

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

~0~



BÁO CÁO LAB 4 – CÁ NHÂN:
MÃ HÓA DỮ LIỆU TỪ CLIENT SỬ DỤNG
CÁC THUẬT TOÁN MÃ HÓA ĐỐI XỨNG

20120313 – Phan Tấn Kiệt

TP Hồ Chí Minh, ngày 27 tháng 4 năm 2023

Mục lục

Câu a, b: Sử dụng lại CSDL của Lab3	3
Câu c: Tạo các stored procedure	3
1. Stored dùng để thêm mới dữ liệu (Insert) vào table SINHVIEN	3
2. Stored procedure SP_SEL_NHANVIEStored dùng để thêm mới dữ liệu (Insert) vào table NHANVIEN	3
3. Stored procedure SP_SEL_NHANVIEN	6
Câu d: Viết màn hình quản lý đăng nhập hệ thống	6
Câu e. Màn hình quản lý nhân viên:.....	7
Câu f: Sử dụng công cụ SQL Profile để theo dõi thao tác đăng nhập và nhận xét	8
Nhận xét:	10
Câu g: Sử dụng công cụ SQL Profile để theo dõi load màn hình danh sách nhân viên và nhận xét.....	10
Nhận xét:	11
Câu h: Sử dụng công cụ SQL Profile để theo dõi thao tác thêm mới nhân viên nhân viên.và nhận xét	12
Nhận xét:	13

Câu a, b: Sử dụng lại CSDL của Lab3

Câu c: Tạo các stored procedure

1. Stored dùng để thêm mới dữ liệu (Insert) vào table SINHVIEN

Với MATKHAU được mã hoá MD5 từ client

```
MD5CryptoServiceProvider md5 = new MD5CryptoServiceProvider();
Byte[] buffer1 = md5.ComputeHash(Encoding.UTF8.GetBytes(txtPass.Text));
```

```
IF OBJECT_ID('dbo.SP_INS_ENCRYPT_SINHVIEN','P') IS NOT NULL
DROP PROCEDURE dbo.SP_INS_ENCRYPT_SINHVIEN
GO
CREATE PROCEDURE dbo.SP_INS_ENCRYPT_SINHVIEN
    @MASV NVARCHAR(20),
    @HOTEN NVARCHAR(100),
    @NGAYSINH DATETIME,
    @DIACHI NVARCHAR(200),
    @MALOP VARCHAR(20),
    @TENDN NVARCHAR(100),
    @MATKHAU varbinary
AS
BEGIN
    INSERT INTO SINHVIEN(MASV, HOTEN, NGAYSINH, DIACHI, MALOP, TENDN, MATKHAU)
    VALUES (@MASV, @HOTEN, @NGAYSINH, @DIACHI, @MALOP, @TENDN, @MATKHAU)
END
GO
```

2. Stored procedure SP_SEL_NHANVIEStored dùng để thêm mới dữ liệu (Insert) vào table NHANVIEN

Thuộc tính MATKHAU được mã hóa (HASH) sử dụng SHA1 và thuộc tính LUONG sẽ được mã hóa sử dụng thuật toán AES 256, với khóa mã hóa là 20120313.

```

IF OBJECT_ID('SP_INS_ENCRYPT_NHANVIEN','P') IS NOT NULL
DROP PROCEDURE SP_INS_ENCRYPT_NHANVIEN
GO
CREATE PROCEDURE SP_INS_ENCRYPT_NHANVIEN
    @MANV VARCHAR(20),
    @HOTEN NVARCHAR(100),
    @EMAIL VARCHAR(20),
    @LUONG varbinary(max),
    @TENDN NVARCHAR(100),
    @MATKHAU varbinary(max)
AS
BEGIN
    INSERT INTO NHANVIEN (MANV, HOTEN, EMAIL, LUONG, TENDN, MATKHAU)
    VALUES (@MANV, @HOTEN, @EMAIL, @LUONG, @TENDN, @MATKHAU);
END
GO

```

Sử dụng mã hoá SHA256 để mã thuộc tính MATKHAU và sử dụng AES để mã hoá thuộc tính LUONG.

```

SHA256 sha256 = SHA256.Create();
Byte[] t6 = sha256.ComputeHash(Encoding.UTF8.GetBytes(textBox6.Text));
Byte[] t5 = AES.Encrypt(textBox5.Text, "20120313");

```

Lớp AES:

```
internal class AES
{
    public static byte[] Encrypt(string plainText, string password)
    {
        byte[] iv = new byte[16];
        byte[] key = new Rfc2898DeriveBytes(password, iv, 1000).GetBytes(32);
        byte[] encrypted;
        using (Aes aes = Aes.Create())
        {
            aes.Key = key;
            aes.IV = iv;
            aes.Padding = PaddingMode.PKCS7;
            aes.Mode = CipherMode.CBC;
            ICryptoTransform encryptor = aes.CreateEncryptor(aes.Key, aes.IV);
            using (System.IO.MemoryStream ms = new System.IO.MemoryStream())
            {
                using (CryptoStream cs = new CryptoStream(ms, encryptor,
CryptoStreamMode.Write))
                {
                    using (System.IO.StreamWriter sw = new System.IO.StreamWriter(cs))
                    {
                        sw.Write(plainText);
                        encrypted = ms.ToArray();
                    }
                }
            }
        }
        return encrypted;
    }
    public static string Decrypt(byte[] cipherBytes, string password)
    {
        byte[] iv = new byte[16];
        byte[] key = new Rfc2898DeriveBytes(password, iv, 1000).GetBytes(32);
        string plainText = null;
        using (Aes aes = Aes.Create())
        {
            aes.Key = key;
            aes.IV = iv;
            aes.Padding = PaddingMode.PKCS7;
            aes.Mode = CipherMode.CBC;
            ICryptoTransform decryptor = aes.CreateDecryptor(aes.Key, aes.IV);
            using (System.IO.MemoryStream ms = new
System.IO.MemoryStream(cipherBytes))
            {
                using (CryptoStream cs = new CryptoStream(ms, decryptor,
CryptoStreamMode.Read))
                {
                    using (System.IO.StreamReader sr = new System.IO.StreamReader(cs))
                    {
                        plainText = sr.ReadToEnd();
                    }
                }
            }
        }
        return plainText;
    }
}
```

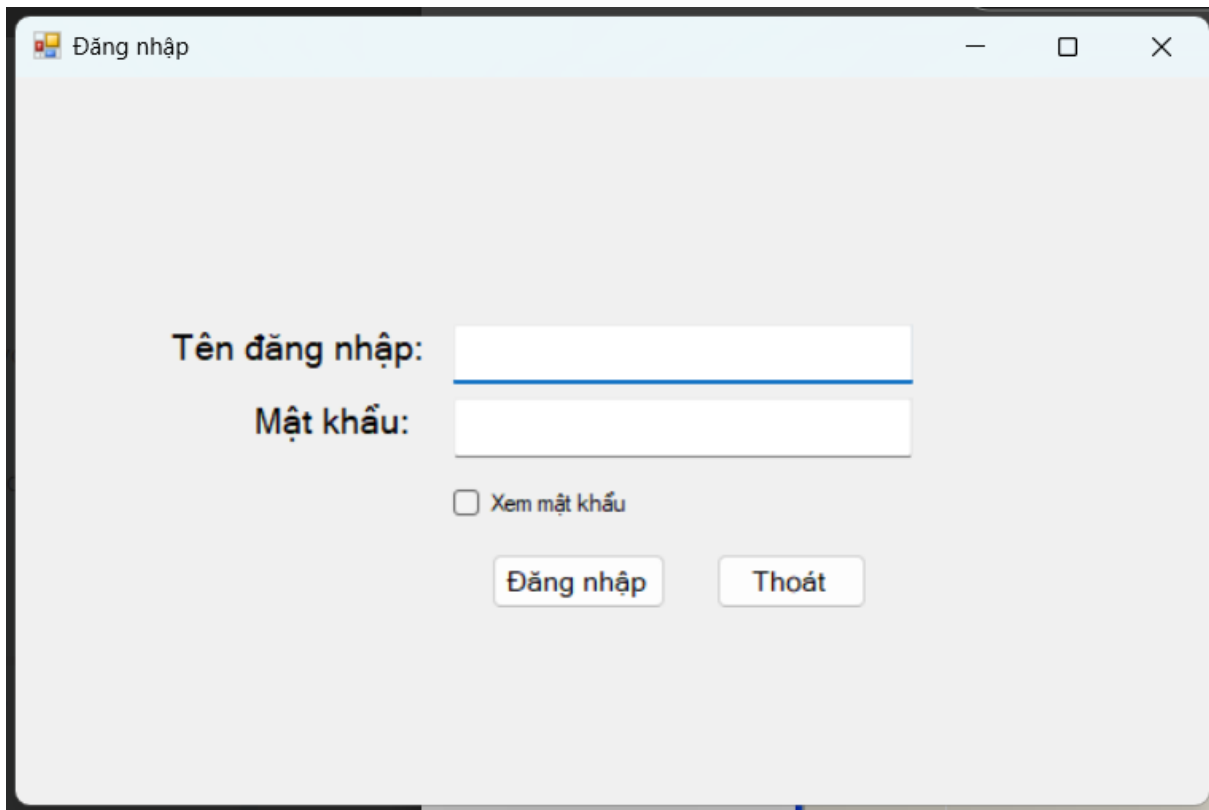
3. Stored procedure SP_SEL_NHANVIEN

Truy vấn dữ liệu từ bảng nhân viên

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

Câu d: Viết màn hình quản lý đăng nhập hệ thống

Màn hình đăng nhập:



Đăng nhập

Tên đăng nhập:

Mật khẩu:

☐ Xem mật khẩu

Câu e. Màn hình quản lý nhân viên:

Màn hình quản lý nhân viên

Danh mục nhân viên

DANH MỤC NHÂN VIÊN

Thông tin nhân viên

Mã NV

Họ tên

Email

Lương

Tên DN

Mật khẩu

	MANV	HOTEN	EMAIL	LUONGNV
▶	NV01	NGUYEN VAN A	NVA@	200000
*				

Thêm

Xoá

Sửa

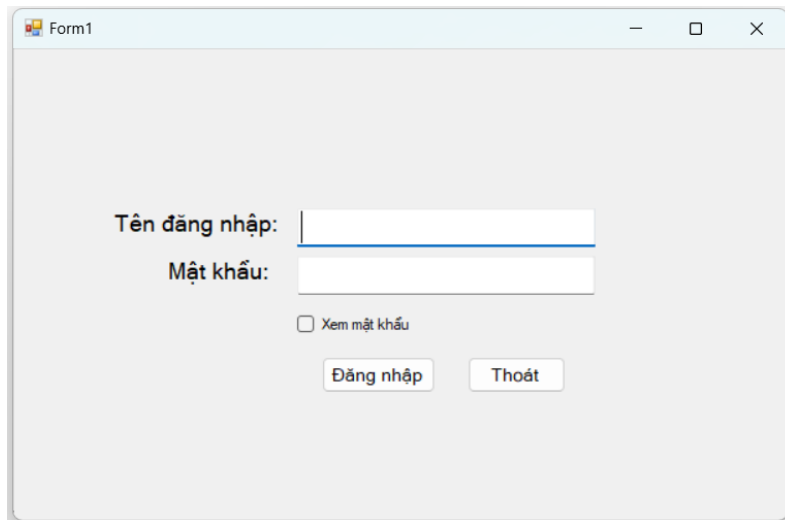
Ghi/Lưu

Không

Thoát

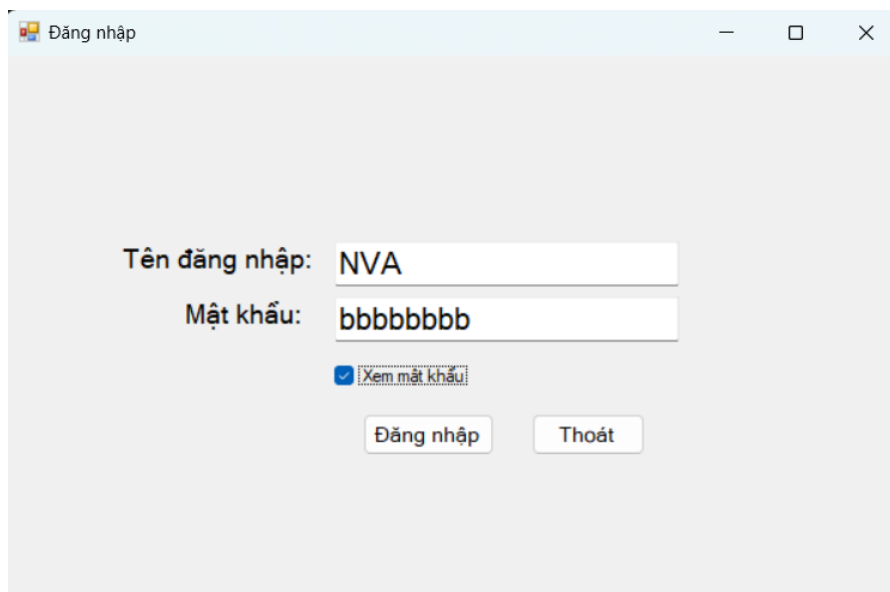
Câu f: Sử dụng công cụ SQL Profile để theo dõi thao tác đăng nhập và nhận xét

Bước 1: Mở màn hình đăng nhập



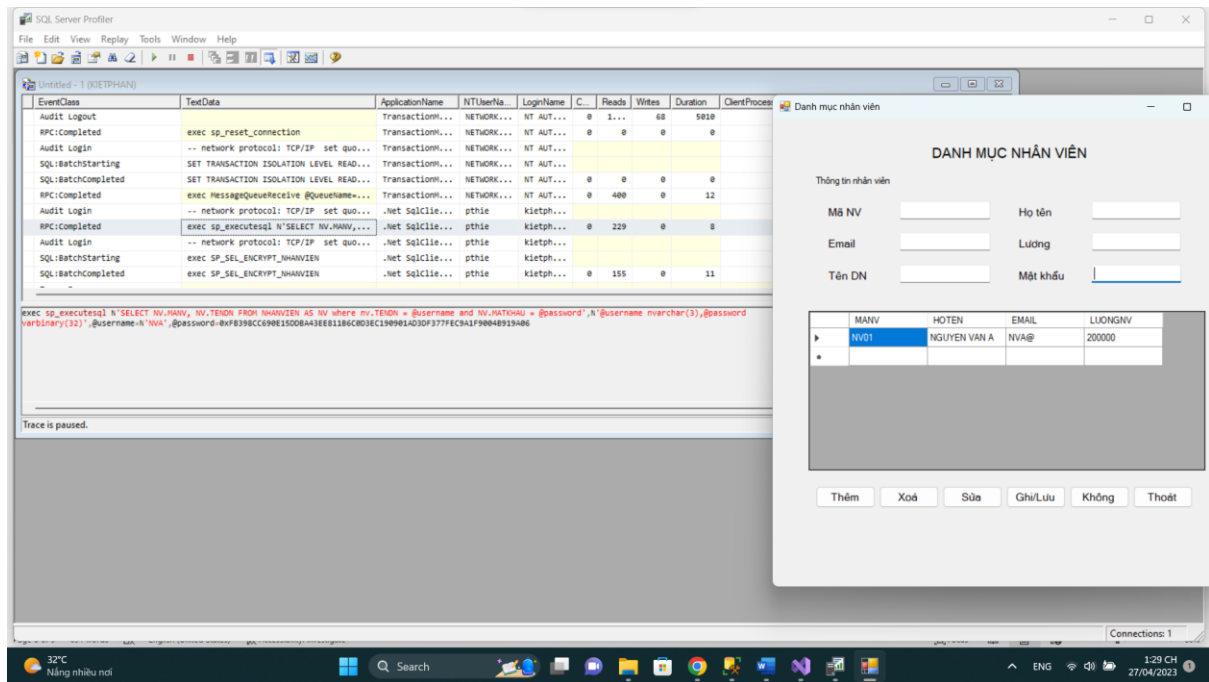
The screenshot shows a Windows-style window titled "Form1". Inside, there is a login form with the following elements: a label "Tên đăng nhập:" followed by a text input field; a label "Mật khẩu:" followed by a text input field; a checkbox labeled "Xem mật khẩu" which is currently unchecked; and two buttons at the bottom labeled "Đăng nhập" and "Thoát".

Bước 2: Nhập tên đăng nhập và mật khẩu



The screenshot shows the same login form, but the window title is now "Đăng nhập". The "Tên đăng nhập:" field contains the text "NVA" and the "Mật khẩu:" field contains "bbbbbbbb". The "Xem mật khẩu" checkbox is now checked, and the text "Xem mật khẩu" is highlighted with a dashed border. The "Đăng nhập" and "Thoát" buttons remain at the bottom.

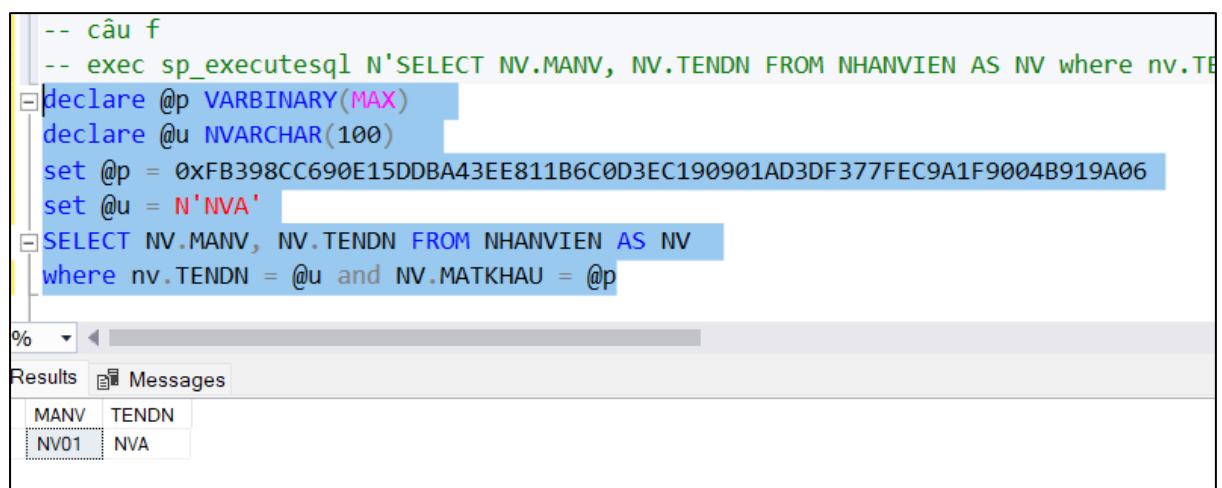
Bước 3: Sau khi nhấn nút đăng nhập và xem SQL profiler



Câu lệnh truy vấn trong SQL Profiler:

```
exec sp_executesql N'SELECT NV.MANV, NV.TENDN FROM NHANVIEN AS NV
where nv.TENDN = @username and NV.MATKHAU = @password',N'@username
nvarchar(3),@password
varbinary(32)',@username='NVA',@password=0xFB398CC690E15DDDBA43EE8
11B6C0D3EC190901AD3DF377FEC9A1F9004B919A06
```

Thực hiện câu lệnh đó trong SQL



Nhận xét:

Câu lệnh trên được thực hiện với thuộc tính MATKHAU được mã hoá thành chuỗi byte

'0xFB398CC690E15DDBA43EE811B6C0D3EC190901AD3DF377FEC9A1F9004B919A06' từ phía client. Ở bên phía server chỉ query xem có tồn tại hay không.

Câu g: Sử dụng công cụ SQL Profile để theo dõi load màn hình danh sách nhân viên và nhận xét

Màn hình danh sách nhân viên::

Danh mục nhân viên

DANH MỤC NHÂN VIÊN

Thông tin nhân viên

Mã NV Họ tên

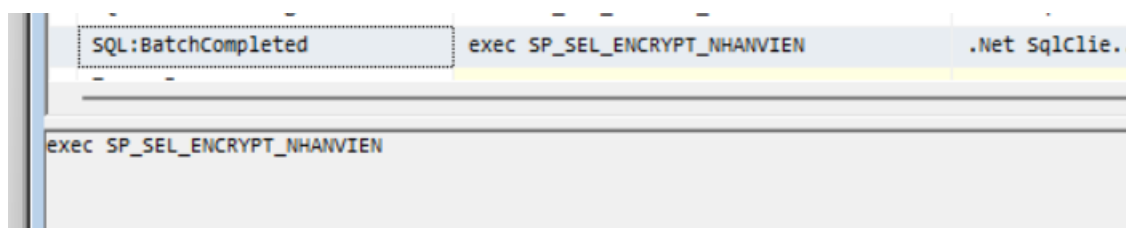
Email Lương

Tên DN Mật khẩu

	MANV	HOTEN	EMAIL	LUONGNV
▶	NV01	NGUYEN VAN A	NVA@	200000
*				

Thêm Xóa Sửa Ghi/Lưu Không Thoát

Màn hình SQL Profiler:



Câu lệnh truy vấn trong SQL Profiler:

```
exec SP_SEL_ENCRYPT_NHANVIEN
```

Thực hiện câu lệnh đó trong SQL

```
IF OBJECT_ID('SP_SEL_ENCRYPT_NHANVIEN','P') IS NOT NULL
DROP PROCEDURE SP_SEL_ENCRYPT_NHANVIEN
GO
CREATE PROCEDURE SP_SEL_ENCRYPT_NHANVIEN
AS
BEGIN
    SELECT NV.MANV, NV.HOTEN, NV.EMAIL, NV.LUONG as LUONG
    FROM NHANVIEN AS NV
END
GO
exec SP_SEL_ENCRYPT_NHANVIEN
-- Chuc nang chinh sua nhan vien
```

9 %

Results Messages

MANV	HOTEN	EMAIL	LUONG
NV01	NGUYEN VAN A	NVA@	0x8BC65D42D5CBA6ACFE41F74BFEECD67B

Nhận xét:

Câu lệnh truy vấn LUONG đã được mã hoá từ trước. Sau khi client nhận về thì mới được giải mã thành giá trị 200000

Câu h: Sử dụng công cụ SQL Profile để theo dõi thao tác thêm mới nhân viên nhân viên.và nhận xét

Màn hình danh sách nhân viên, tiến hành chọn nút “thêm”, sau đó nhập thông tin nhân viên và bấm nút ghi/lưu

Danh mục nhân viên

DANH MỤC NHÂN VIÊN

Thông tin nhân viên

Mã NV: NV02 Họ tên: B

Email: B@ Lương: 1000000

Tên DN: NVB Mật khẩu: ***

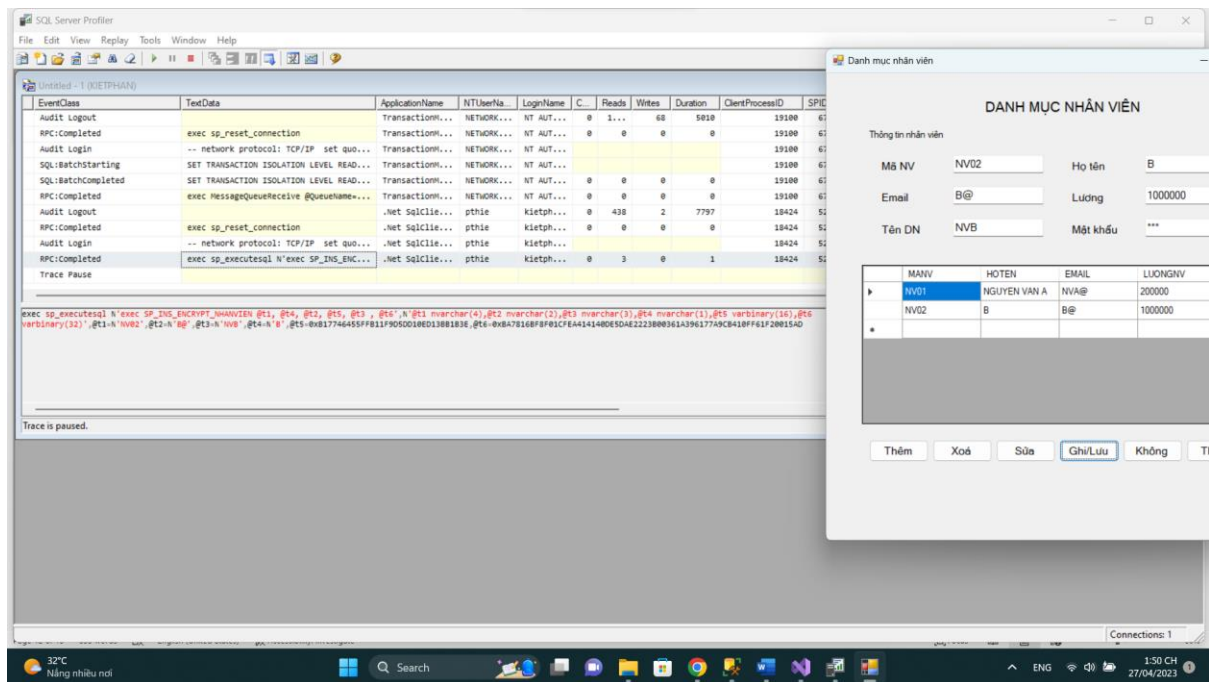
	MANV	HOTEN	EMAIL	LUONGNV
▶	NV01	NGUYEN VAN A	NVA@	200000
*				

Ghi/Lưu thành công.

OK

Thêm Xoá Sửa Ghi/Lưu Không Thoát

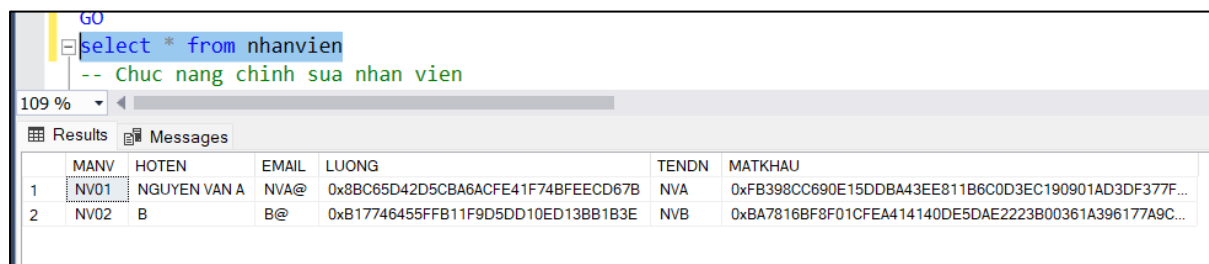
Màn hình SQL Profiler:



Câu lệnh truy vấn trong SQL Profiler:

```
exec sp_executesql N'exec SP_INS_ENCRYPT_NHANVIEN @t1, @t4, @t2, @t5, @t3, @t6', N'@t1 nvarchar(4),@t2 nvarchar(2),@t3 nvarchar(3),@t4 nvarchar(1),@t5 varbinary(16),@t6 varbinary(32)', @t1=N'NV02', @t2=N'B@', @t3=N'NVB', @t4=N'B', @t5=0xB17746455FFB11F9D5DD10ED13BB1B3E, @t6=0xBA7816BF8F01CFEA414140DE5DAE2223B00361A396177A9CB410FF61F20015AD
```

Thực hiện câu lệnh select bảng NHANVIEN trong SQL



Nhận xét:

Khi thêm mới nhân viên cột LUONG và MATKHAU đã được mã hoá ở phía client sau đó mới gửi đến Server để ghi xuống.

Ngoài ra, em cũng đã thêm cả chức năng xoá và chỉnh sửa nhân viên