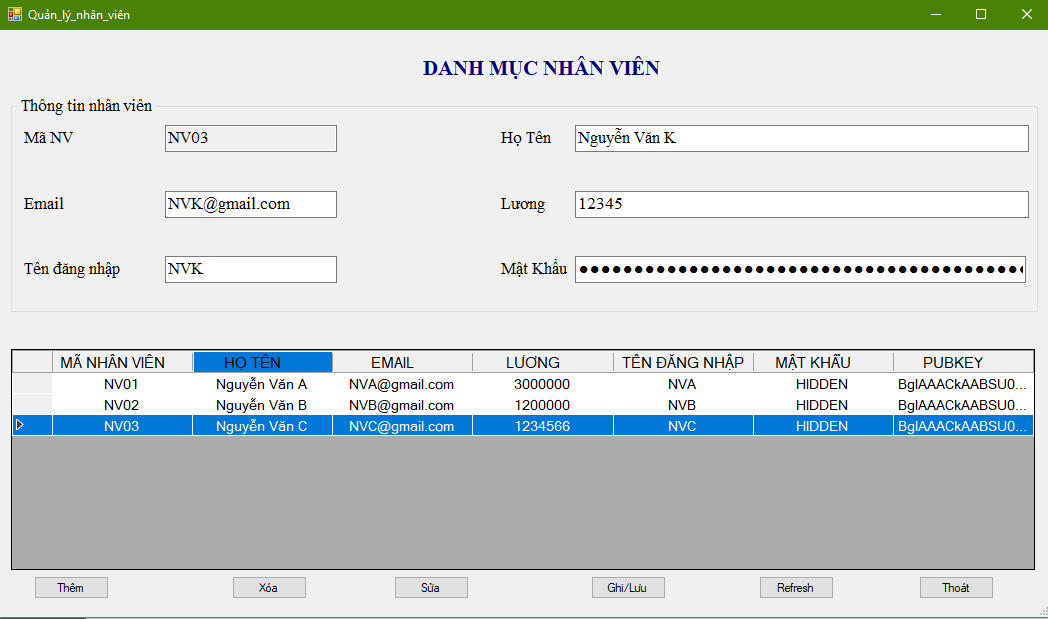
* Kiểm tra trên Database

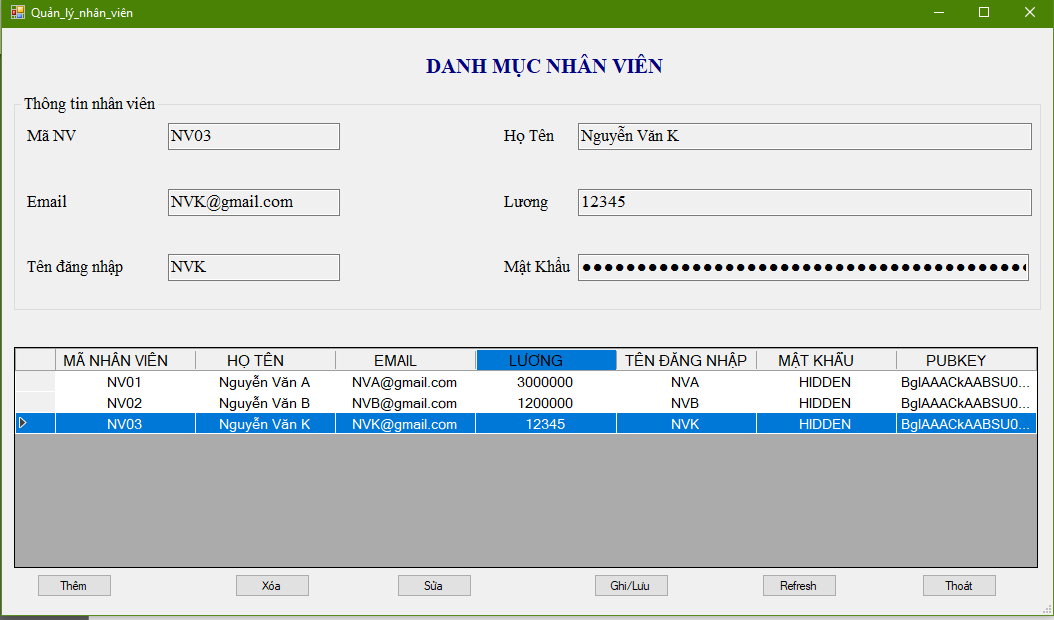


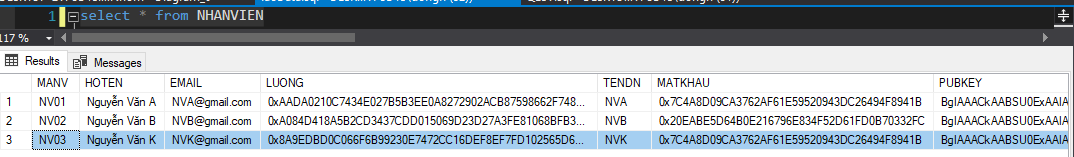
* + 1. Chỉnh sửa nhân viên
* Chọn nhân viên cần chỉnh sửa, sau đó chọn “Sửa”, trường mã nhân viên sẽ bị khóa lại vì là Primary Key

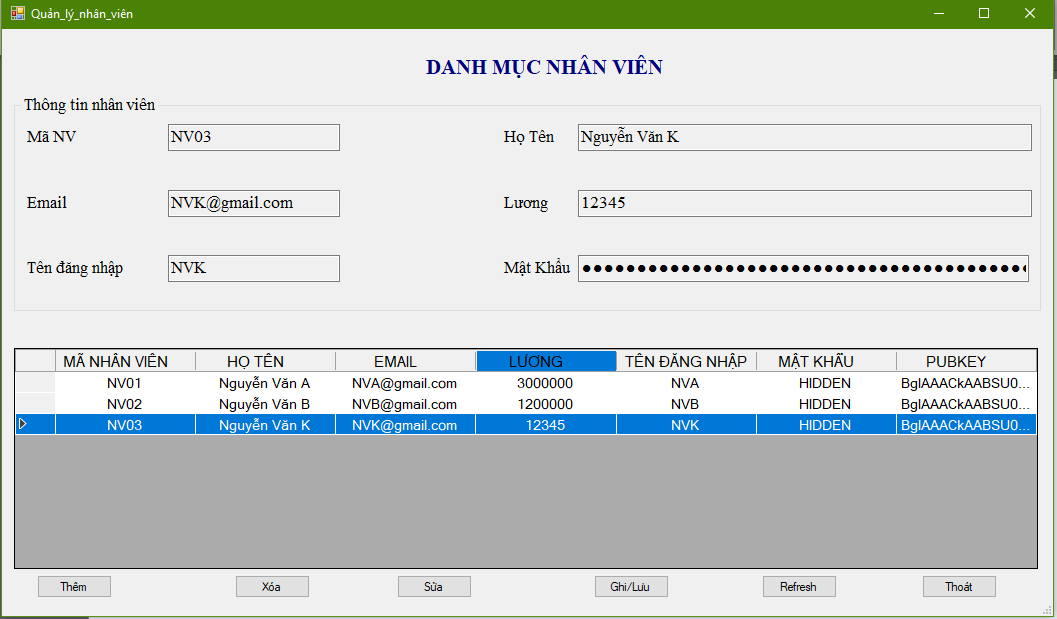


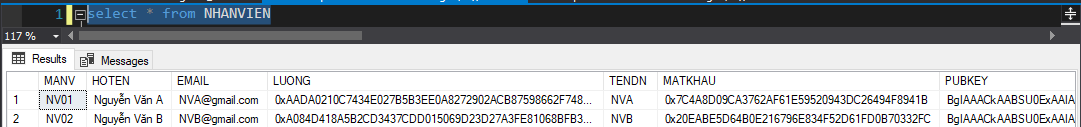
* Tiến hành sửa nhân viên, sau đó chọn “Ghi/Lưu” để lưu lại

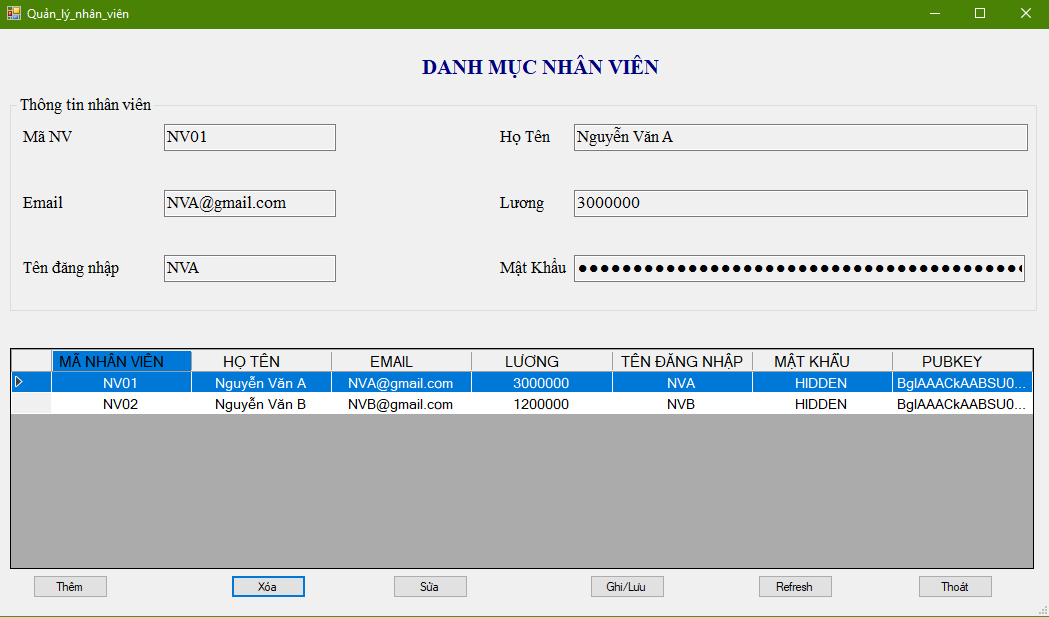




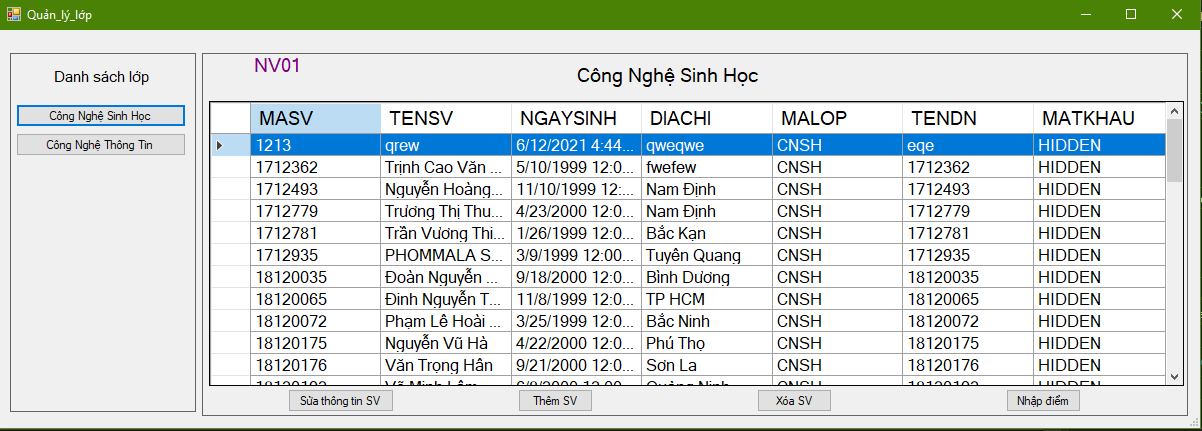
* Kiểm tra ở Database

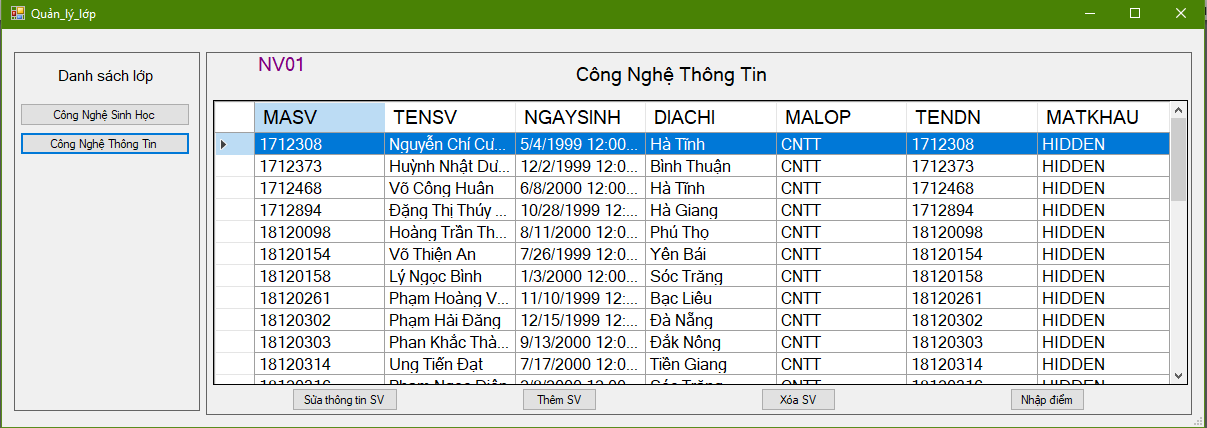
* + 1. Xóa nhân viên
* Chọn vào một nhân viên sau đó chọn “Xóa”
* Kiểm tra ở Database



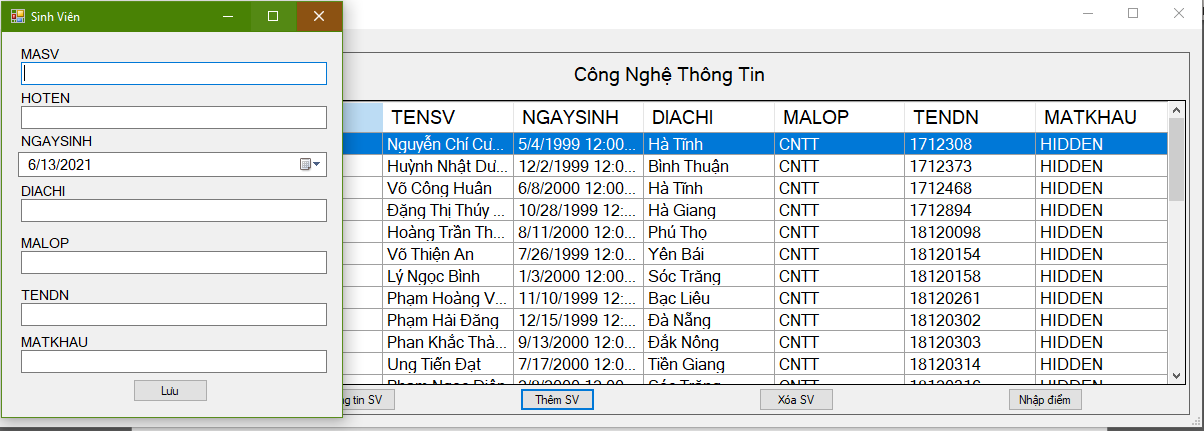


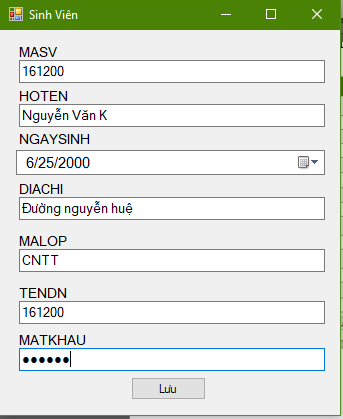
* 1. Màn hình quản lí sinh viên
* Bao gồm danh sách sinh viên của từng lớp mà người nhân viên đó quản lí



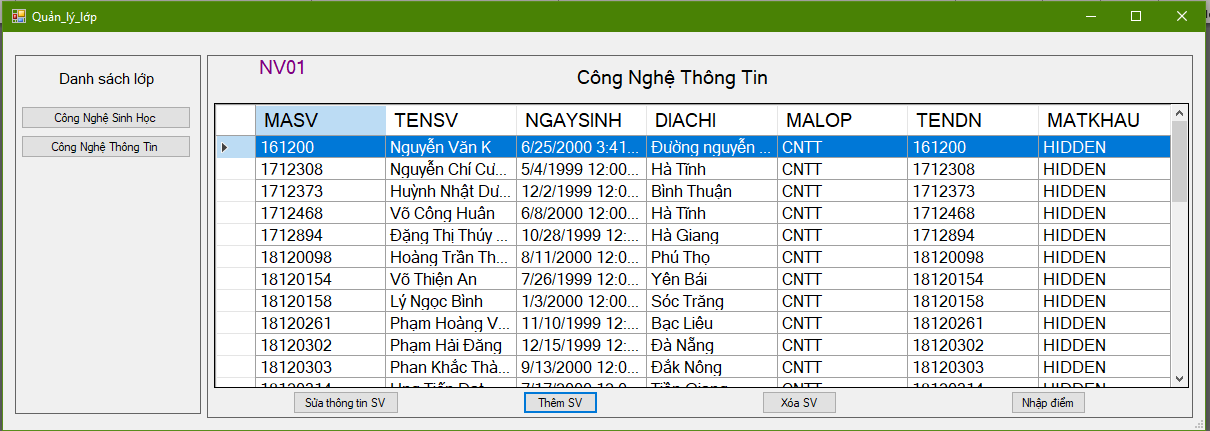


* + 1. Thêm sinh viên
* Chọn “Thêm SV”, sau đó điền vào form. Chú ý các trường không được để trống, không trùng lặp mã sinh viên và lớp phải tồn tại trong cơ sở dữ liệu

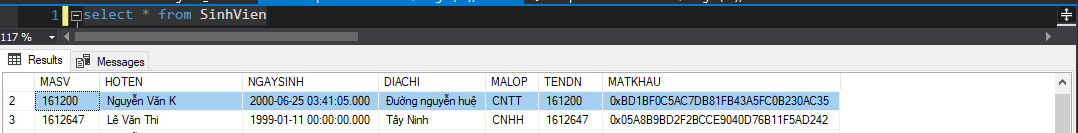




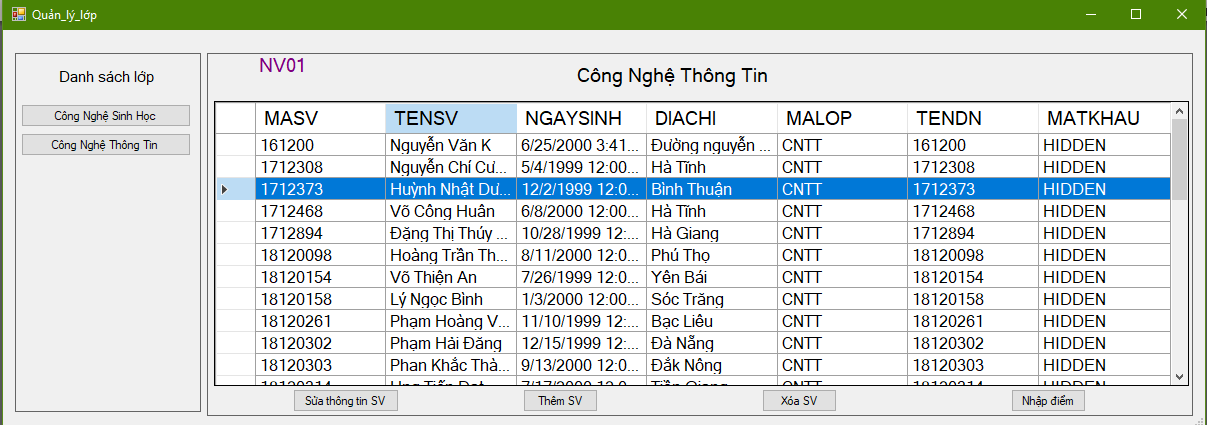
* Sau đó chọn “Lưu” để lưu sinh viên. Nếu đúng, có thông báo thành công, ngược lại có thông báo sai.
* Sinh viên được thêm thành công

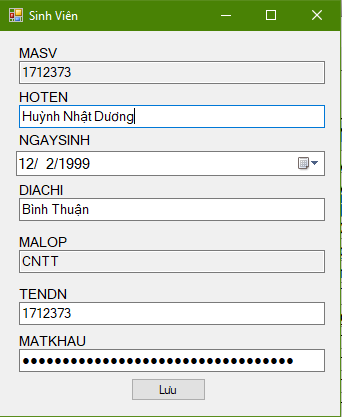


* Kiểm tra trong Database

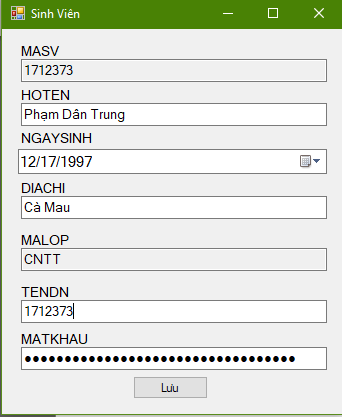


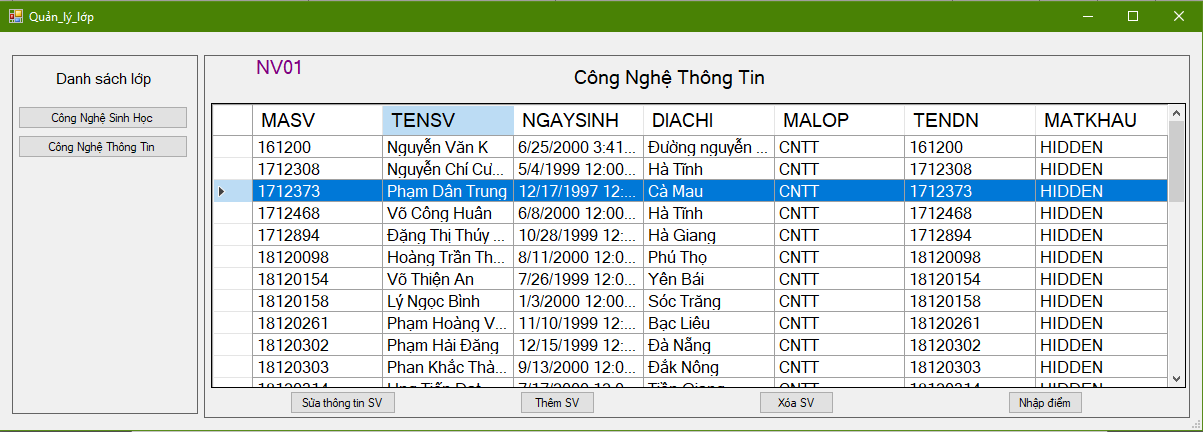
* + 1. Chỉnh sửa sinh viên
* Chọn một sinh viên, sau đó chọn nút “Sửa thông tin SV”

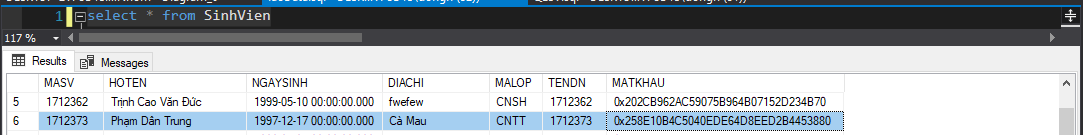
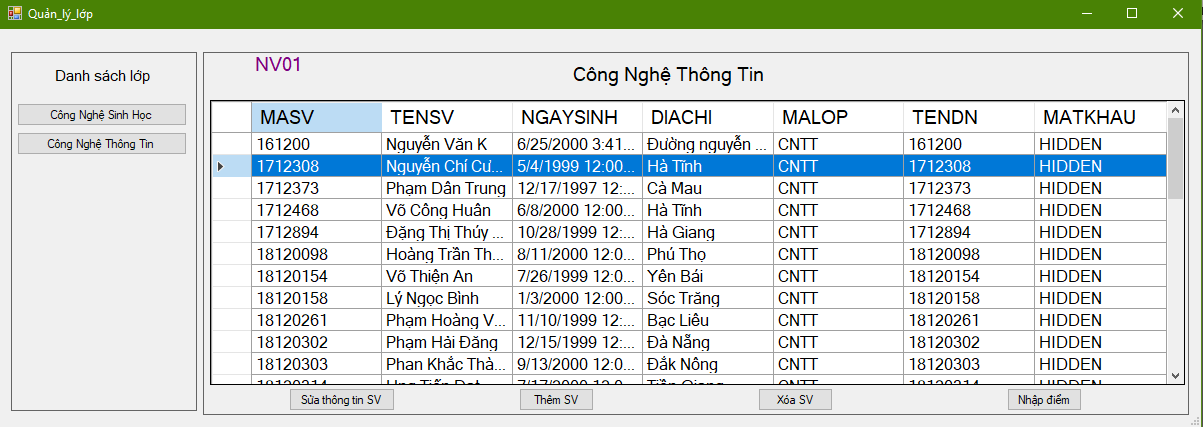


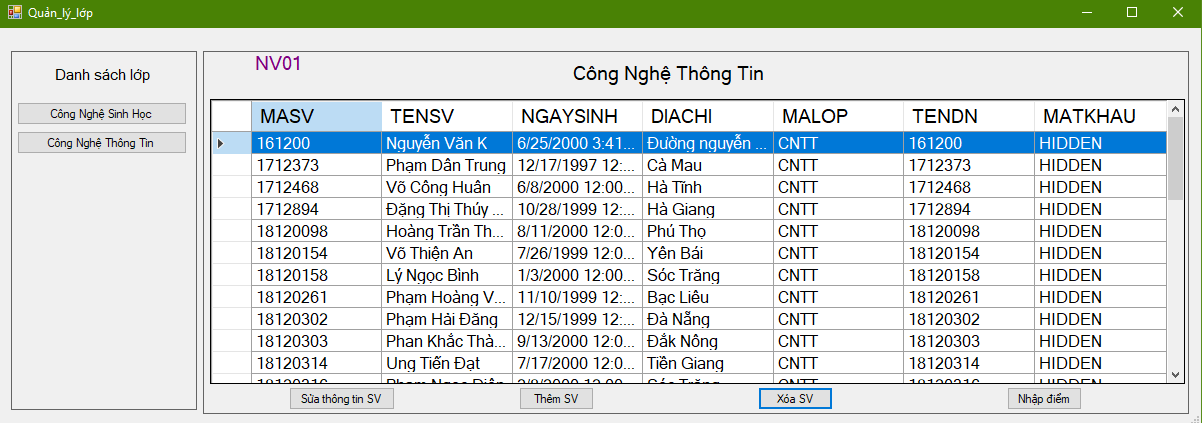


* Tiến hành nhập các thông tin mới. Vì mã sinh viên là Primary Key và mã lớp là khóa ngoại nên các ô đó không sửa. Ô MATKHAU thực chất chỉ là chuỗi hash mật khẩu của sinh viên, ta vẫn có thể chỉnh sửa mật khẩu như bình thường nếu cần thiết
* Sau đó chọn “Lưu” để lưu thông tin

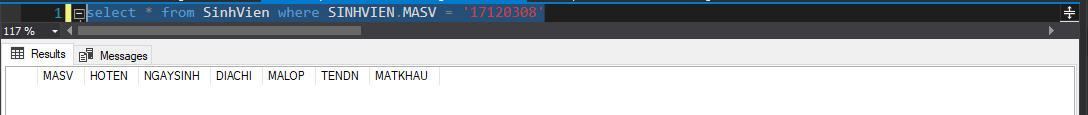


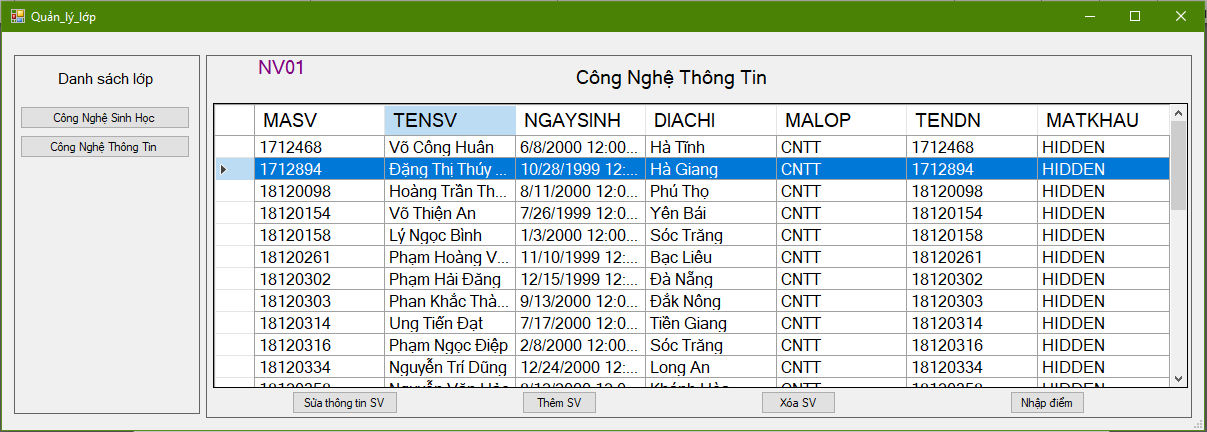


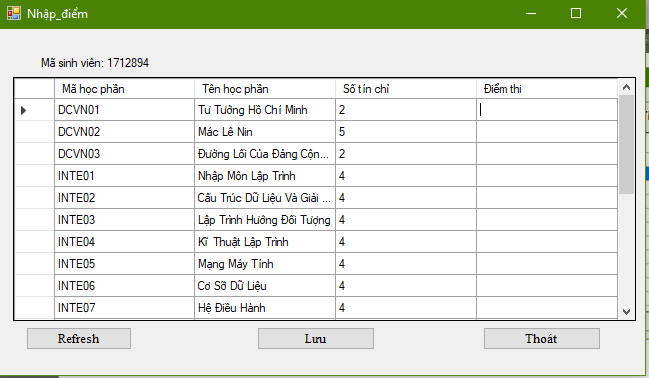
* Kiểm tra trong Database
  + 1. Xóa sinh viên
* Chọn một sinh viên và chọn “Xóa SV” (xóa sinh viên có mã số “1712308”)
* Sau khi xóa



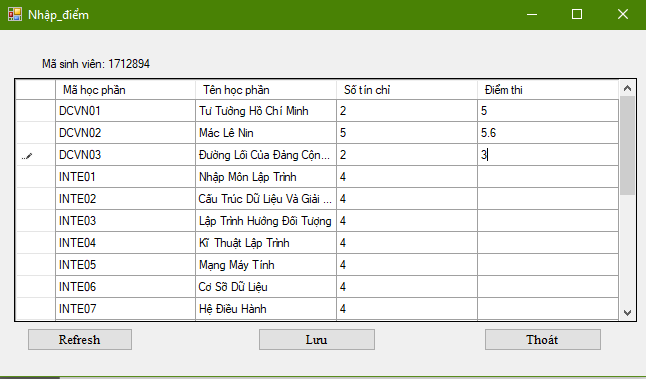
* Kiểm tra trong Database



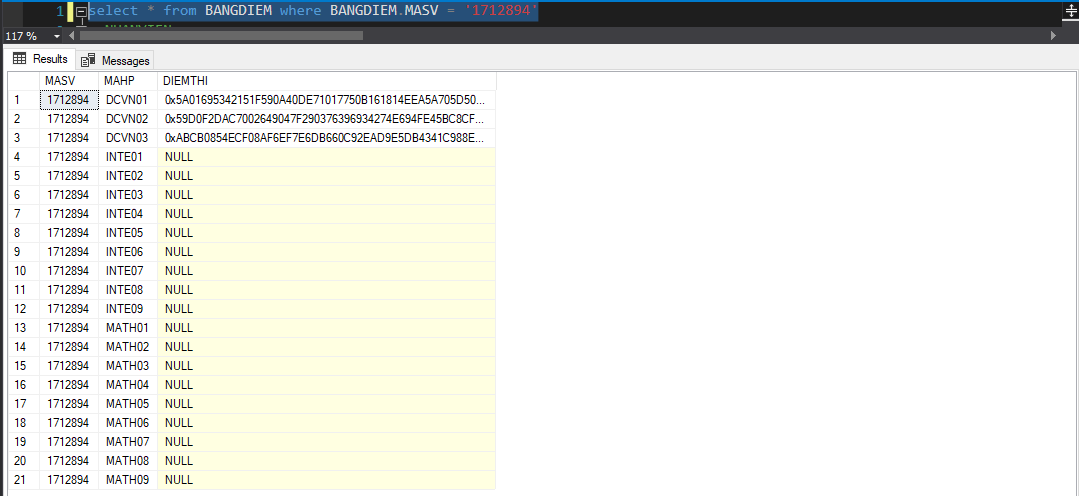
* + 1. Màn hình nhập điểm
* Chọn một sinh viên, sau đó chọn “Nhập điểm”. Nhập điểm cho sinh viên có mã số là “1712894”.
* Chọn vào cột điểm thi để tiến hành nhập điểm. Định dạng là số thập phân không âm và nhỏ hơn 10, nếu nhập sai định dạng thì khi chọn “lưu” sẽ có thông báo.



* Khi nhập xong, chọn “lưu” để lưu. Điểm sẽ được mã hóa bằng thuât toán RSA512 với Public Key của nhân viên.

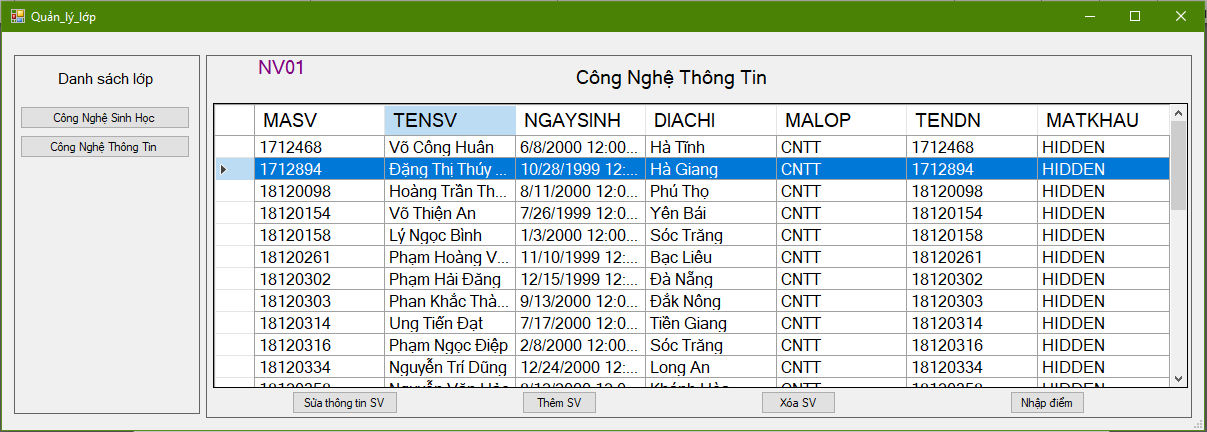


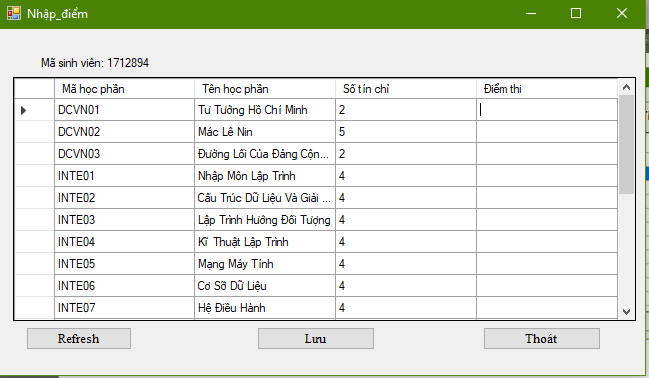
* Kiểm tra trong Database



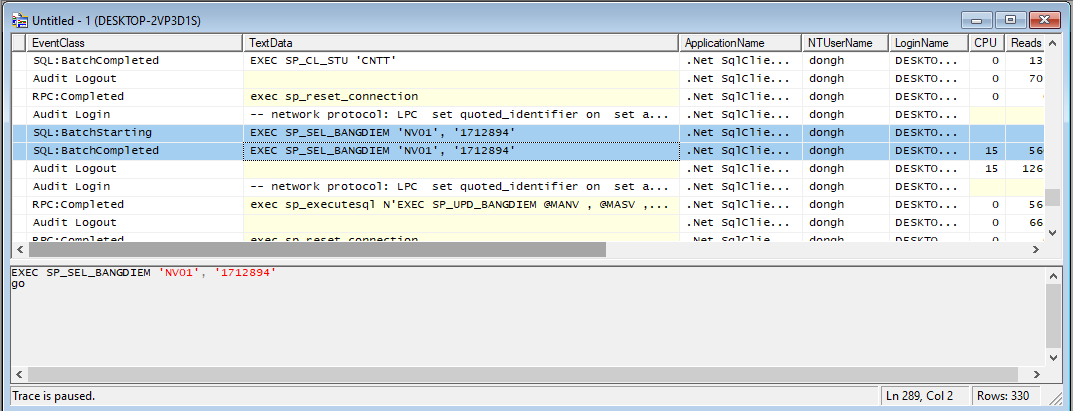
1. Sử dụng công cụ SQL Profile để theo dõi thao tác trong màn hình nhập điểm sinh viên

* Tải bảng điểm theo mã sinh viên và nhân viên

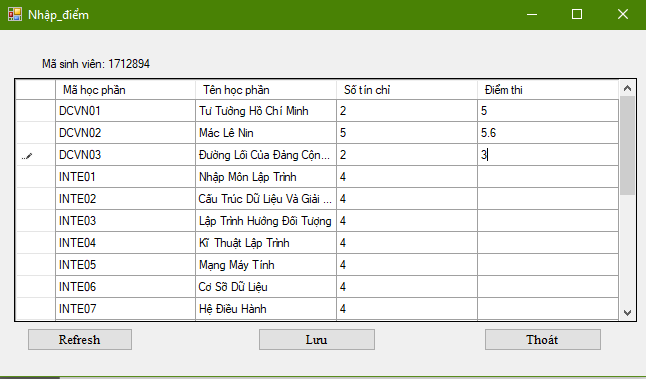


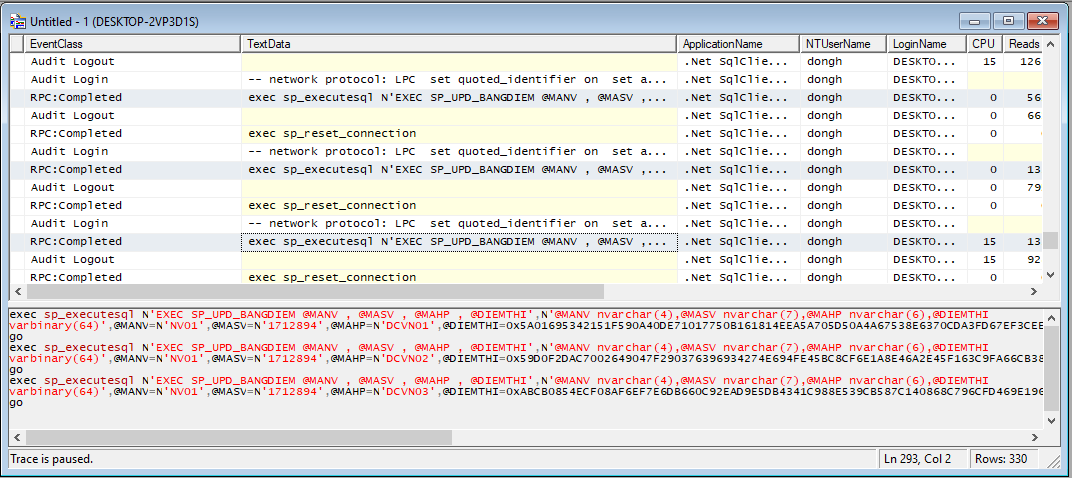


* Kết quả trong SQL Profile

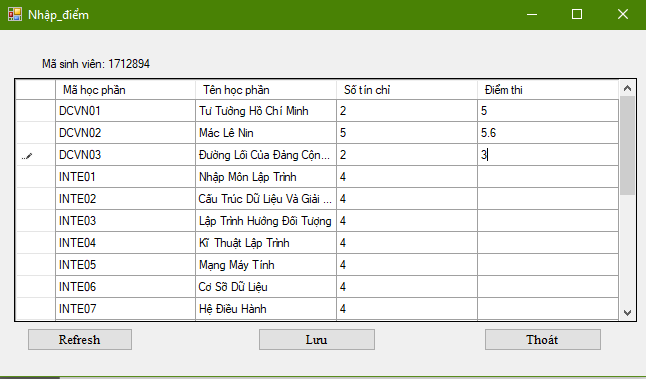


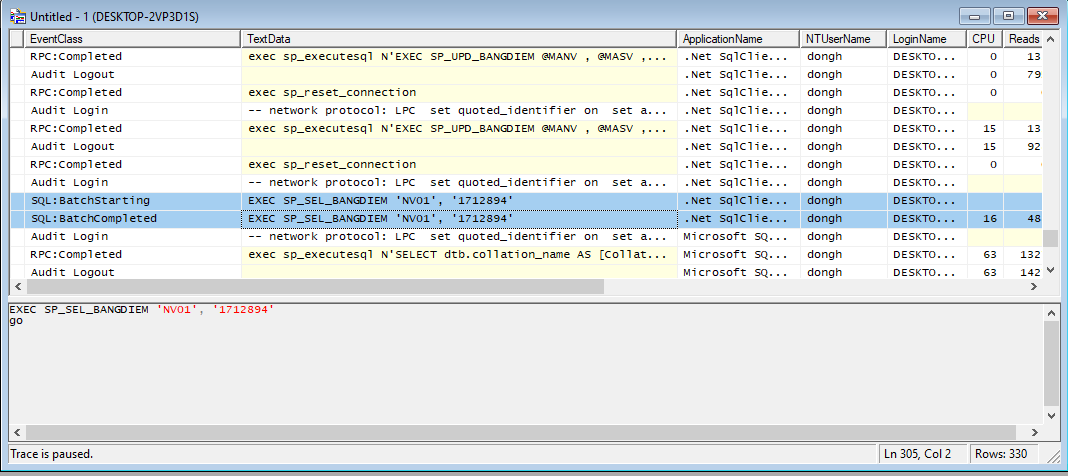
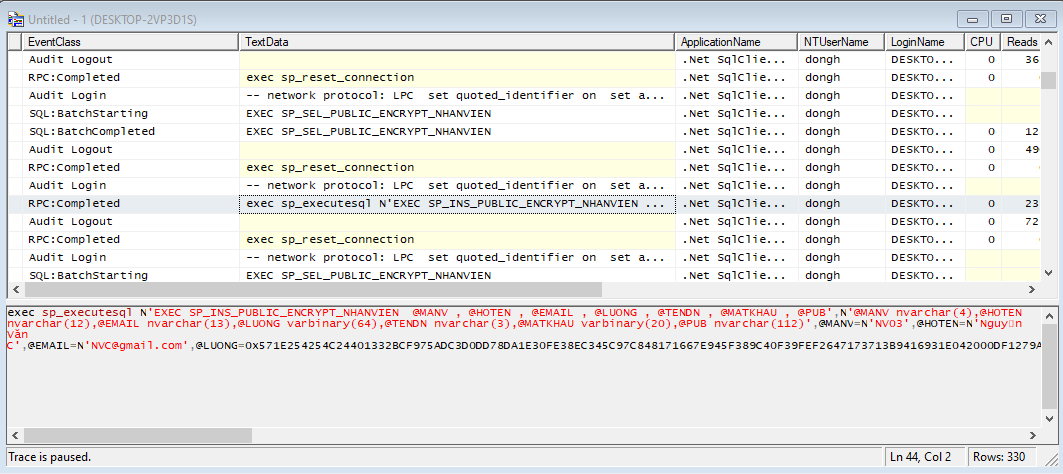
* Khi nhập điểm và lưu



* Kết quả trong SQL Profile (vì nhập điểm cho 3 môn nên có ba query)

* Sau khi lưu và tải lại danh sách



* Kết quả trong SQL Profile
* Kết quả trong SQL Profile khi thêm mới một nhân viên (giá trị lương đã được mã hóa bằng thuật toán RSA512

Nhận xét: Các giá trị điểm được mã hóa bằng thuật toán RSA512 trên Client sau đó gọi SP\_UPD\_BANDIEM để lưu xuống Database. Điều này đảm bảo tính riêng tư và bảo mật vì ngoài chính mình ra thì bên trung gin, kẻ tấn công, người quản lý Database không ai có khóa bí mật để giải mã nội dung (cụ thể ở đây là điểm). 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.