

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

------------------------

**An Toàn Ứng Dụng Web Và CSDL**

**Bài Lab 4**

**Họ Tên: Trần Quốc Trượng**

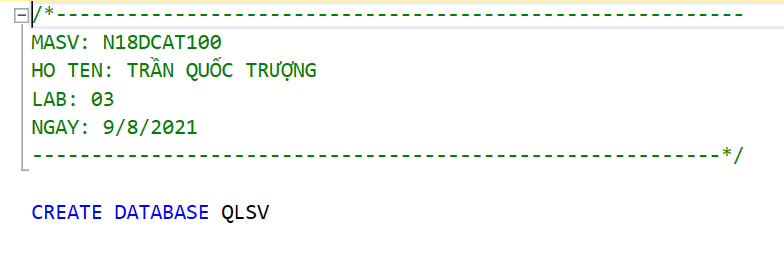
**MSSV: N18DCAT100**

**Lớp: D18CQAT02-N**

**TP.HCM - 2021**

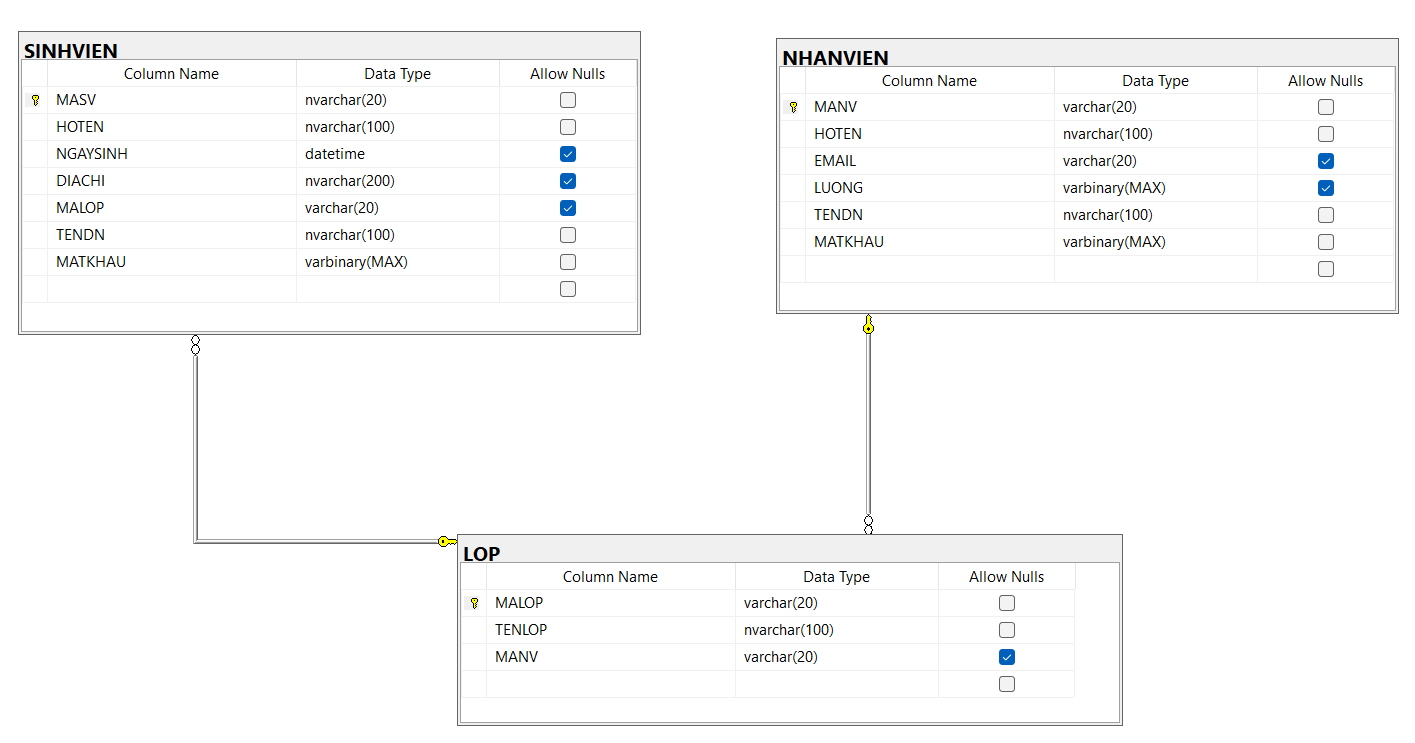


### a) Viết script tạo Database có tên QLSV.



### b) Viết script tạo mới các Table SINHVIEN, NHANVIEN, LOP

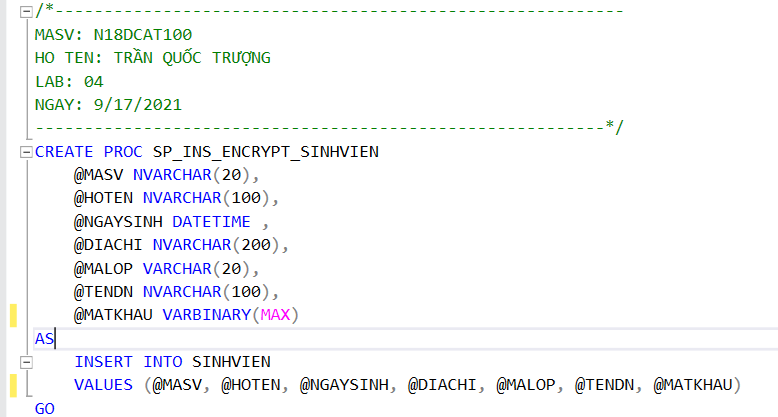




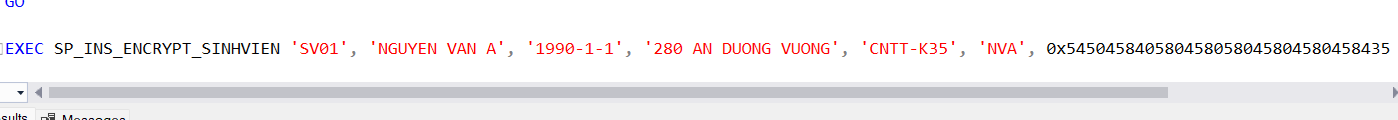
### c) Viết các Stored procedure sau

#### i) Stored dùng để thêm mới dữ liệu (Insert) vào table SINHVIEN

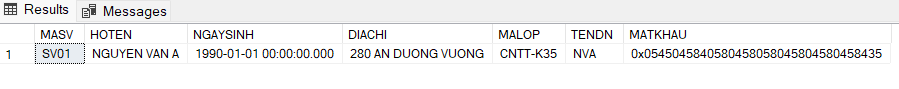
* Bước 1: Tạo Proc



* Bước 2: Thực hiện thêm dữ liệu với mật khẩu đã được hash MD5 từ client

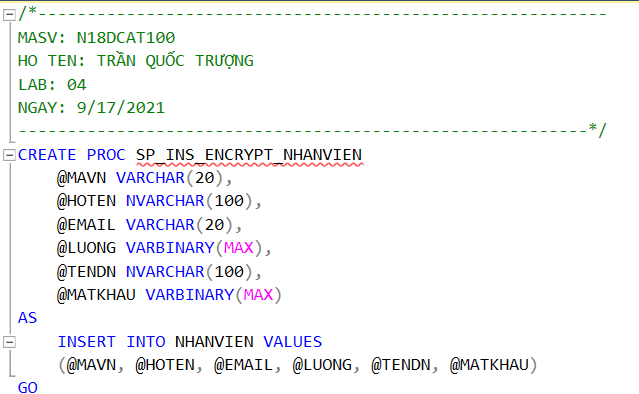


* Bước 3: Kết quả SELECT \* FROM SINHVIEN

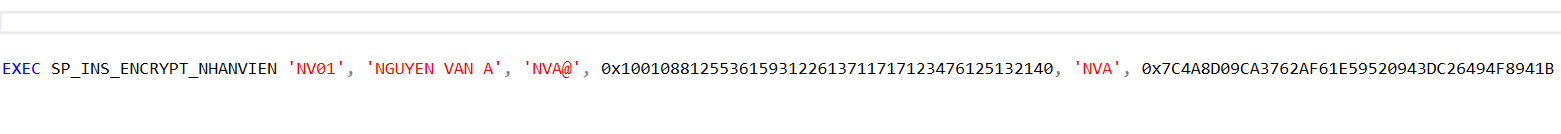


#### ii) Stored dùng để thêm mới dữ liệu (Insert) vào table NHANVIEN, trong đó thuộc tính MATKHAU đã được mã hóa (HASH) sử dụng SHA1 từ Client và thuộc tính LUONG sẽ được mã hóa sử dụng thuật toán AES 256 từ Client, với khóa mã hóa là mã số của sinh viên thực hiện bài Lab này

* Bước 1: Tạo Stored procedure



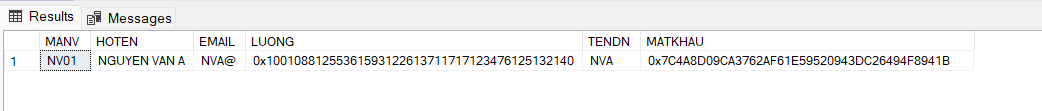
* Bước 2: Thực thi stored



Trong đó tham số lương là 3000000 đã được mã hóa AES 256 từ client

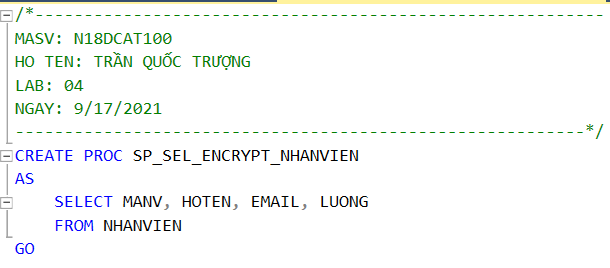
Và tham số mật khẩu 123456 đã được hash SHA1 từ client

* Bước 3: Kết quả Select \* from NHANVIEN



#### iii) Stored dùng để truy vấn dữ liệu nhân viên (NHANVIEN)

* Bước 1: Tạo Proc



* Bước 2: Kiểm tra kết quả

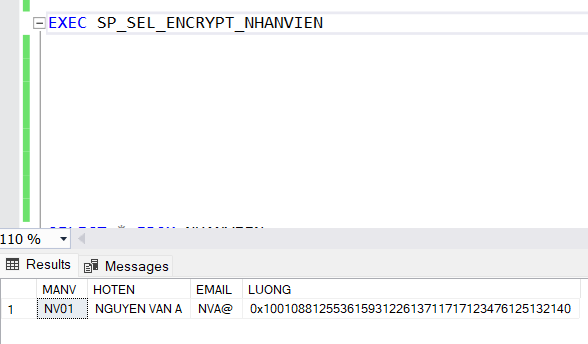
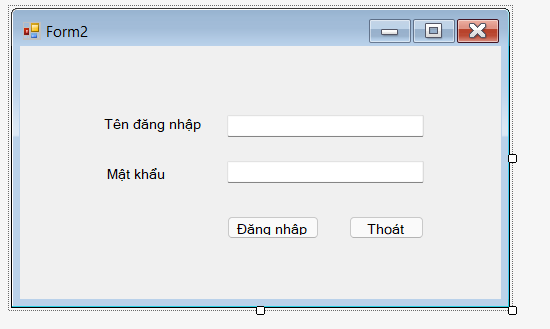


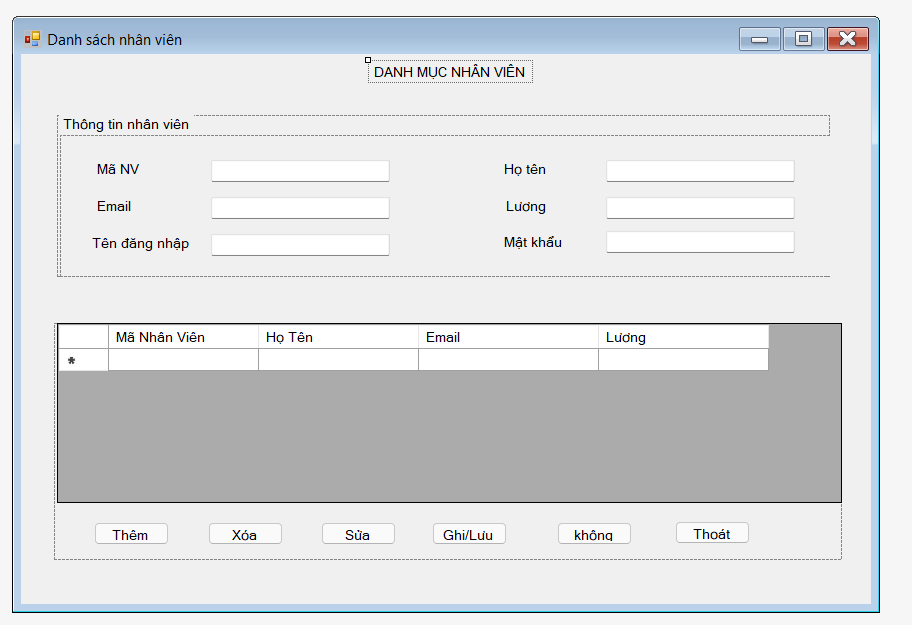
Figure 1. Giá trị Luong vẫn còn mã hóa

### d + e) Viết màn hình quản lý đăng nhập hệ thống (sử dụng C#)

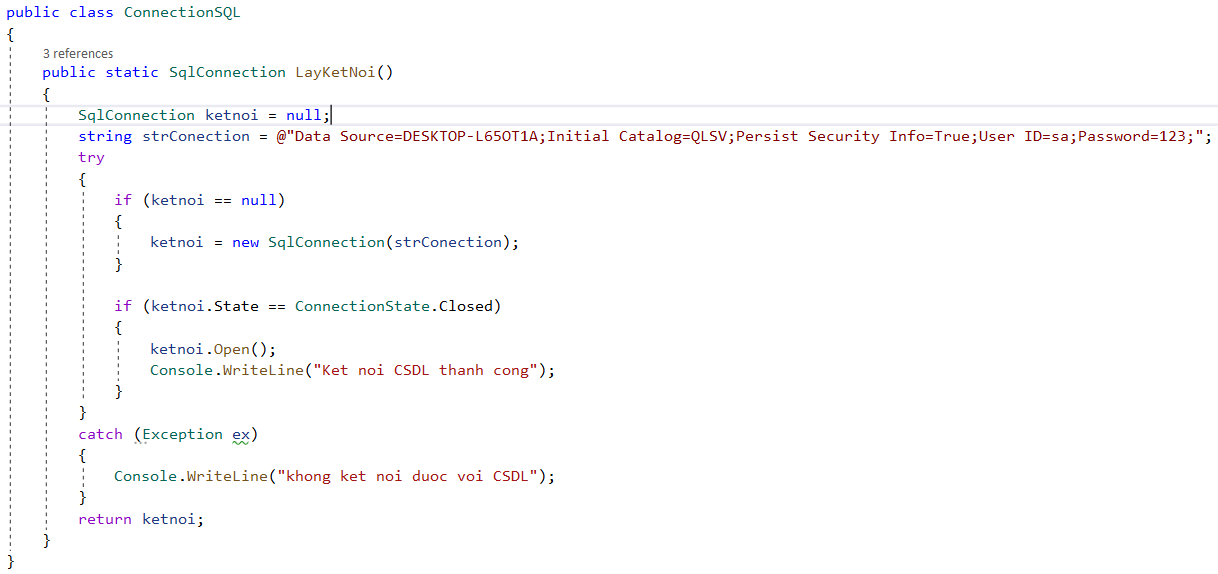
* Bước 1: Tạo form đăng nhập



* Bước 2: Tạo form Danh sách nhân viên



* Bước 3: Viết mã C# Class “ConnectionSQL” kết nối CSDL QLSV



* Bước 4: Viết Class “Cryption” chứa các function mã hóa và giải mã dữ liệu

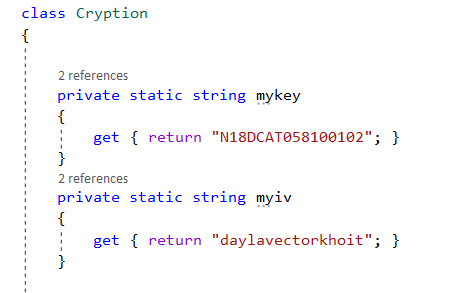


Figure 2. key 256 bit và initialVector dùng cho AES



Figure 3. phương thức mã hóa AES



Figure 4. Phương thức giải mã AES

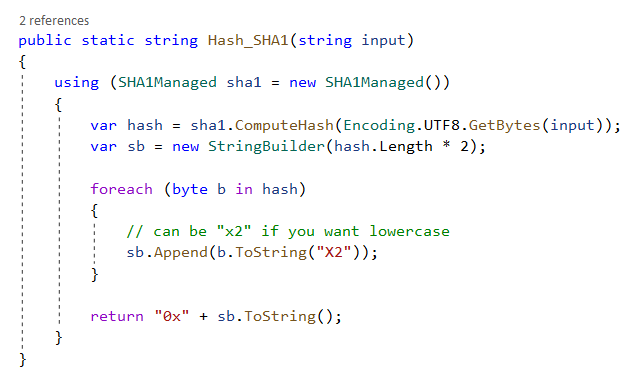


Figure 5. Phương thức Hash mật khẩu SHA1

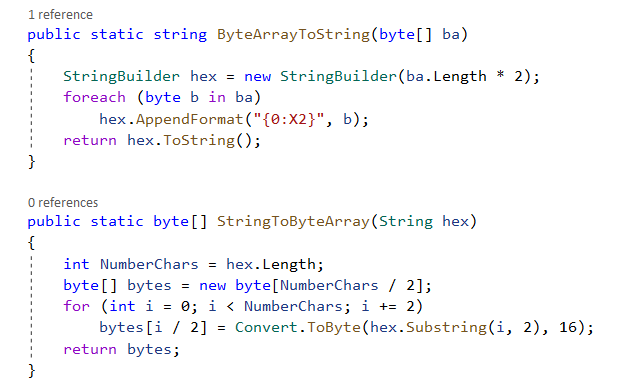
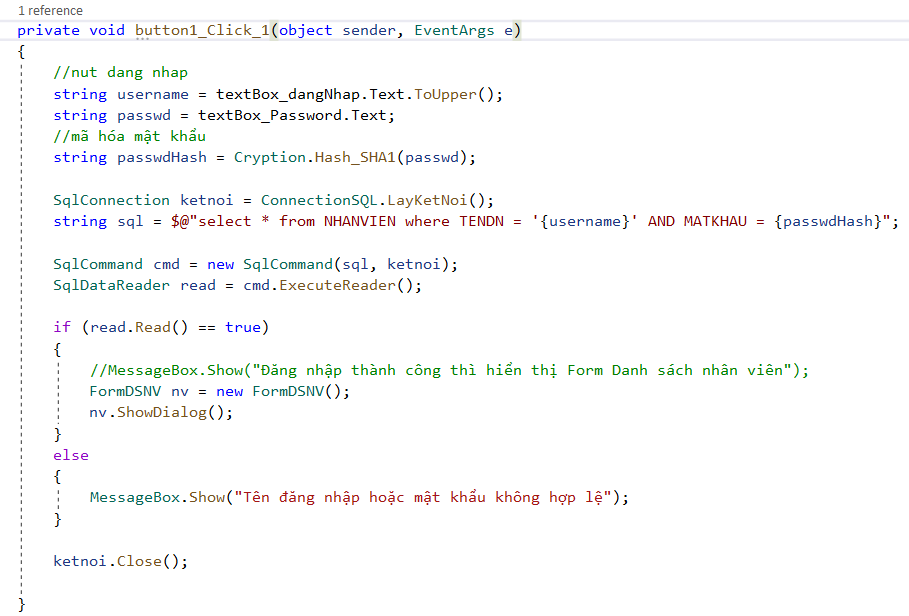
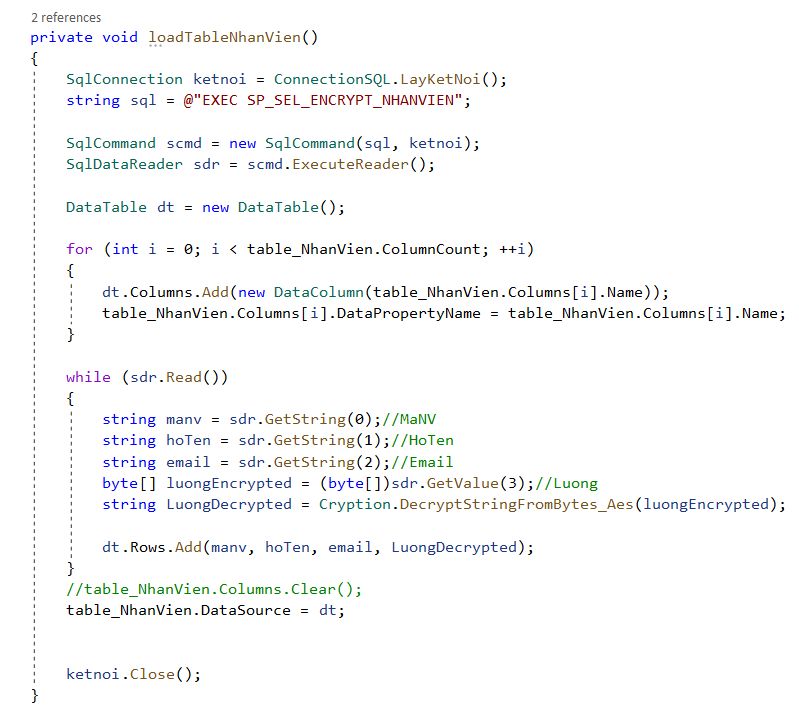


Figure 6. Các method khác

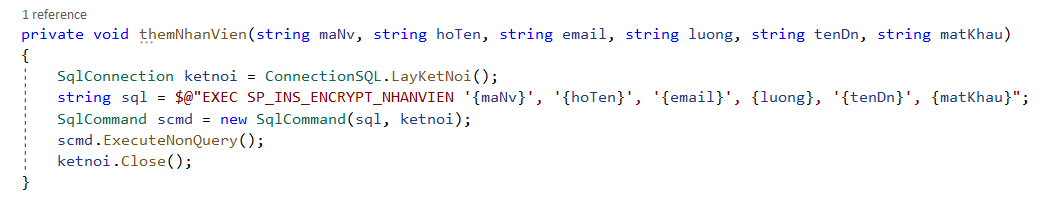
* Bước 5: Viết mã xử lý chức năng đăng nhập

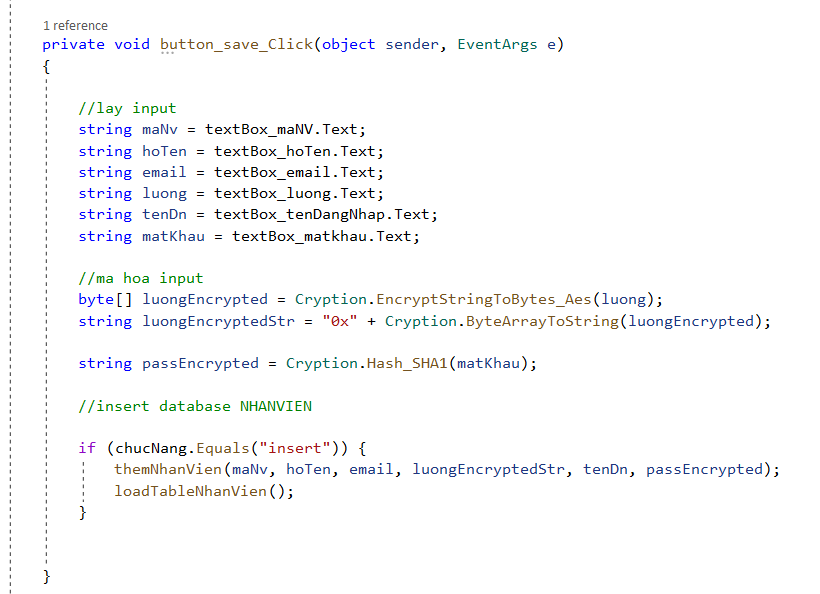


* Bước 6: Viết mã giải mã dữ liệu lương và hiển thị lên màn hình



* Bước 7: Viết code mã hóa dữ liệu và thêm 1 nhân viên vào CSDL





* Bước 8: Chạy ct và kiểm tra kết quả

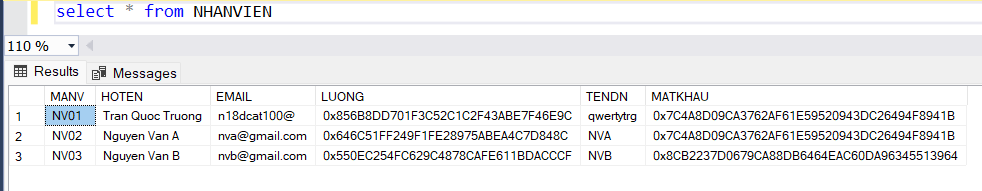


Figure 7. Dữ liệu hiện có trong DB

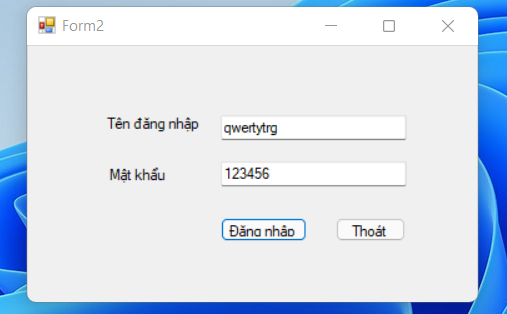


Figure 8. Nhập thông tin đăng nhập

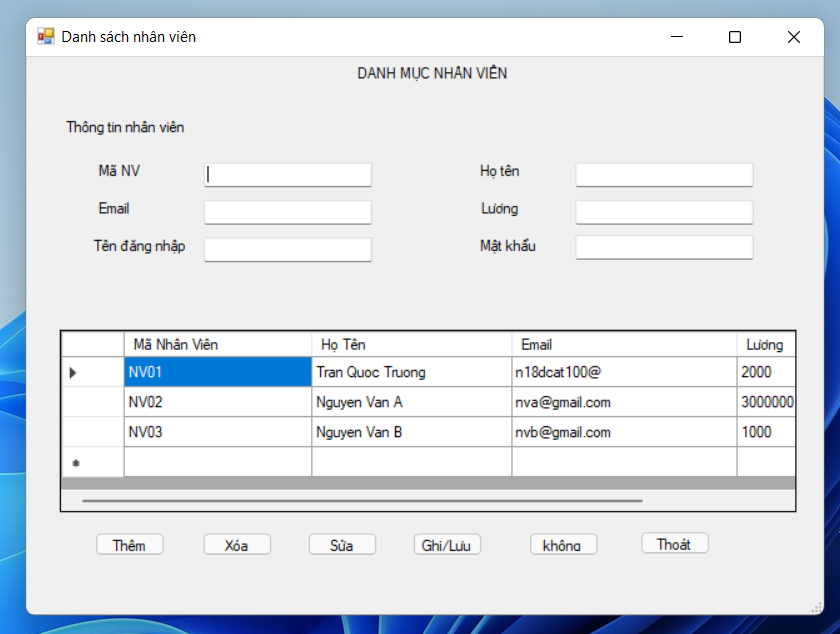


Figure 9. Đăng nhập thành công và hiển thị DSNV với luong đã được gải mã

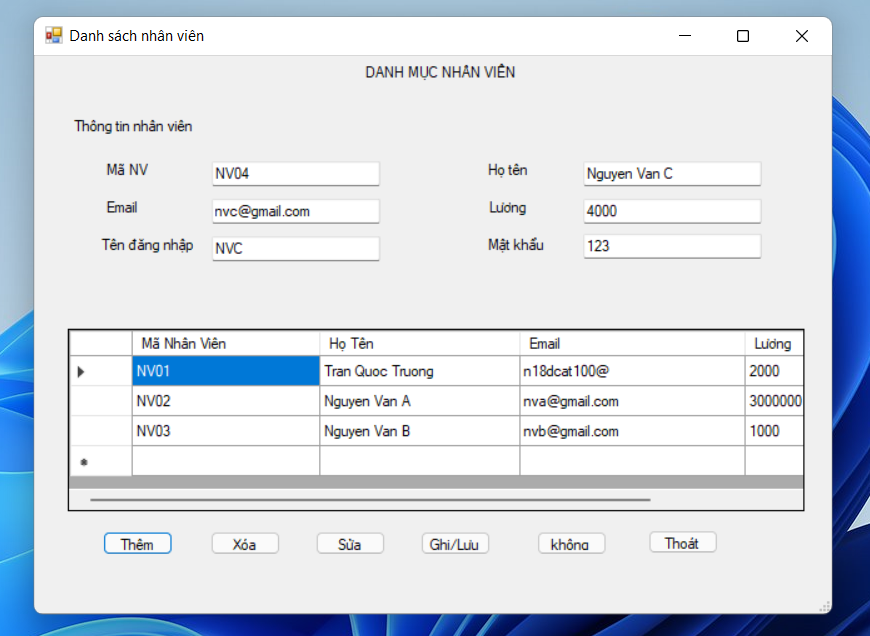


Figure 10. Nhấn nút thêm > nhập thông tin nv mới > nhấn Ghi/Lưu

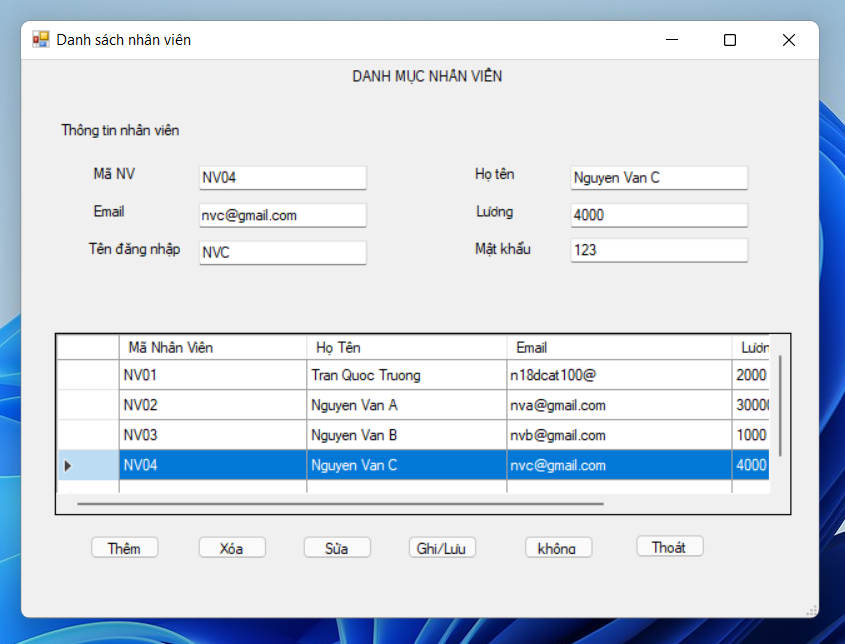
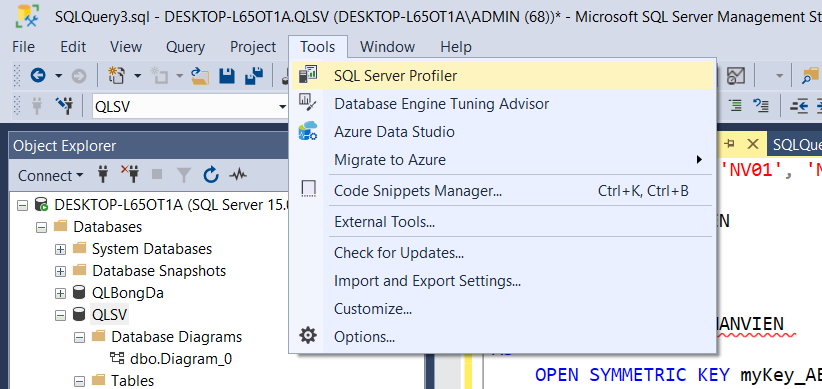


Figure 11. Sau khi nhấn Ghi/Lưu và Load lại table

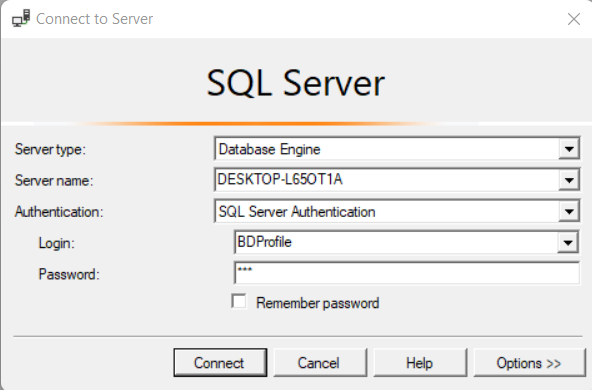
### f) Sử dụng công cụ SQL Profile để theo dõi thao tác đăng nhập từ màn hình quản lý đăng nhập trên, nhận xét.

i) Mở màn hình quản lý đăng nhập

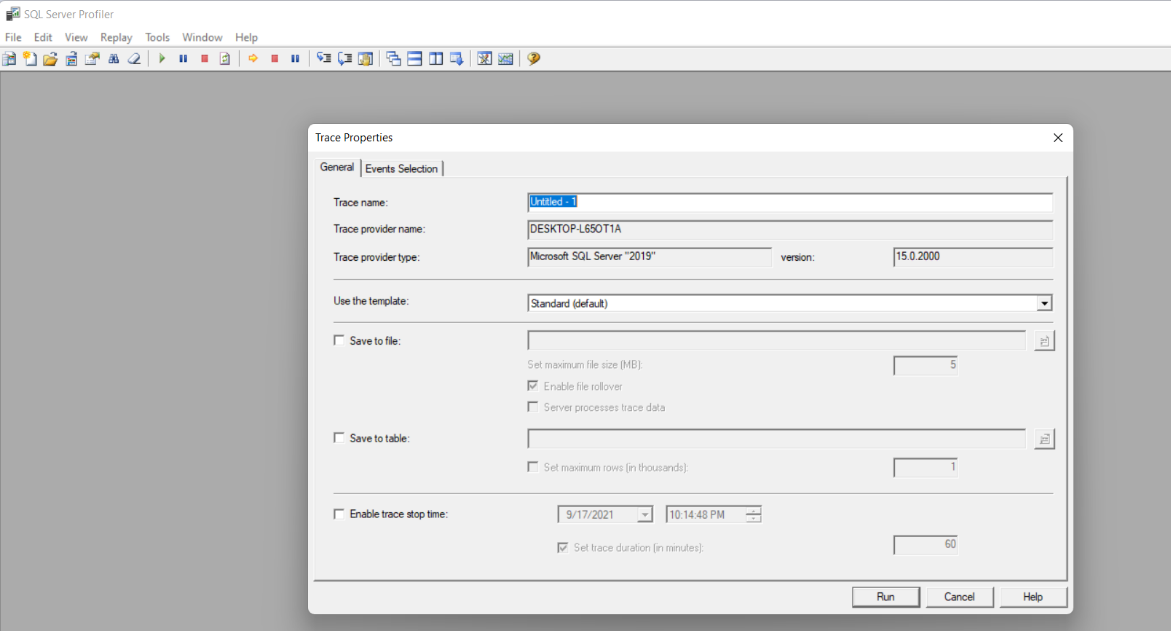


Hình 3. Tools > SQL Server Profiler

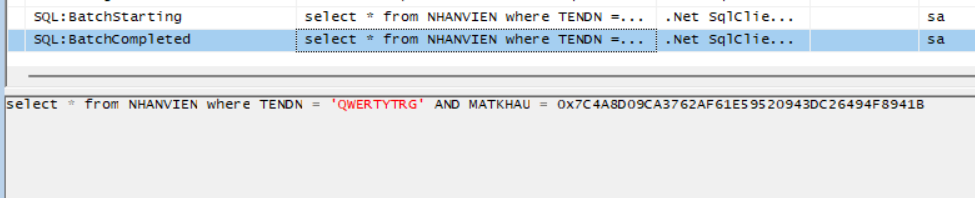
ii) Nhập tên đăng nhập và mật khẩu



iii) Nhấn nút đăng nhập



iv) Chuyển sang màn hình SQL Profile, xem kết quả



v) Copy câu lệnh truy vấn trong SQL Profile

vi) Thực thi câu lệnh này và viết nhận xét.

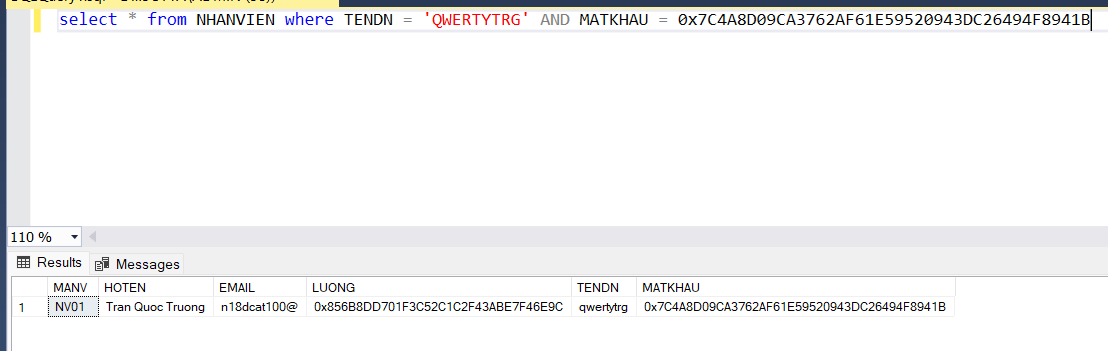
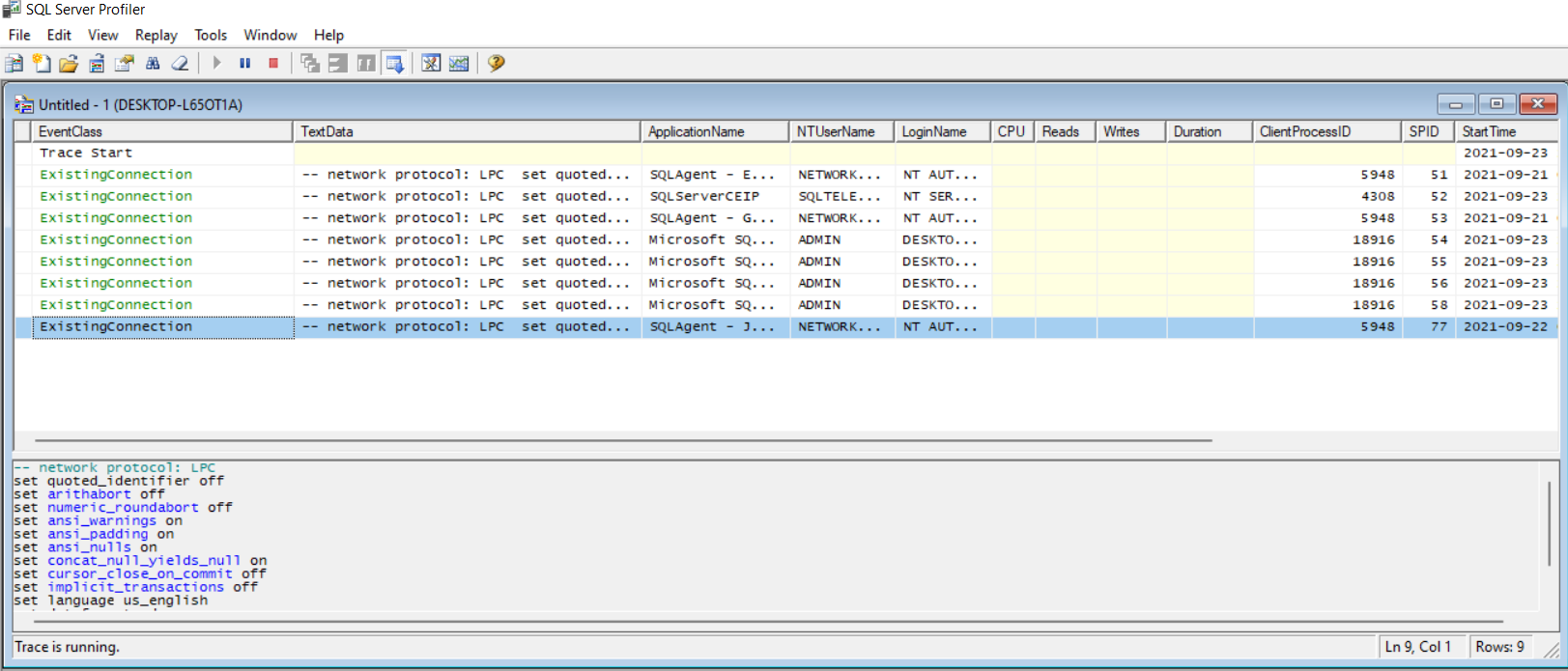


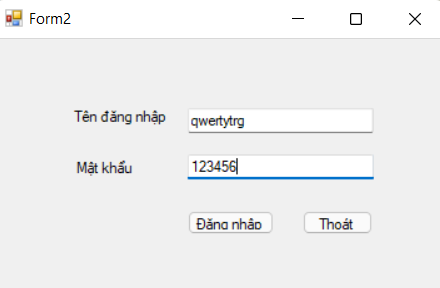
Figure 12. Admin Server có thể lấy được dữ liệu từ Client gửi tới nhưng không thể biết được nội dung vì dữ liệu đã được mã hóa

### g) Sử dụng công cụ SQL Profile để theo dõi load màn hình danh sách nhân viên.

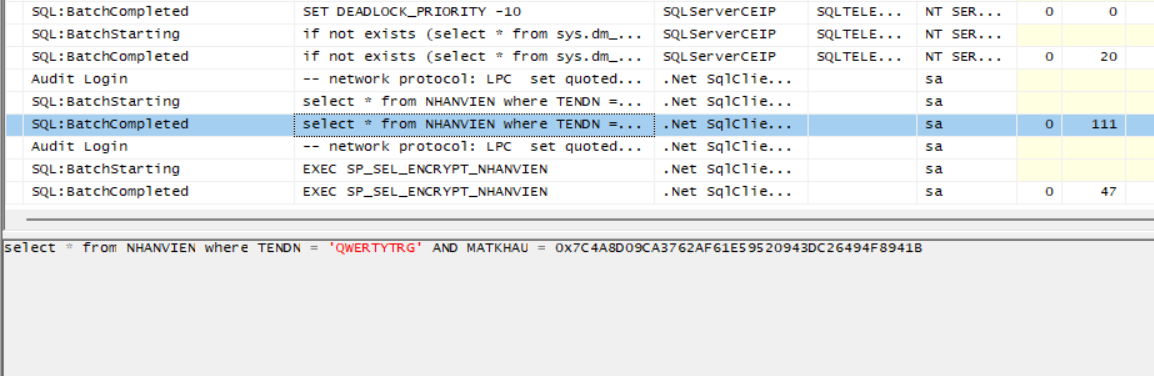
i) Mở màn hình quản lý đăng nhập



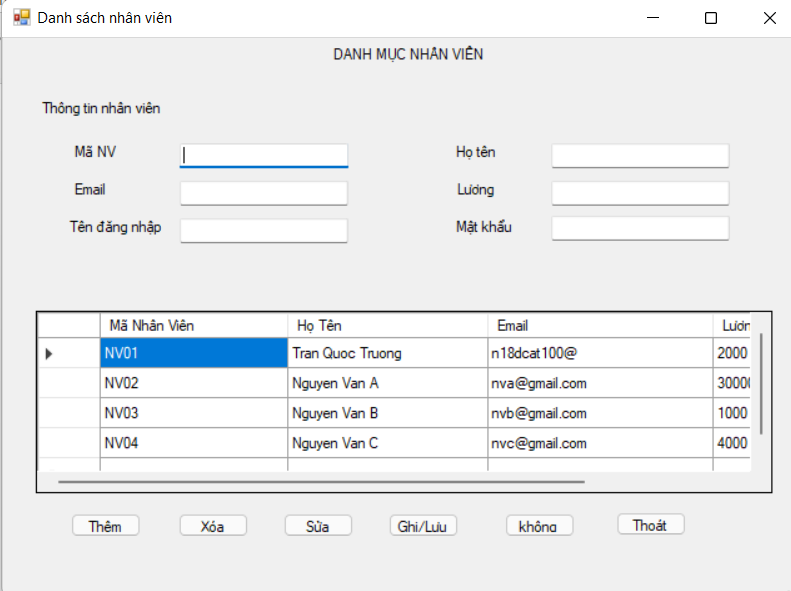
ii) Nhập tên đăng nhập và mật khẩu đúng



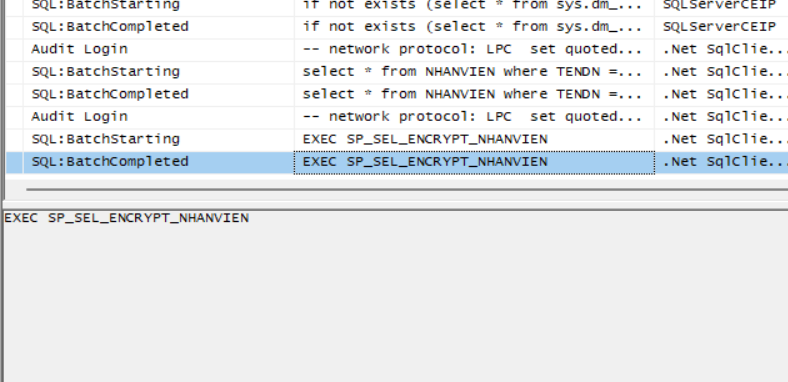
iii) Nhấn nút đăng nhập



iv) Hiển thị màn hình danh sách nhân viên



v) Chuyển sang màn hình SQL Profile, xem kết quả



vi) Copy câu lệnh truy vấn trong SQL Profile

vii)Thực thi câu lệnh này và viết nhận xét

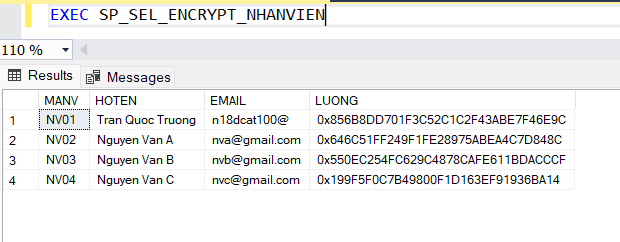


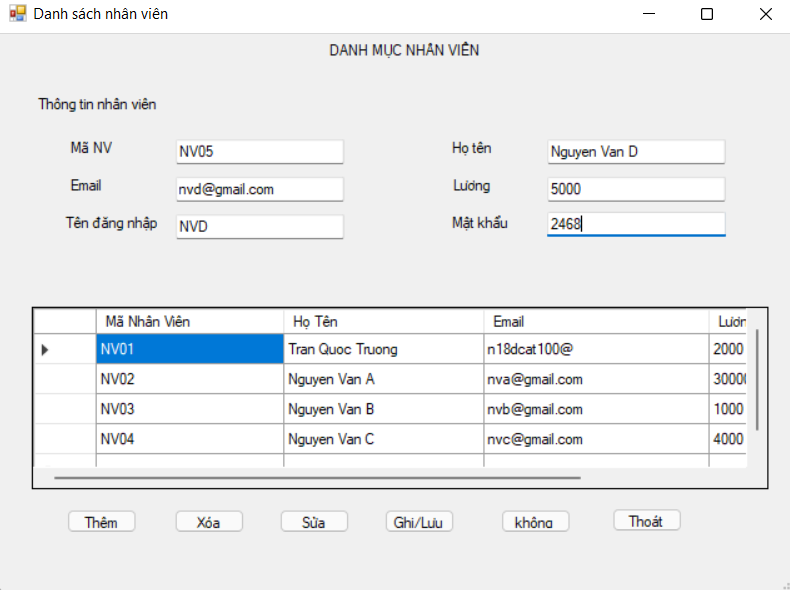
Figure 13. Admin Server không thể biết được lương của các nhân viên

### h) Sử dụng công cụ SQL Profile để theo dõi thao tác thêm mới nhân viên nhân viên.

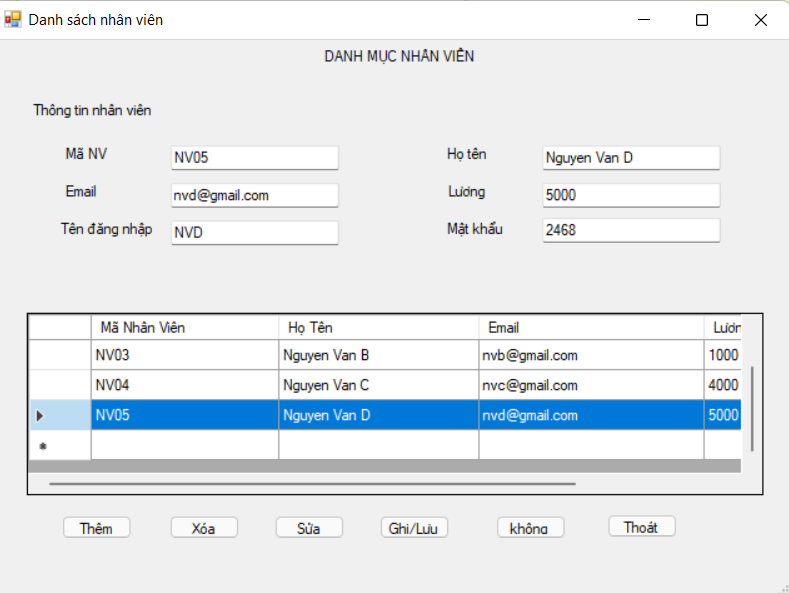
i) Màn hình danh sách nhân viên

ii) Chọn chức năng thêm

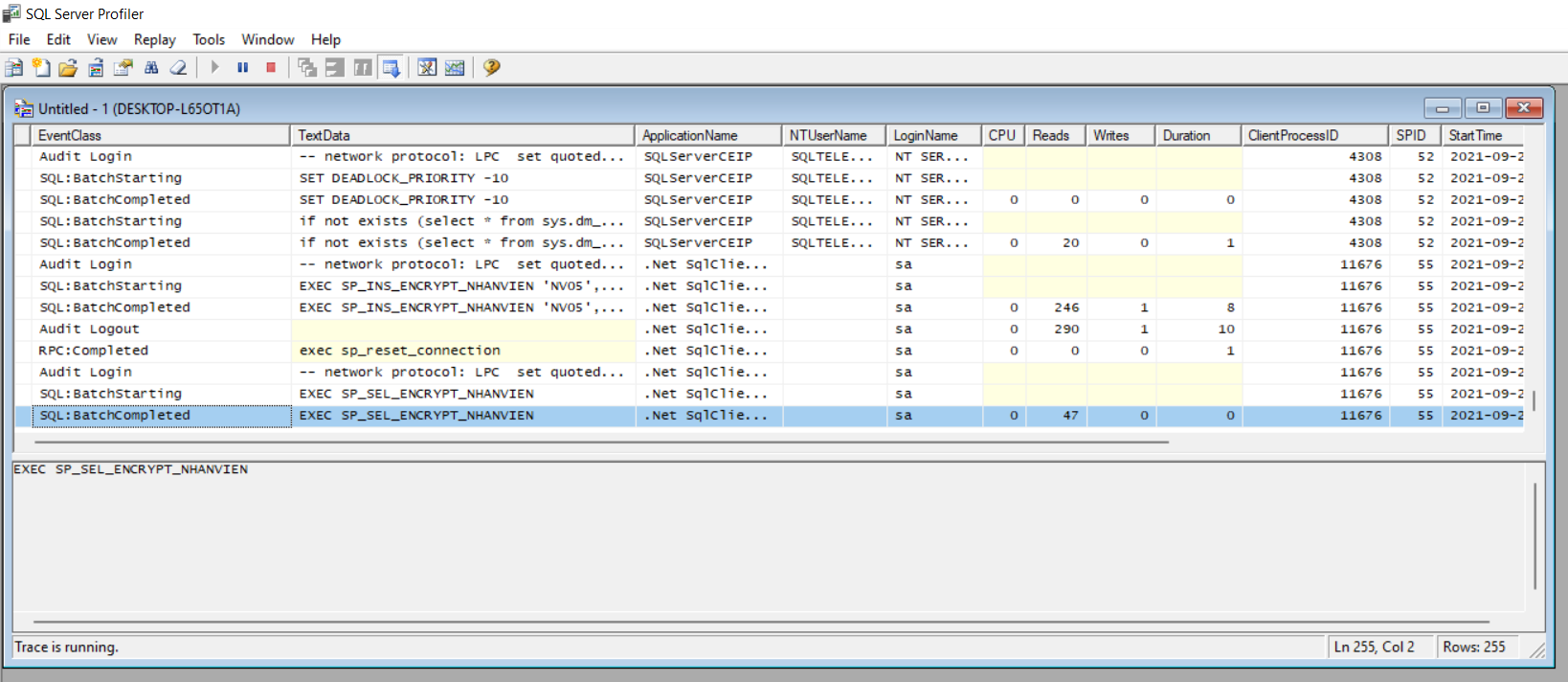
iii) Nhập thông tin nhân viên mới

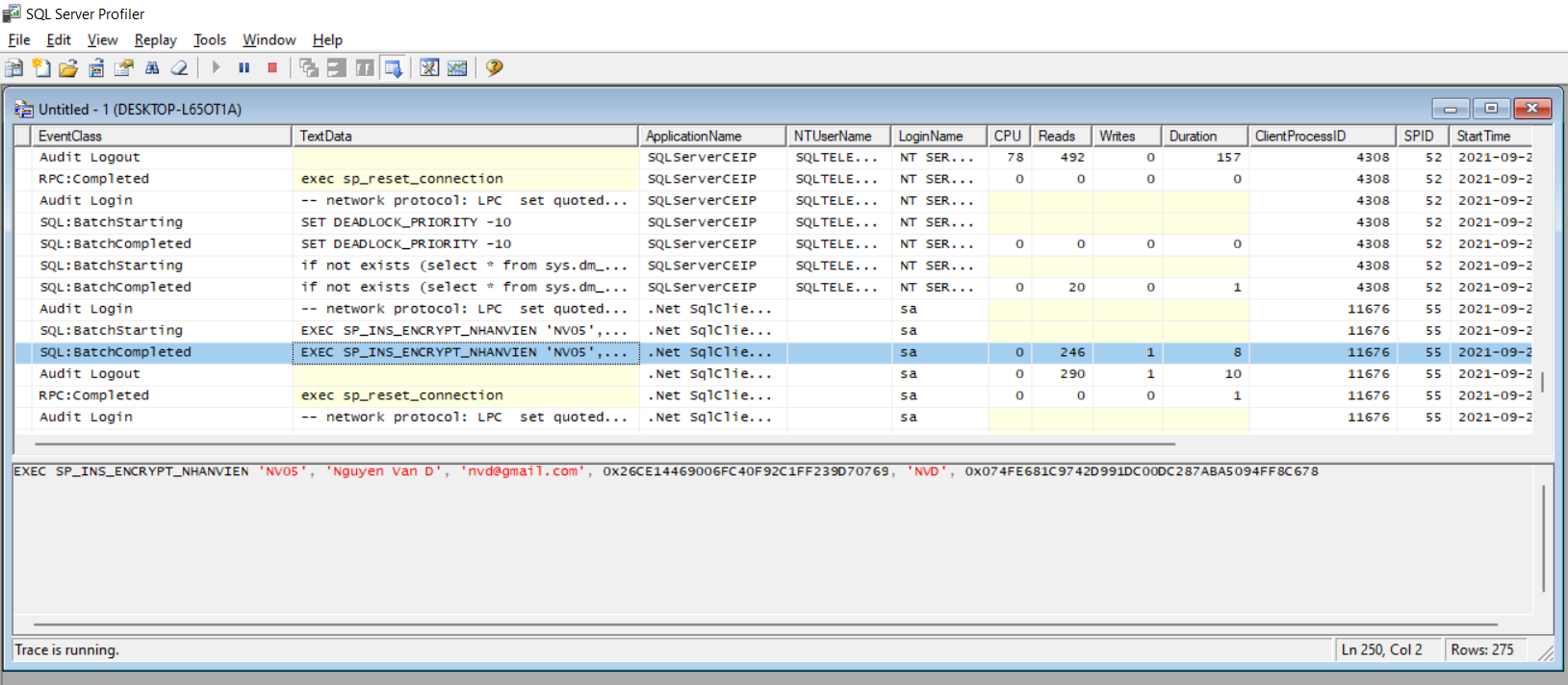


iv) Nhấn nút lưu để lưu thông tin nhân viên xuống CSDL



v) Chuyển sang màn hình SQL Profile, xem kết quả





vi) Copy câu lệnh SP\_INS\_ENCRYPT\_NHANVIEN trong SQL Profile

vii)Xem và viết nhận xét.

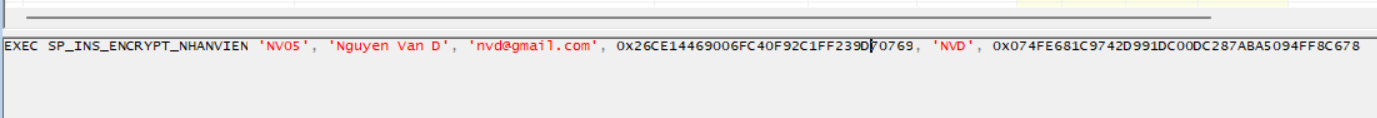


Figure 14. Attacker đứng giữa hoặc Admin server sẽ không biết được nội dung luong và mật khẩu của client nhập