

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ
KHOA CÔNG NGHỆ THÔNG TIN



BÁO CÁO LAB 04 – CÁ NHÂN

Bộ môn: Bảo mật cơ sở dữ liệu

Giảng viên lý thuyết: Nguyễn Đình Thúc

Giảng viên thực hành: Trần Ngọc Bảo

Nguyễn Thị Hương

Hồ Chí Minh, ngày 27 tháng 04 năm 2023

I. Tạo Database QLSV

```

--a)
CREATE DATABASE QLSV;
GO
USE QLSV;
GO

```

II. Tạo Table SINHVIEN, NHANVIEN, LOP

```
/*-----  
MASV:      20127318  
HO TEN:    Phan Trí Tài  
LAB:       04  
NGAY:      27/04/2023  
-----*/  
--b)  
  
CREATE TABLE SINHVIEN(  
    MASV NVARCHAR(20) NOT NULL ,  
    HOTEN NVARCHAR(20) NOT NULL ,  
    NGAYSINH DATETIME,  
    DIACHI NVARCHAR(200),  
    MALOP VARCHAR(20),  
    TENDN NVARCHAR(100) NOT NULL UNIQUE ,  
    MATKHAU VARBINARY(MAX) NOT NULL  
    CONSTRAINT PK_SINHVIEN PRIMARY KEY (MASV)  
);  
  
CREATE TABLE NHANVIEN(  
    MANV NVARCHAR(20) NOT NULL ,  
    HOTEN NVARCHAR(20) NOT NULL ,  
    EMAIL NVARCHAR(20),  
    LUONG VARBINARY(MAX) NOT NULL,  
    TENDN NVARCHAR(100) NOT NULL UNIQUE ,  
    MATKHAU VARBINARY(MAX) NOT NULL  
    CONSTRAINT PK_NHANVIEN PRIMARY KEY (MANV)  
);  
  
CREATE TABLE LOP(  
    MALOP VARCHAR(20) NOT NULL ,  
    TENLOP NVARCHAR(100) NOT NULL ,  
    MANV NVARCHAR(20) ,  
    CONSTRAINT PK_LOP PRIMARY KEY (MALOP)  
);  
  
ALTER TABLE LOP ADD CONSTRAINT FK_LOP_NHANVIEN FOREIGN KEY (MANV)  
REFERENCES NHANVIEN (MANV)  
  
ALTER TABLE SINHVIEN ADD CONSTRAINT FK_SINHVIEN_LOP FOREIGN KEY (MALOP)  
REFERENCES LOP (MALOP)
```

III. Stored procedure

a) SP_INS_ENCRYPT_SINHVIEN

```
/*-----*/
MASV:      20127318
HO TEN:    Phan Trí Tài
LAB:       04
NGAY:      27/04/2023
-----*/
--c)

--i)
--THEM SINH VIEN PROCEDURE

GO
CREATE OR ALTER PROCEDURE SP_INS_ENCRYPT_SINHVIEN(
    @MASV NVARCHAR(20),
    @HOTEN NVARCHAR(20),
    @NGAYSINH DATETIME,
    @DIACHI NVARCHAR(200),
    @MALOP VARCHAR(20),
    @TENDN NVARCHAR(100),
    @MATKHAU NVARCHAR(100)
) AS
BEGIN
    INSERT INTO SINHVIEN (MASV, HOTEN, NGAYSINH, DIACHI, MALOP, TENDN, MATKHAU)
    VALUES (@MASV, @HOTEN, @NGAYSINH, @DIACHI, @MALOP, @TENDN, CAST(@MATKHAU AS varbinary(max)))
END;
```

b) SP_INS_ENCRYPT_NHANVIEN

```
--ii)
-- THEM NHAN VIEN PROCEDURE

GO
CREATE OR ALTER PROCEDURE SP_INS_ENCRYPT_NHANVIEN(
    @MANV NVARCHAR(20),
    @HOTEN NVARCHAR(20),
    @EMAIL NVARCHAR(20),
    @LUONG VARCHAR(100),
    @TENDN NVARCHAR(100),
    @MATKHAU VARCHAR(MAX)
) AS
BEGIN
    INSERT INTO NHANVIEN (MANV, HOTEN, EMAIL, LUONG, TENDN, MATKHAU)
    VALUES (@MANV, @HOTEN, @EMAIL, CAST(@LUONG as varbinary(max)) , @TENDN, CAST(@MATKHAU as varbinary(max)))
END;
```

c) ENCRYPT_AES_256

```
/*-----*/
MASV:      20127318
HO TEN:    Phan Tri Tài
LAB:       04
NGAY:      27/04/2023
-----*/
--d)
-- XAC MINH TAI KHOAN SINH VIEN PROCEDURE

-- MÃ HÓA
GO
create symmetric key KEY_NHANVIEN
with algorithm = AES_256
encryption by password = '20127318';
GO
CREATE OR ALTER PROCEDURE ENCRYPT_AES_256(
    @LUONG INT
)
AS
BEGIN
    IF NOT EXISTS(
        SELECT * FROM sys.symmetric_keys
        WHERE name = 'KEY_NHANVIEN'
    )
    BEGIN
        create symmetric key KEY_NHANVIEN
        with algorithm = AES_256
        encryption by password = '20127318';
    END
    open symmetric key KEY_NHANVIEN
    decryption by password = '20127318';

    SELECT CAST(encryptbykey(key_guid('KEY_NHANVIEN'), cast(@LUONG as varchar)) as varbinary(max)) AS ENCRYPTVALUE
    close symmetric key KEY_NHANVIEN;
END
```

d) DECRYPT_AES_256

```
-- GIẢI MÃ
GO
CREATE OR ALTER PROCEDURE DECRYPT_AES_256(
    @LUONG VARBINARY(MAX)
)
AS
BEGIN
    open symmetric key KEY_NHANVIEN
    decryption by password = '20127318';
    SELECT CONVERT(VARCHAR, DecryptByKey(@LUONG)) AS DECRYPTVALUE;
    close symmetric key KEY_NHANVIEN;
END;
GO
```

e) SP_SEL_ENCRYPT_NHANVIEN

```
--SELECT NHAN VIEN
CREATE OR ALTER PROCEDURE SP_SEL_ENCRYPT_NHANVIEN
as
begin
    open symmetric key KEY_NHANVIEN
    decryption by password = '20127318';
    select MANV, HOTEN, EMAIL, LUONG, TENDN, MATKHAU
    from NHANVIEN
    close symmetric key KEY_NHANVIEN;
end;
```

f) SP_AUTHEN_SINHVIEN

```
-- XÁC THỰC TÀI KHOẢN SV
GO
CREATE OR ALTER PROCEDURE SP_AUTHEN_SINHVIEN(
    @TENDN NVARCHAR(100),
    @MATKHAU NVARCHAR(100)
)
AS
BEGIN
    select MASV, HOTEN, NGAYSINH, DIACHI, MALOP from SINHVIEN
    where TENDN = @TENDN and MATKHAU = @MATKHAU;
END;
```

g) SP_AUTHEN_NHANVIEN

```
-- XÁC THỰC TÀI KHOẢN NV
GO
CREATE OR ALTER PROCEDURE SP_AUTHEN_NHANVIEN(
    @TENDN NVARCHAR(100),
    @MATKHAU NVARCHAR(100)
)
AS
BEGIN
    select *
    from NHANVIEN
    where TENDN = @TENDN
        and MATKHAU = @MATKHAU
END;
```

IV. Insert dữ liệu

Trước khi insert dữ liệu thì chạy 2 dòng lệnh này để việc nhận Lương không xảy ra lỗi.

```
EXEC ENCRYPT_AES_256 3000
EXEC DECRYPT_AES_256 0x006B431D902D5F43A41739877B48ADA202000007F63545AFE0A740960C2E197E38C21E3478A15B3EB52294FDBBAD0694607A428
```

Sau đó lấy dữ liệu Lương đã đc giải mã bỏ vào insert nhân viên.

a) Insert nhân viên

```
--INSERT NHANVIEN
EXEC SP_INS_ENCRYPT_NHANVIEN
    'NV01', 'LE VAN A', 'NVA0', 0x006B431D902D5F43A41739877B48ADA202000007F63545AFE0A740960C2E197E38C21E3478A15B3EB52294FDBBAD0694607A428, 'NVA', 0x7C4A8D09CA3762AF61E595209430C26494F89418;
EXEC SP_INS_ENCRYPT_NHANVIEN
    'NV02', 'LE VAN B', 'NVB0', 0x006B431D902D5F43A41739877B48ADA202000007F63545AFE0A740960C2E197E38C21E3478A15B3EB52294FDBBAD0694607A428, 'NVB', 0x7C4A8D09CA3762AF61E595209430C26494F89418;
EXEC SP_INS_ENCRYPT_NHANVIEN
    'NV03', 'LE VAN C', 'NVC0', 0x006B431D902D5F43A41739877B48ADA202000007F63545AFE0A740960C2E197E38C21E3478A15B3EB52294FDBBAD0694607A428, 'NVC', 0x7C4A8D09CA3762AF61E595209430C26494F89418;
EXEC SP_INS_ENCRYPT_NHANVIEN
    'NV04', 'LE VAN D', 'NVD0', 0x006B431D902D5F43A41739877B48ADA202000007F63545AFE0A740960C2E197E38C21E3478A15B3EB52294FDBBAD0694607A428, 'NVD', 0x7C4A8D09CA3762AF61E595209430C26494F89418;
```

b) Insert lớp

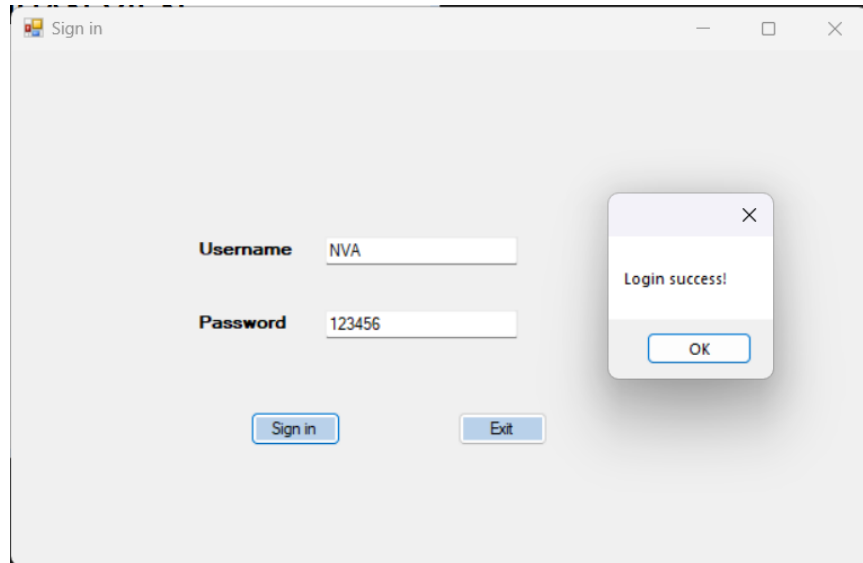
```
--INSERT LOP
INSERT INTO LOP (MALOP, TENLOP, MANV) VALUES ('19CTT4', N'K19 CNTT lớp 4', 'NV01');
INSERT INTO LOP (MALOP, TENLOP, MANV) VALUES ('19CNTN', N'CNTT Cử nhân tài năng', 'NV02');
INSERT INTO LOP (MALOP, TENLOP, MANV) VALUES ('20CTT3', N'K20 CNTT lớp 3', 'NV03');
INSERT INTO LOP (MALOP, TENLOP, MANV) VALUES ('20CLC', N'K20 CNTT CLC', 'NV04');
```

c) Insert sinh viên

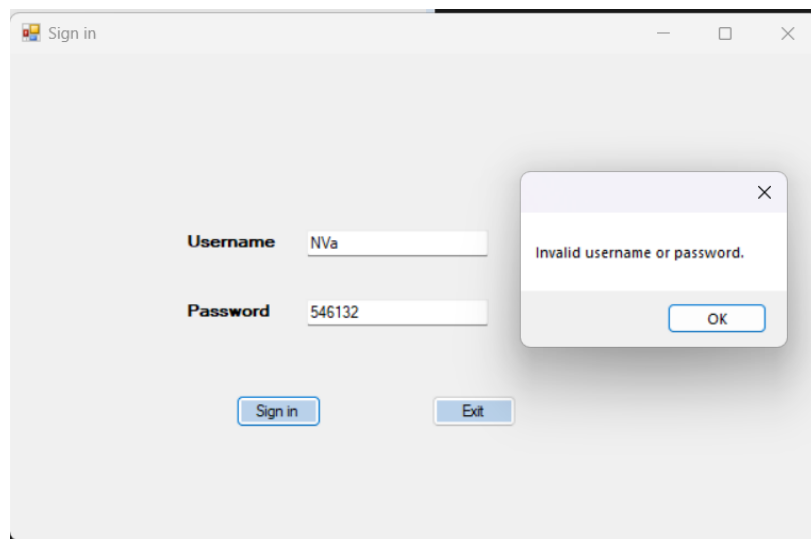
```
--INSERT SINHVIEN
EXEC SP_INS_ENCRYPT_SINHVIEN
    '20127318', N'PHAN TRÍ TÀI', '07/16/2002', N'NAM ĐỊNH', '20CLC', '20127318', 0x7C4A8D09CA3762AF61E59520943DC26494F8941B;
EXEC SP_INS_ENCRYPT_SINHVIEN
    'SV01', 'NGUYEN VAN A', '11/1/2001', '280 AN DUONG VUONG', '19CNTN', 'SVA', 0x7C4A8D09CA3762AF61E59520943DC26494F8941B;
EXEC SP_INS_ENCRYPT_SINHVIEN
    'SV02', 'NGUYEN VAN B', '07/12/2002', '280 AN DUONG VUONG', '20CTT3', 'SVB', 0x7C4A8D09CA3762AF61E59520943DC26494F8941B;
EXEC SP_INS_ENCRYPT_SINHVIEN
    'SV03', 'NGUYEN VAN C', '06/07/2001', '280 AN DUONG VUONG', '19CTT4', 'SVC', 0x7C4A8D09CA3762AF61E59520943DC26494F8941B;
```

V. Chạy chương trình

a) Đăng nhập



Đăng nhập hợp lệ



Đăng nhập không hợp lệ

b) Bảng danh sách nhân viên

The screenshot shows a web application window titled "Danh Sách Quản Lý NV". On the left is a sidebar with a list of employee IDs: NV01, NV02, NV03, and NV04. The main area is titled "DANH MỤC NHÂN VIÊN" and contains a form with the following fields:

Field	Value
Mã NV	NV01
Họ Tên	LE VAN A
Email	NVA@
Lương	3000
Username	NVA
Password	7c4a8d09ca3762af61e59520943

At the bottom of the form are two buttons: "Thêm" (Add) and "Lưu" (Save).

Nhân viên NVA

c) Thêm nhân viên mới

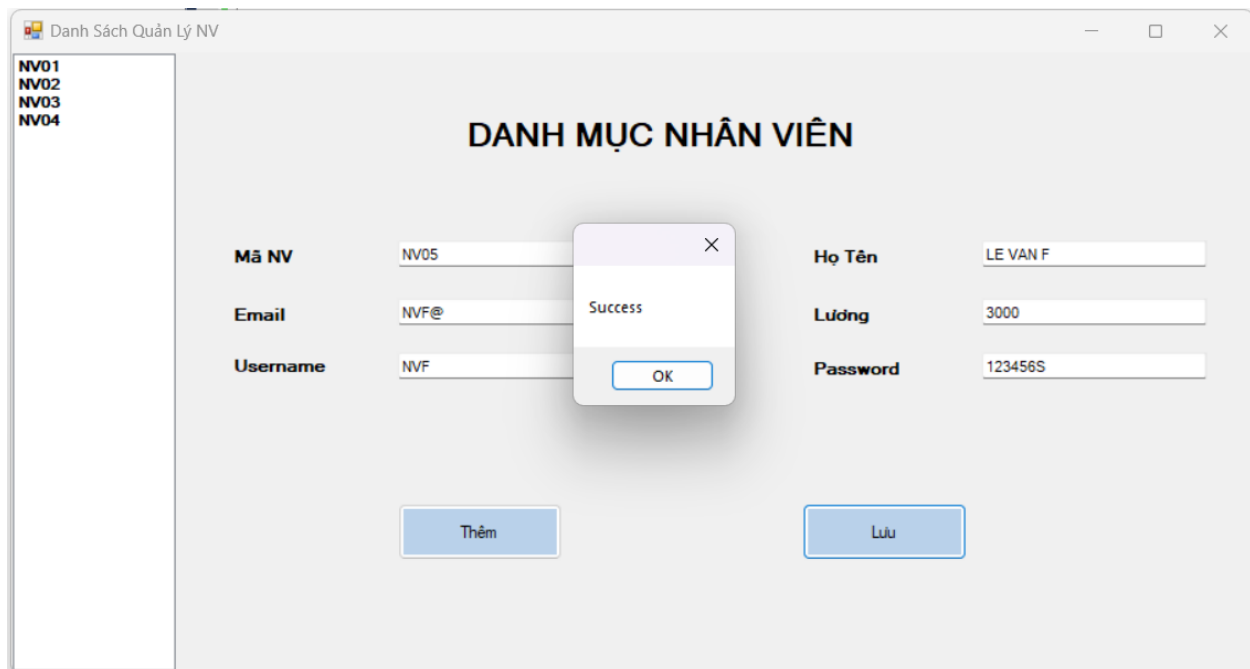
Bấm vào nút Thêm và nhập dữ liệu để thêm nhân viên mới .

This screenshot shows the same "Danh Sách Quản Lý NV" window, but with the "Thêm" button highlighted. The form fields are now populated with data for a new employee:

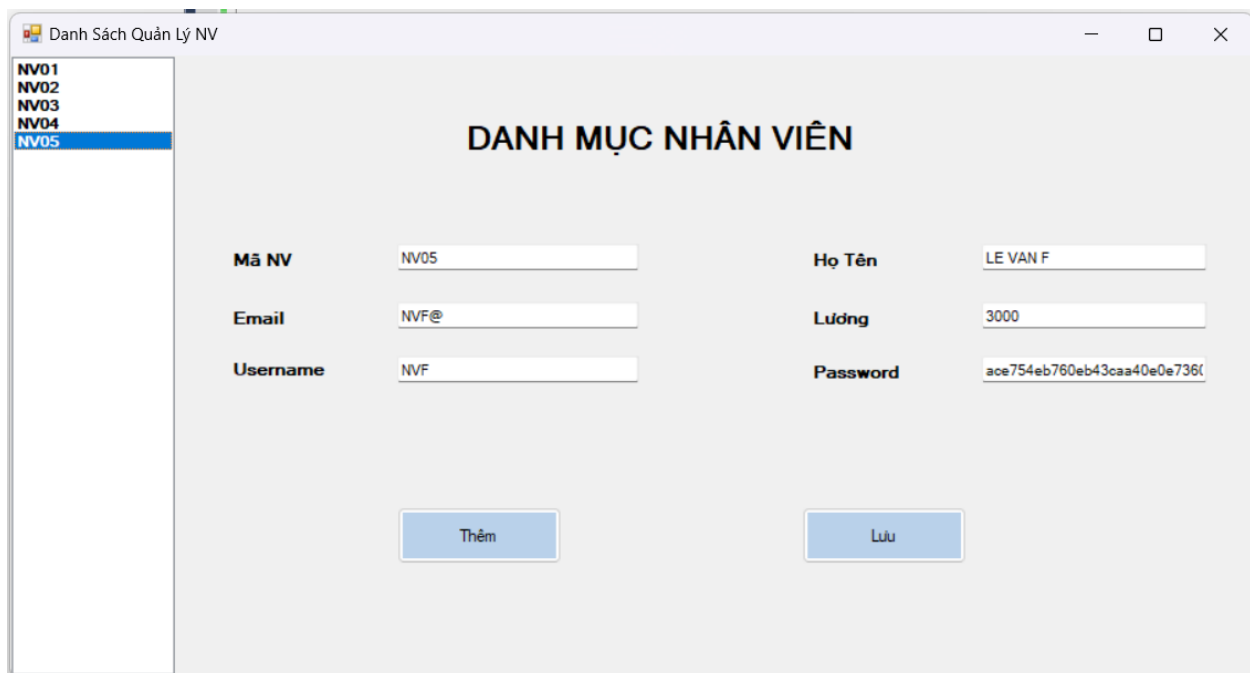
Field	Value
Mã NV	NV05
Họ Tên	LE VAN F
Email	NVF@
Lương	3000
Username	NVF
Password	123456S

The "Thêm" button is highlighted with a blue border, indicating it is the active element for adding a new employee.

Sau khi đã nhập dữ liệu thì bấm Lưu để lưu thông tin của nhân viên mới.



The screenshot shows a web application window titled "Danh Sách Quản Lý NV". On the left is a sidebar with a list of employee IDs: NV01, NV02, NV03, NV04, and NV05. The main area is titled "DANH MỤC NHÂN VIÊN" and contains a form with the following fields: "Mã NV" (NV05), "Email" (NVF@), "Username" (NVF), "Họ Tên" (LE VAN F), "Lương" (3000), and "Password" (123456S). A modal dialog box with the title "Success" and an "OK" button is centered over the form. At the bottom of the form are two buttons: "Thêm" and "Lưu".



This screenshot shows the same "Danh Mục Nhân Viên" form after the data has been saved. The "Mã NV" field remains "NV05", "Email" is "NVF@", and "Username" is "NVF". The "Họ Tên" field is "LE VAN F", "Lương" is "3000", and the "Password" field now displays a hashed value: "ace754eb760eb43caa40e0e736f". The "Thêm" and "Lưu" buttons are still present at the bottom. In the sidebar, the "NV05" item is now highlighted with a blue background, indicating it is the selected or active record.

Thế là bảng đã cập nhập nhân viên mới NV05.

VI. Sử dụng công cụ SQL Profile để theo dõi các thao tác với chương trình

a) Đăng nhập

EventClass	TextData	ApplicationName	NTUserName	LoginName	CPU	Reads	Writes	Duration	ClientProcessID	SPID	StartTime
Trace Start											2023-04-2
ExistingConnection	-- network protocol: LPC set quoted...	SQLServerCEIP	SQLTELE...	NT SER...					5812	51	2023-04-2
ExistingConnection	-- network protocol: LPC set quoted...	Microsoft SQ...	ADMIN	LAPTOP...					17236	52	2023-04-2
ExistingConnection	-- network protocol: LPC set quoted...	Microsoft SQ...	ADMIN	LAPTOP...					17236	54	2023-04-2
Audit Login	-- network protocol: LPC set quoted...	.Net SqlClie...	ADMIN	LAPTOP...					20304	55	2023-04-2
RPC:Completed	exec SP_AUTHEN_NHANVIEN @TENDN=N'NV4...	.Net SqlClie...	ADMIN	LAPTOP...	0	137	0	1	20304	55	2023-04-2
RPC:Completed	exec SP_AUTHEN_SINHVIEN @TENDN=N'NV4...	.Net SqlClie...	ADMIN	LAPTOP...	0	140	0	0	20304	55	2023-04-2
Audit Logout		.Net SqlClie...	ADMIN	LAPTOP...	0	277	0	52427	20304	55	2023-04-2
Audit Login	-- network protocol: LPC set quoted...	.Net SqlClie...	ADMIN	LAPTOP...					24740	58	2023-04-2
RPC:Completed	exec SP_AUTHEN_NHANVIEN @TENDN=N'NVA...	.Net SqlClie...	ADMIN	LAPTOP...	0	139	0	1	24740	58	2023-04-2
RPC:Completed	exec SP_AUTHEN_SINHVIEN @TENDN=N'NVA...	.Net SqlClie...	ADMIN	LAPTOP...	0	140	0	0	24740	58	2023-04-2
RPC:Completed	exec SP_SEL_ENCRYPT_NHANVIEN	.Net SqlClie...	ADMIN	LAPTOP...	0	57	0	1	24740	58	2023-04-2

exec SP_AUTHEN_NHANVIEN @TENDN=N'NVA',@MATKHAU=0x7C4A8D09CA3762AF61E59520943DC26494F8941B

Trace is running. Ln 10, Col 2 Rows: 12

EventClass	TextData	ApplicationName	NTUserName	LoginName	CPU	Reads	Writes	Duration	ClientProcessID	SPID	StartTime
SQL:BatchCompleted	SET DEADLOCK_PRIORITY -10	SQLServerCEIP	SQLTELE...	NT SER...	0	0	0	0	5812	51	2023-0
SQL:BatchStarting	if not exists (select * from sys.dm_...	SQLServerCEIP	SQLTELE...	NT SER...					5812	51	2023-0
SQL:BatchCompleted	if not exists (select * from sys.dm_...	SQLServerCEIP	SQLTELE...	NT SER...	0	20	0	1	5812	51	2023-0
Audit Logout		SQLServerCEIP	SQLTELE...	NT SER...	0	500	0	0	5812	51	2023-0
RPC:Completed	exec sp_reset_connection	SQLServerCEIP	SQLTELE...	NT SER...	0	0	0	0	5812	51	2023-0
Audit Login	-- network protocol: LPC set quoted...	SQLServerCEIP	SQLTELE...	NT SER...					5812	51	2023-0
SQL:BatchStarting	SET DEADLOCK_PRIORITY -10	SQLServerCEIP	SQLTELE...	NT SER...					5812	51	2023-0
SQL:BatchCompleted	SET DEADLOCK_PRIORITY -10	SQLServerCEIP	SQLTELE...	NT SER...	0	0	0	0	5812	51	2023-0
SQL:BatchStarting	DECLARE @msticks...	SQLServerCEIP	SQLTELE...	NT SER...					5812	51	2023-0
SQL:BatchCompleted	DECLARE @msticks...	SQLServerCEIP	SQLTELE...	NT SER...	47	1156	4	75	5812	51	2023-0
Audit Logout		.Net SqlClie...	ADMIN	LAPTOP...	0	436	0	225937	24740	58	2023-0
Audit Login	-- network protocol: LPC set quoted...	.Net SqlClie...	ADMIN	LAPTOP...					24612	57	2023-0
RPC:Completed	exec SP_AUTHEN_NHANVIEN @TENDN=N'SVA...	.Net SqlClie...	ADMIN	LAPTOP...	0	137	0	1	24612	57	2023-0
RPC:Completed	exec SP_AUTHEN_SINHVIEN @TENDN=N'SVA...	.Net SqlClie...	ADMIN	LAPTOP...	0	142	0	0	24612	57	2023-0

exec SP_AUTHEN_SINHVIEN @TENDN=N'SVA',@MATKHAU=0x7C4A8D09CA3762AF61E59520943DC26494F8941B

Trace is running. Ln 36, Col 1 Rows: 36

Nhận xét: Chương trình kiểm tra tài khoản nhân viên bằng SP_AUTHEN_NHANVIEN và tài khoản sinh viên bằng SP_AUTHEN_SINHVIEN.

EventClass	TextData	ApplicationName	NTUserName	LoginName	CPU	Reads	Writes	Duration	ClientProcessID	SPID	StartTime
RPC:Completed	exec sp_reset_connection	SQLServerCEIP	SQLTELE...	NT SER...	0	0	0	0		5812	51 2023-0-
Audit Login	-- network protocol: LPC set quoted...	SQLServerCEIP	SQLTELE...	NT SER...						5812	51 2023-0-
SQL:BatchStarting	SET DEADLOCK_PRIORITY -10	SQLServerCEIP	SQLTELE...	NT SER...						5812	51 2023-0-
SQL:BatchCompleted	SET DEADLOCK_PRIORITY -10	SQLServerCEIP	SQLTELE...	NT SER...	0	0	0	0		5812	51 2023-0-
SQL:BatchStarting	DECLARE @msticks...	SQLServerCEIP	SQLTELE...	NT SER...						5812	51 2023-0-
SQL:BatchCompleted	DECLARE @msticks...	SQLServerCEIP	SQLTELE...	NT SER...	47	1156	4	75		5812	51 2023-0-
Audit Logout		.Net SqlClie...	ADMIN	LAPTOP...	0	436	0	225937		24740	58 2023-0-
Audit Login	-- network protocol: LPC set quoted...	.Net SqlClie...	ADMIN	LAPTOP...						24612	57 2023-0-
RPC:Completed	exec SP_AUTHEN_NHANVIEN @TENDN=N'SVA...	.Net SqlClie...	ADMIN	LAPTOP...	0	137	0	1		24612	57 2023-0-
RPC:Completed	exec SP_AUTHEN_SINHVIEN @TENDN=N'SVA...	.Net SqlClie...	ADMIN	LAPTOP...	0	142	0	0		24612	57 2023-0-
Audit Logout		.Net SqlClie...	ADMIN	LAPTOP...	0	379	0	72740		24612	57 2023-0-
Audit Login	-- network protocol: LPC set quoted...	.Net SqlClie...	ADMIN	LAPTOP...						21960	57 2023-0-
RPC:Completed	exec SP_AUTHEN_NHANVIEN @TENDN=N'Nva...	.Net SqlClie...	ADMIN	LAPTOP...	0	137	0	1		21960	57 2023-0-
RPC:Completed	exec SP_AUTHEN_SINHVIEN @TENDN=N'Nva...	.Net SqlClie...	ADMIN	LAPTOP...	0	140	0	0		21960	57 2023-0-


```
exec SP_AUTHEN_SINHVIEN @TENDN=N'Nvaýf',@MATKHAU=0x01F7408F66F0C266FFC093C771ED71C59361BED0
```

Nhận xét: Đăng nhập sai thì vẫn sẽ gửi dữ liệu vào SP_AUTHEN_NHANVIEN và SP_AUTHEN_SINHVIEN để kiểm tra.

b) Thêm nhân viên mới

EventClass	TextData	ApplicationName	NTUserName	LoginName	CPU	Reads	Writes	Duration	ClientProcessID	SPID	StartTime
RPC:Completed	exec sp_reset_connection	SQLServerCEIP	SQLTELE...	NT SER...	0	0	0	0		5812	51 2023-0-
Audit Login	-- network protocol: LPC set quoted...	SQLServerCEIP	SQLTELE...	NT SER...						5812	51 2023-0-
SQL:BatchStarting	SET DEADLOCK_PRIORITY -10	SQLServerCEIP	SQLTELE...	NT SER...						5812	51 2023-0-
SQL:BatchCompleted	SET DEADLOCK_PRIORITY -10	SQLServerCEIP	SQLTELE...	NT SER...	0	0	0	0		5812	51 2023-0-
SQL:BatchStarting	if exists(select * from sys.server_e...	SQLServerCEIP	SQLTELE...	NT SER...						5812	51 2023-0-
SQL:BatchCompleted	if exists(select * from sys.server_e...	SQLServerCEIP	SQLTELE...	NT SER...	15	1518	0	11		5812	51 2023-0-
Audit Login	-- network protocol: LPC set quoted...	.Net SqlClie...	ADMIN	LAPTOP...						3932	55 2023-0-
RPC:Completed	exec SP_AUTHEN_NHANVIEN @TENDN=N'NVA...	.Net SqlClie...	ADMIN	LAPTOP...	0	139	0	1		3932	55 2023-0-
RPC:Completed	exec SP_AUTHEN_SINHVIEN @TENDN=N'NVA...	.Net SqlClie...	ADMIN	LAPTOP...	0	140	0	0		3932	55 2023-0-
RPC:Completed	exec SP_SEL_ENCRYPT_NHANVIEN	.Net SqlClie...	ADMIN	LAPTOP...	0	57	0	1		3932	55 2023-0-
RPC:Completed	exec DECRYPT_AES_256 @LUONG=0x006843...	.Net SqlClie...	ADMIN	LAPTOP...	0	26	0	0		3932	55 2023-0-
RPC:Completed	exec DECRYPT_AES_256 @LUONG=0x006843...	.Net SqlClie...	ADMIN	LAPTOP...	0	2	0	0		3932	55 2023-0-
RPC:Completed	exec ENCRYPT_AES_256 @LUONG=3000	.Net SqlClie...	ADMIN	LAPTOP...	0	661	0	4		3932	55 2023-0-
RPC:Completed	exec SP_INS_ENCRYPT_NHANVIEN @MAN=N...	.Net SqlClie...	ADMIN	LAPTOP...	0	248	0	2		3932	55 2023-0-


```
exec SP_INS_ENCRYPT_NHANVIEN @MAN=N'NV06',@HOTEN=N'LE VAN E',@EMAIL=N'NVE@',@LUONG=0x006843D902D5F43A41739877B48ADA202000000E45C1E105DB7D5B7DEB08D6DC1FAE032CF92E0752B438A864A008C2B1CEDBA10,@TENDN=N'NVE',@MATKHAU=0x7C4A8D09CA3762AF61E59
```

Nhận xét: Chương trình chạy ENCRYPT_AES_256 để mã hóa lương và SP_INS_ENCRYPT_NHANVIEN để thêm nhân viên mới.