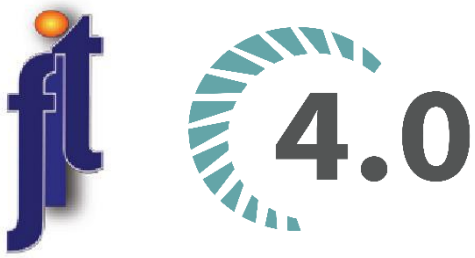
BỘ MÔN CÔNG NGHỆ TRI THỨC - KHOA CÔNG NGHỆ THÔNG TIN
ĐẠI HỌC KHOA HỌC TỰ NHIÊN - ĐẠI HỌC QUỐC GIA TP HCM



LAB #3 – CÁ NHÂN

DATABASE SECURITY

Giảng viên phụ trách:

PGS, TS. Nguyễn Đình Thúc

TS. Trần Ngọc Bảo

GV. Huỳnh Thanh Tâm

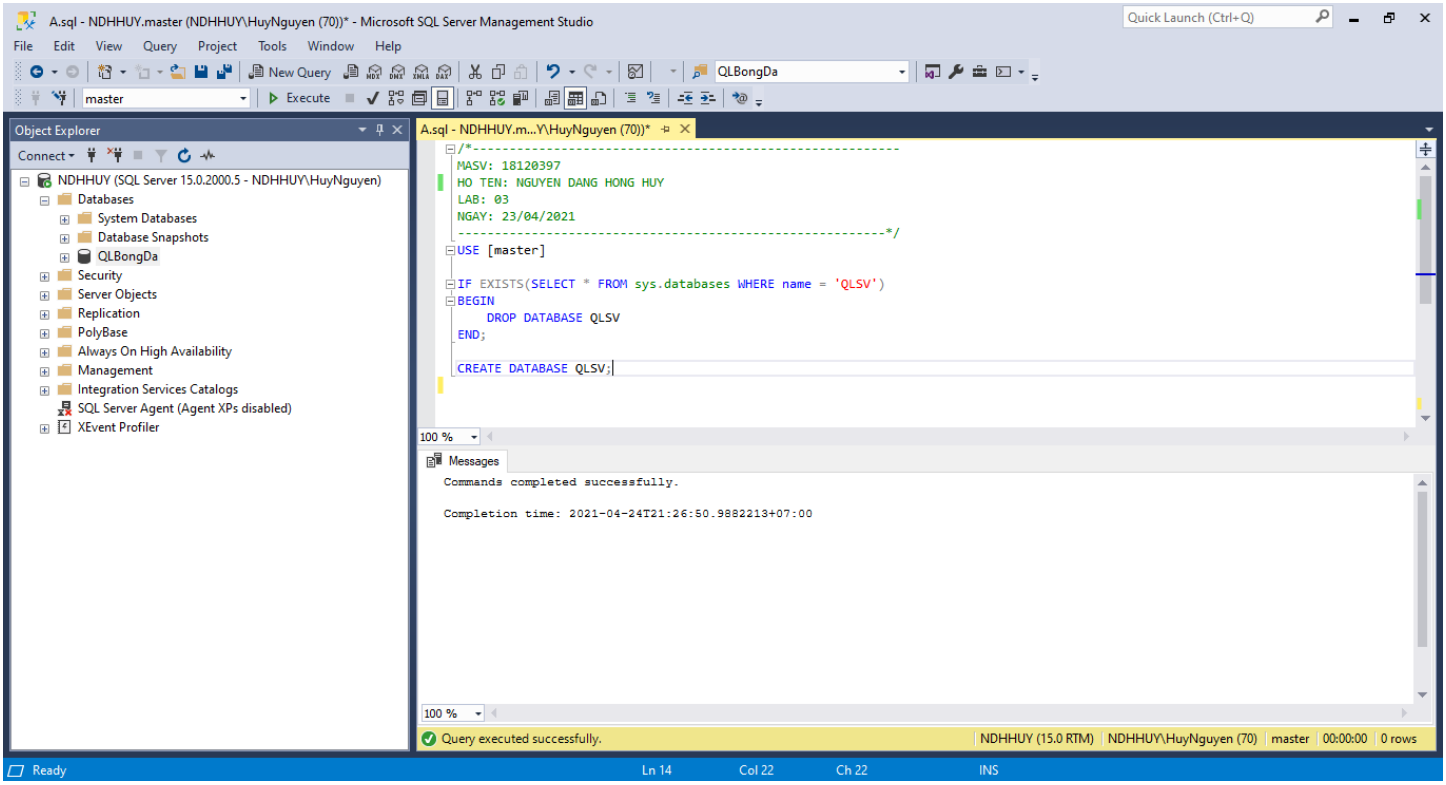
Sinh viên thực hiện:

18120397 – Nguyễn Đặng Hồng Huy

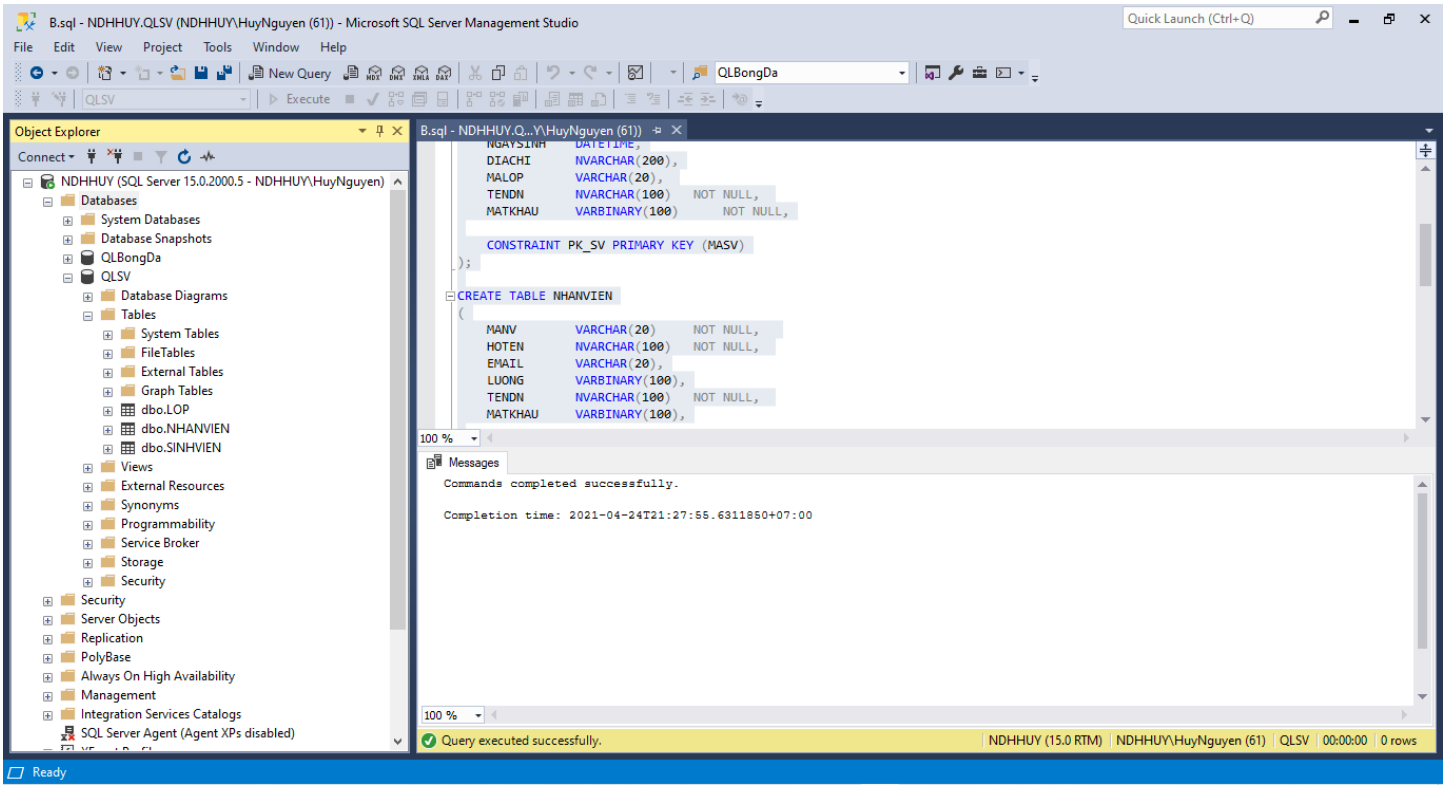
Học Kỳ 2 – Năm Học 2020-2021

Thành phố Hồ Chí Minh, tháng 04 năm 2021

CÂU A

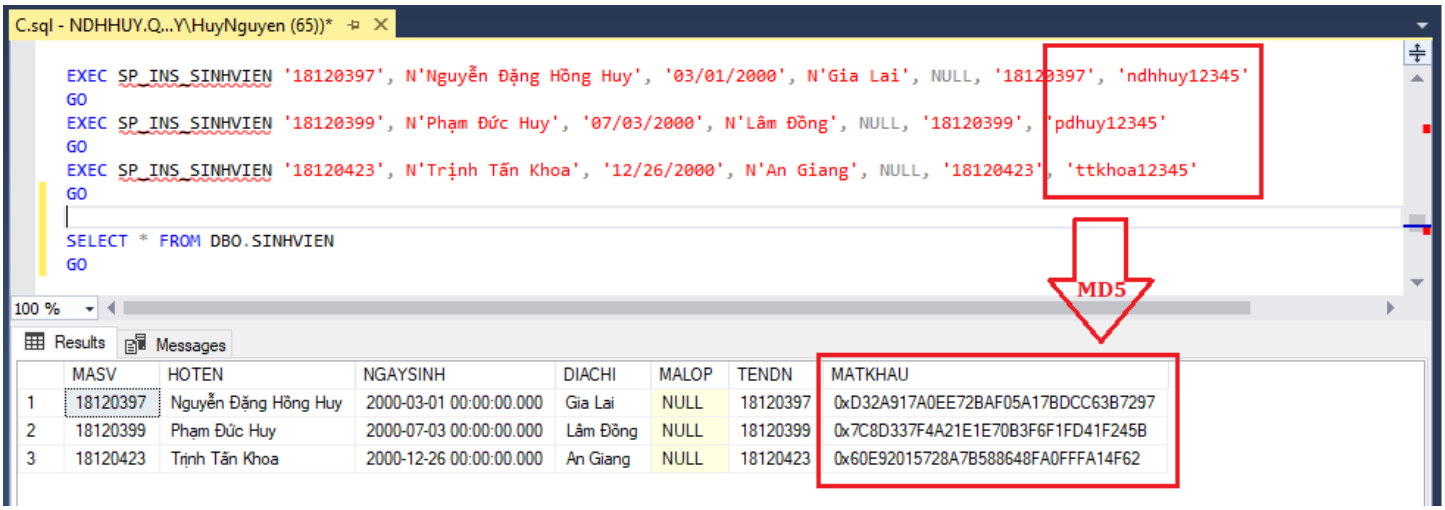

A.sql - NDHHUY.master (NDHHUY\HuyNguyen (70))* - Microsoft SQL Server Management Studio
Object Explorer
NDHHUY (SQL Server 15.0.2000.5 - NDHHUY\HuyNguyen)
Databases
System Databases
Database Snapshots
QLBongDa
Security
Server Objects
Replication
PolyBase
Always On High Availability
Management
Integration Services Catalogs
SQL Server Agent (Agent XPs disabled)
XEvent Profiler
/*----------
MASV: 18120397
HO TEN: NGUYEN DANG HONG HUY
LAB: 03
NGAY: 23/04/2021
----------*/
USE [master]
IF EXISTS(SELECT * FROM sys.databases WHERE name = 'QLSV')
BEGIN
DROP DATABASE QLSV
END;
CREATE DATABASE QLSV;
Commands completed successfully.
Completion time: 2021-04-24T21:26:50.9882213+07:00
Query executed successfully.
Ready

CÂU B


B.sql - NDHHUY.QLSV (NDHHUY\HuyNguyen (61)) - Microsoft SQL Server Management Studio
Object Explorer
NDHHUY (SQL Server 15.0.2000.5 - NDHHUY\HuyNguyen)
Databases
QLBongDa
QLSV
Database Diagrams
Tables
System Tables
FileTables
External Tables
Graph Tables
dbo.LOP
dbo.NHANVIEN
dbo.SINHVIEN
Views
External Resources
Synonyms
Programmability
Service Broker
Storage
Security
DIACHI NVARCHAR(200),
MALOP VARCHAR(20),
TENDN NVARCHAR(100) NOT NULL,
MATKHAU VARBINARY(100) NOT NULL,
CONSTRAINT PK_SV PRIMARY KEY (MASV)
);
CREATE TABLE NHANVIEN
(
MANV VARCHAR(20) NOT NULL,
HOTEN NVARCHAR(100) NOT NULL,
EMAIL VARCHAR(20),
LUONG VARBINARY(100),
TENDN NVARCHAR(100) NOT NULL,
MATKHAU VARBINARY(100),
Commands completed successfully.
Completion time: 2021-04-24T21:27:55.6311850+07:00
Query executed successfully.
Ready

CÂU C

SP_INS_SINHVIEN	Giải thích
CREATE PROCEDURE SP_INS_SINHVIEN @MASV NVARCHAR(20), @HOTEN NVARCHAR(100), @NGAYSINH DATETIME, @DIACHI NVARCHAR(200), @MALOP VARCHAR(20), @TENDN NVARCHAR(100), @MATKHAU VARCHAR(100) AS BEGIN SET NOCOUNT ON; DECLARE @MATKHAU_MD5 VARBINARY(100); SET @MATKHAU_MD5 = CONVERT(VARBINARY(100),HASHBYTES('MD5', @MATKHAU)); INSERT INTO DBO.SINHVIEN VALUES (@MASV, @HOTEN, @NGAYSINH, @DIACHI, @MALOP, @TENDN, @MATKHAU_MD5) END GO	Đầu vào: MASV, HOTEN, NGAYSINH, DIACHI, MALOP, TENDN, MATKHAU (chưa mã hóa) Cần mã hóa MATKHAU trước khi INSERT vào bảng dữ liệu • Dùng HASHBYTES ('<algorithhm>', {@input | 'input'} • '<algorithhm>' = MD5 • @input = @MATKHAU

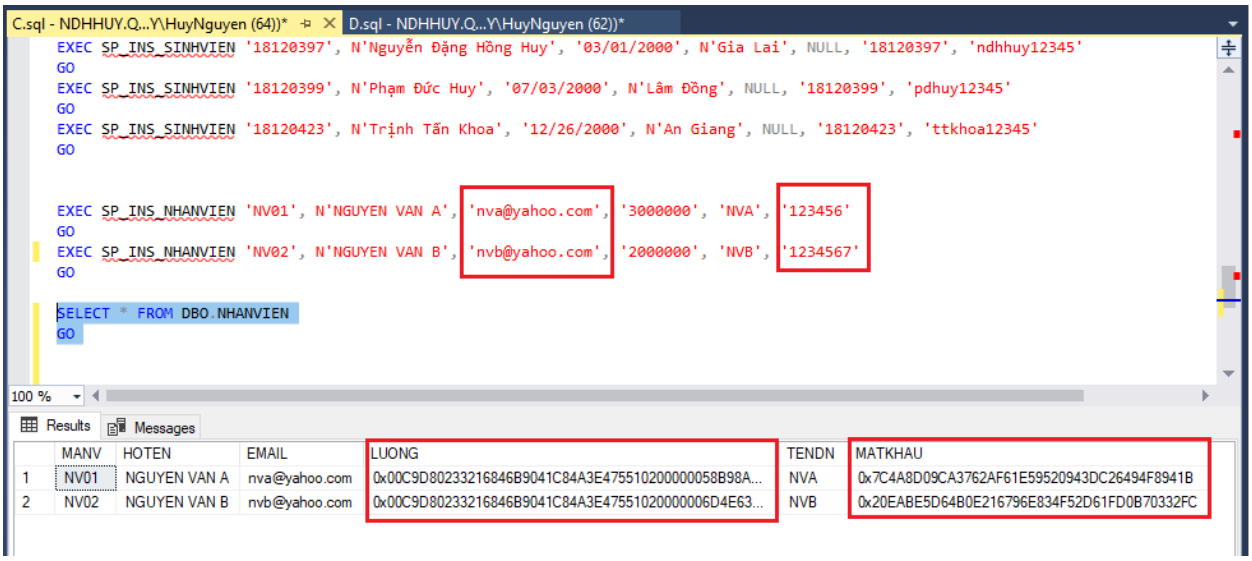


SP_INS_NHANVIEN	Giải thích
CREATE SYMMETRIC KEY SK WITH ALGORITHM = AES_256 ENCRYPTION BY PASSWORD = '18120397'; GO CREATE PROCEDURE SP_INS_NHANVIEN @MANV VARCHAR(20) , @HOTEN NVARCHAR(100), @EMAIL VARCHAR (20), @LUONG VARCHAR(100), @TENDN NVARCHAR(100), @MATKHAU VARCHAR(100) AS BEGIN SET NOCOUNT ON;	Đầu vào: MANV, HOTEN, EMAIL, LUONG (chưa mã hóa), TENDN, MATKHAU (chưa mã hóa) Mã hóa MATKHAU trước khi INSERT vào bảng dữ liệu: • Dùng HASHBYTES ('<algorithhm>', {@input | 'input'} • <algorithhm> = SHA1 • @input = @MATKHAU

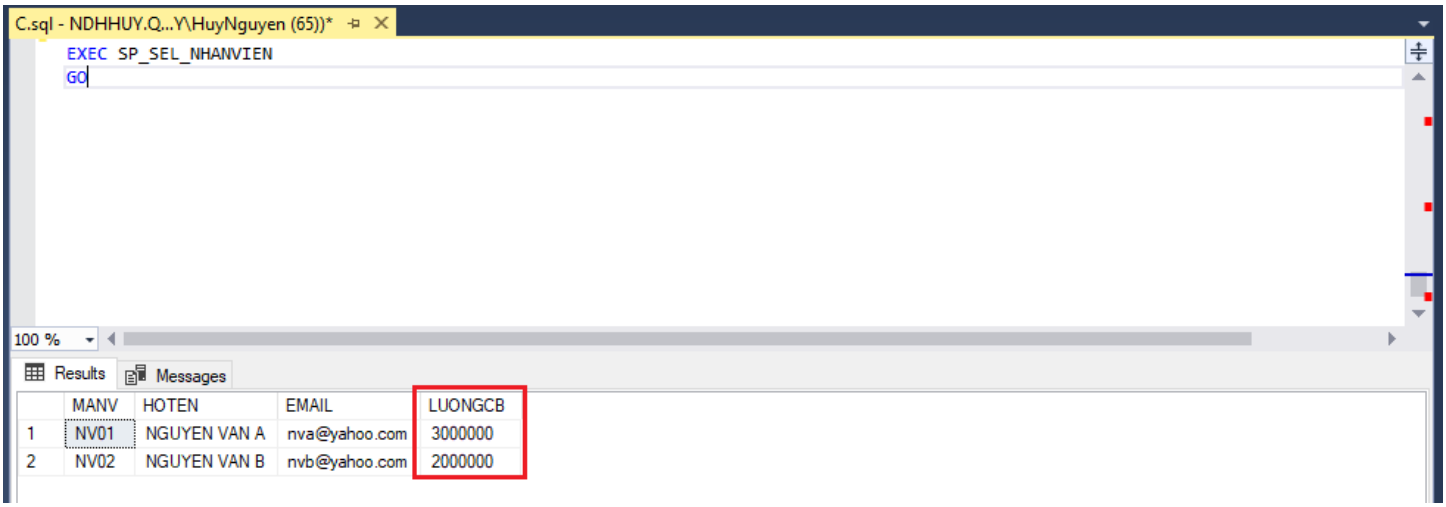
```
        OPEN SYMMETRIC KEY SK DECRYPTION BY PASSWORD = '18120397';

        DECLARE @MATKHAU_SHA1 VARBINARY(100);
        SET @MATKHAU_SHA1 =
CONVERT(VARBINARY(100),HASHBYTES('SHA1', @MATKHAU));

        DECLARE @LUONG_AES256 VARBINARY(100);
        SET @LUONG_AES256 = ENCRYPTBYKEY(KEY_GUID('SK'),
CONVERT(VARBINARY(100),@LUONG));

        INSERT INTO DBO.NHANVIEN
        VALUES (@MANV, @HOTEN, @EMAIL, @LUONG_AES256, @TENDN,
@MATKHAU_SHA1);

        CLOSE SYMMETRIC KEY SK;
END
GO
```

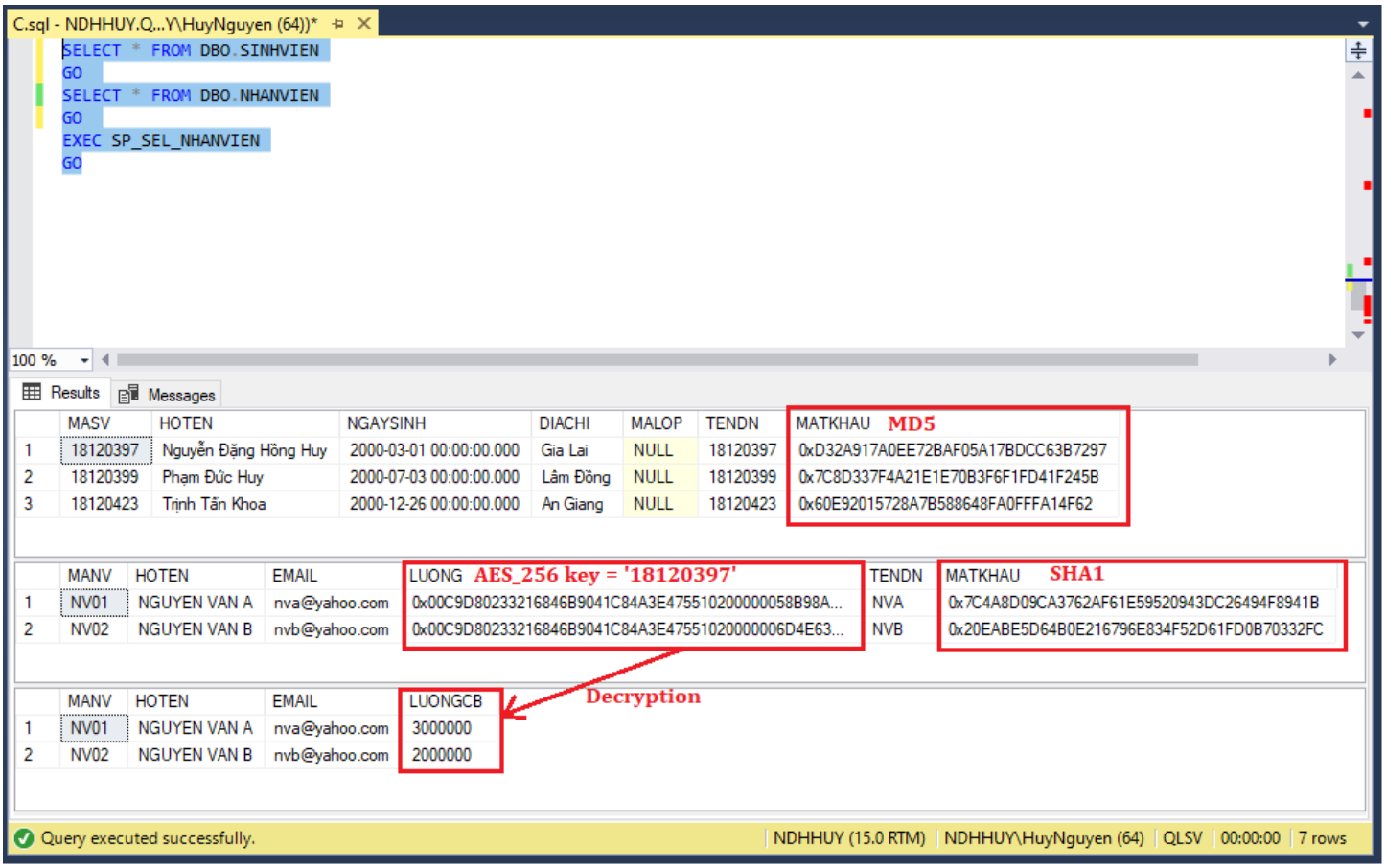
Mã hóa LUONG trước khi INSERT vào bảng dữ liệu:

- Tạo SYMMETRIC KEY
- ALGORITHM = AES_256
- ENCRYPTION BY PASSWORD = '18120397';
- Mở khóa giải mã hóa
- Dùng ENCRYPTBYKEY (KEY_GUID , { 'cleartext' | @cleartext })
- Đóng khóa giải mã hóa



SP_SEL_NHANVIEN	Giải thích
CREATE PROCEDURE SP_SEL_NHANVIEN AS BEGIN SET NOCOUNT ON; OPEN SYMMETRIC KEY SK DECRYPTION BY PASSWORD = '18120397'; SELECT MANV, HOTEN, EMAIL, CONVERT(VARCHAR(100), DECRYPTBYKEY(LUONG)) "LUONGCB" FROM NHANVIEN CLOSE SYMMETRIC KEY SK; END GO	• Mở khóa giải mã hóa • Dùng DECRYPTBYKEY(LUONG) để giải mã • Đóng khóa giải mã hóa

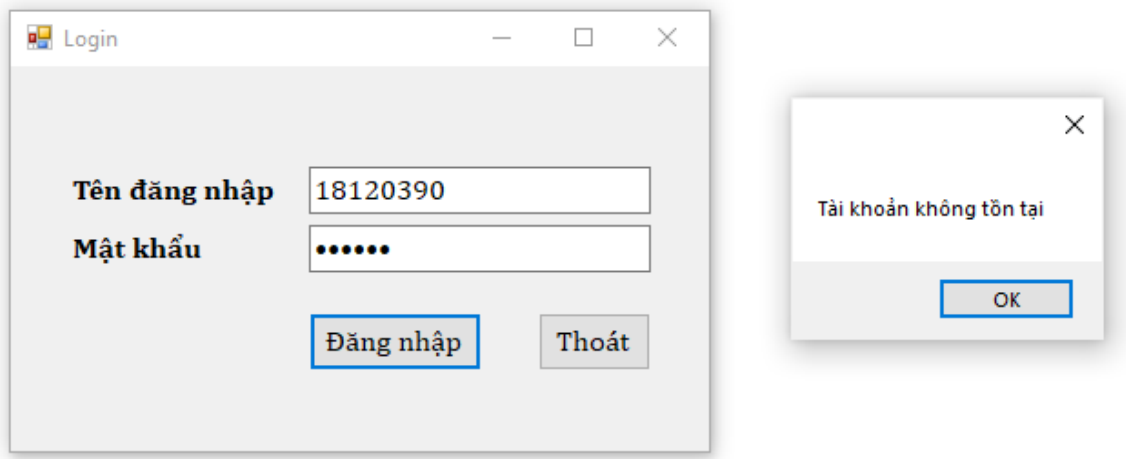

C.sql - NDHHUY.Q...Y\HuyNguyen (65))*
EXEC SP_SEL_NHANVIEN
GO
100 %
Results
Messages
MANV HOTEN EMAIL LUONGCB
1 NV01 NGUYEN VAN A nva@yahoo.com 3000000
2 NV02 NGUYEN VAN B nvb@yahoo.com 2000000


C.sql - NDHHUY.Q...Y\HuyNguyen (64))*
SELECT * FROM DBO.SINHVIEN
GO
SELECT * FROM DBO.NHANVIEN
GO
EXEC SP_SEL_NHANVIEN
GO
100 %
Results
Messages
MASV HOTEN NGAYSINH DIACHI MALOP TENDN MATKHAU MD5
1 18120397 Nguyễn Đặng Hồng Huy 2000-03-01 00:00:00.000 Gia Lai NULL 18120397 0xD32A917A0EE72BAF05A17BDCC63B7297
2 18120399 Phạm Đức Huy 2000-07-03 00:00:00.000 Lâm Đồng NULL 18120399 0x7C8D337F4A21E1E70B3F6F1FD41F245B
3 18120423 Trịnh Tấn Khoa 2000-12-26 00:00:00.000 An Giang NULL 18120423 0x60E92015728A7B588648FA0FFFA14F62
MANV HOTEN EMAIL LUONG AES_256 key = '18120397' TENDN MATKHAU SHA1
1 NV01 NGUYEN VAN A nva@yahoo.com 0x00C9D80233216846B9041C84A3E475510200000058B98A... NVA 0x7C4A8D09CA3762AF61E59520943DC26494F8941B
2 NV02 NGUYEN VAN B nvb@yahoo.com 0x00C9D80233216846B9041C84A3E475510200000006D4E63... NVB 0x20EABE5D64B0E216796E834F52D61FD0B70332FC
Decryption
MANV HOTEN EMAIL LUONGCB
1 NV01 NGUYEN VAN A nva@yahoo.com 3000000
2 NV02 NGUYEN VAN B nvb@yahoo.com 2000000
Query executed successfully.
NDHHUY (15.0 RTM) NDHHUY\HuyNguyen (64) QLSV 00:00:00 7 rows

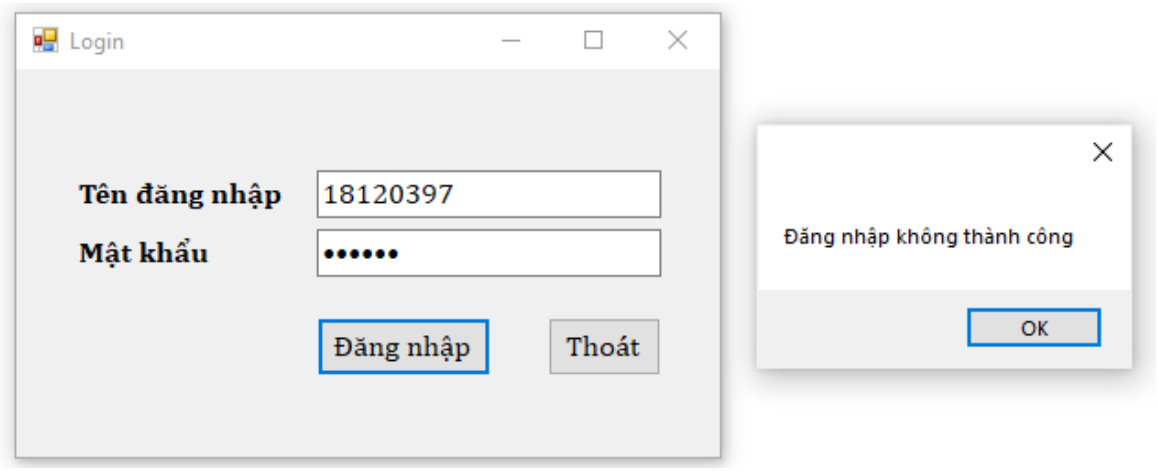
CÂU D

PROCEDURE SP_LOGIN	Giải thích

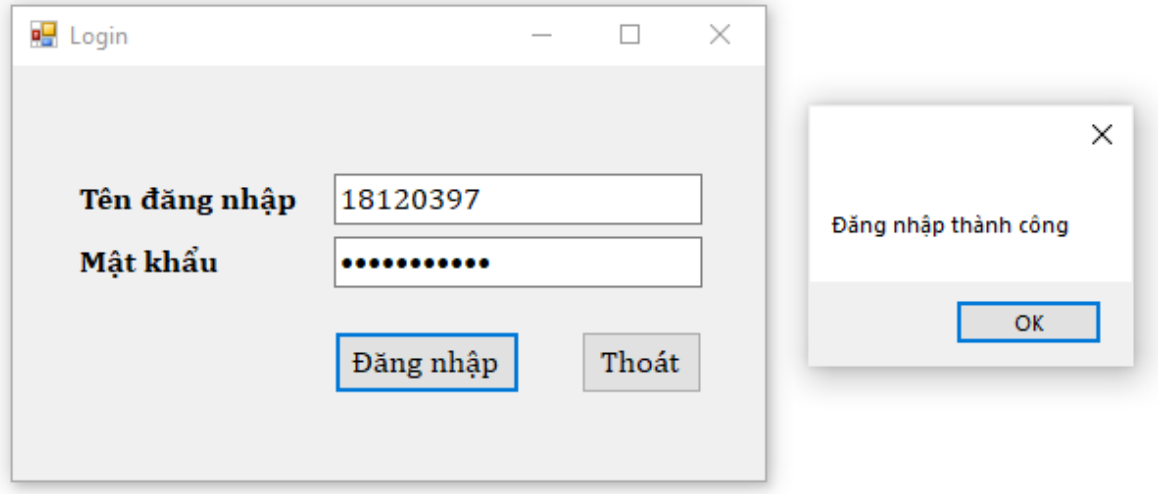
CREATE PROCEDURE SP_LOGIN @USERNAME NVARCHAR(100), @PASSWORD VARCHAR(100)
AS
BEGIN
DECLARE @MATKHAU VARBINARY(100);
IF EXISTS (SELECT TENDN FROM DBO.SINHVIEN WHERE TENDN = @USERNAME)
BEGIN
SET @MATKHAU = CONVERT(VARBINARY(100),HASHBYTES('MD5', @PASSWORD));
IF EXISTS (SELECT TENDN FROM DBO.SINHVIEN WHERE TENDN = @USERNAME AND MATKHAU = @MATKHAU)
BEGIN
PRINT N'Đăng nhập thành công'
END
ELSE
BEGIN
RAISERROR(N'Đăng nhập không thành công',16,1)
END
END
ELSE IF EXISTS (SELECT TENDN FROM DBO.NHANVIEN WHERE TENDN = @USERNAME)
BEGIN
SET @MATKHAU = CONVERT(VARBINARY(100),HASHBYTES('SHA1', @PASSWORD));
IF EXISTS (SELECT TENDN FROM DBO.NHANVIEN WHERE TENDN = @USERNAME AND MATKHAU = @MATKHAU)
BEGIN
PRINT N'Đăng nhập thành công'
END
ELSE
BEGIN
RAISERROR(N'Đăng nhập không thành công',16,1)
END
END
ELSE
BEGIN
RAISERROR(N'Tài khoản không tồn tại',16,1)
END
END
GO
	Kiểm tra NHANVIEN hay SINHVIEN với TENDN đó có tồn tại hay không?
	• Nếu không tồn tại thì báo lỗi không tồn tại.
	• Nếu tồn tại thì tiến hành mã hóa @PASSWORD theo thuật toán MD5(SINHVIEN) và SHA1(NHANVIEN). Tiếp theo kiểm tra trùng TENDN và MAKHAU hay không?
	▪ Nếu trùng thì đăng nhập thành công.
	▪ Ngược lại đăng nhập thất bại.



Trong bảng NHANVIEN và SINHVIEN không tồn tại TENDN = ‘18120390’



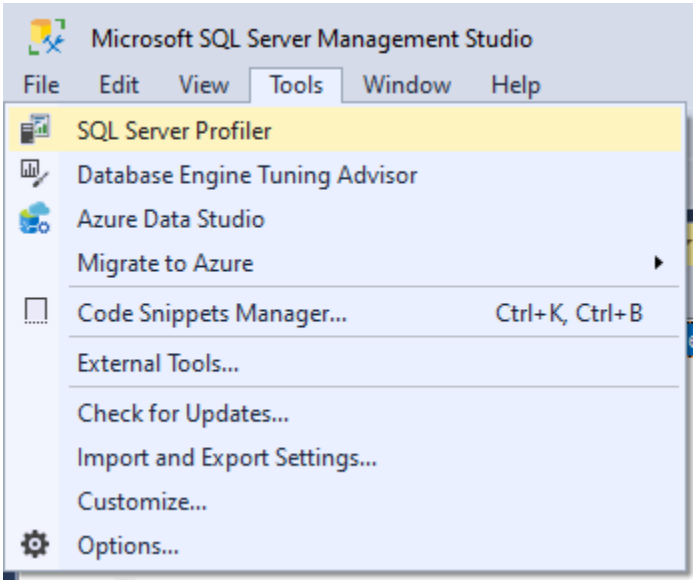
Trong bảng SINHVIEN có TENDN = ‘18120397’ nhưng MATKHAU không đúng



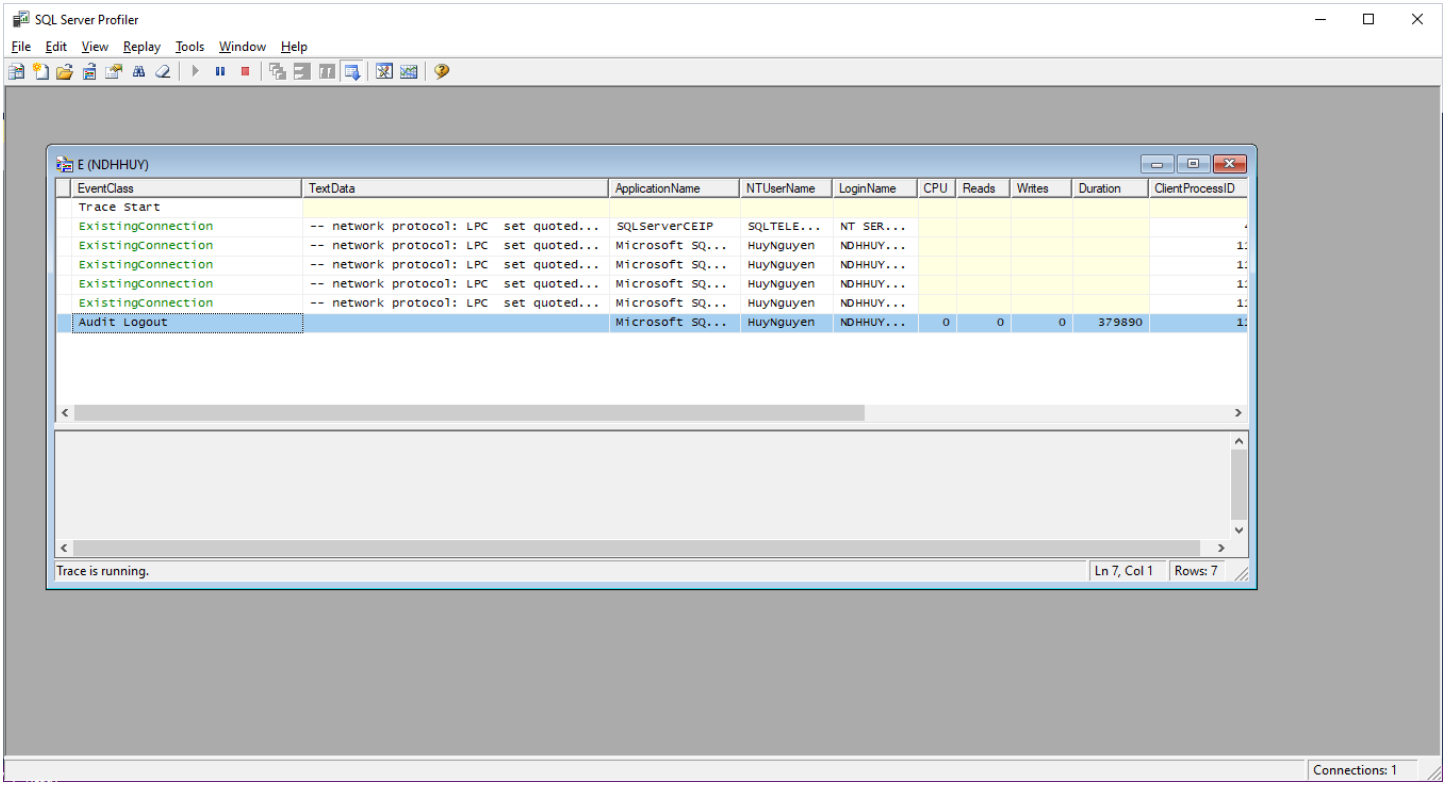
Trong bảng SINHVIEN có TENDN = ‘18120397’ và MATKHAU = HASH(‘**********’) đúng

CÂU E

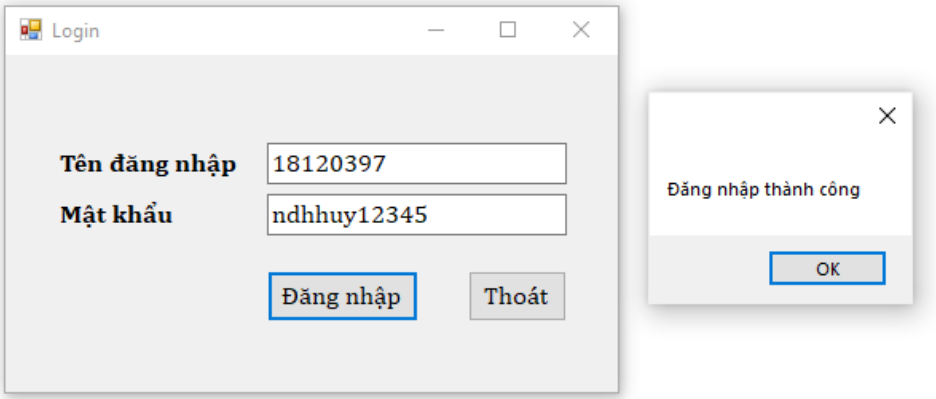
Bước 1: **Tools → SQl Server Profiler**



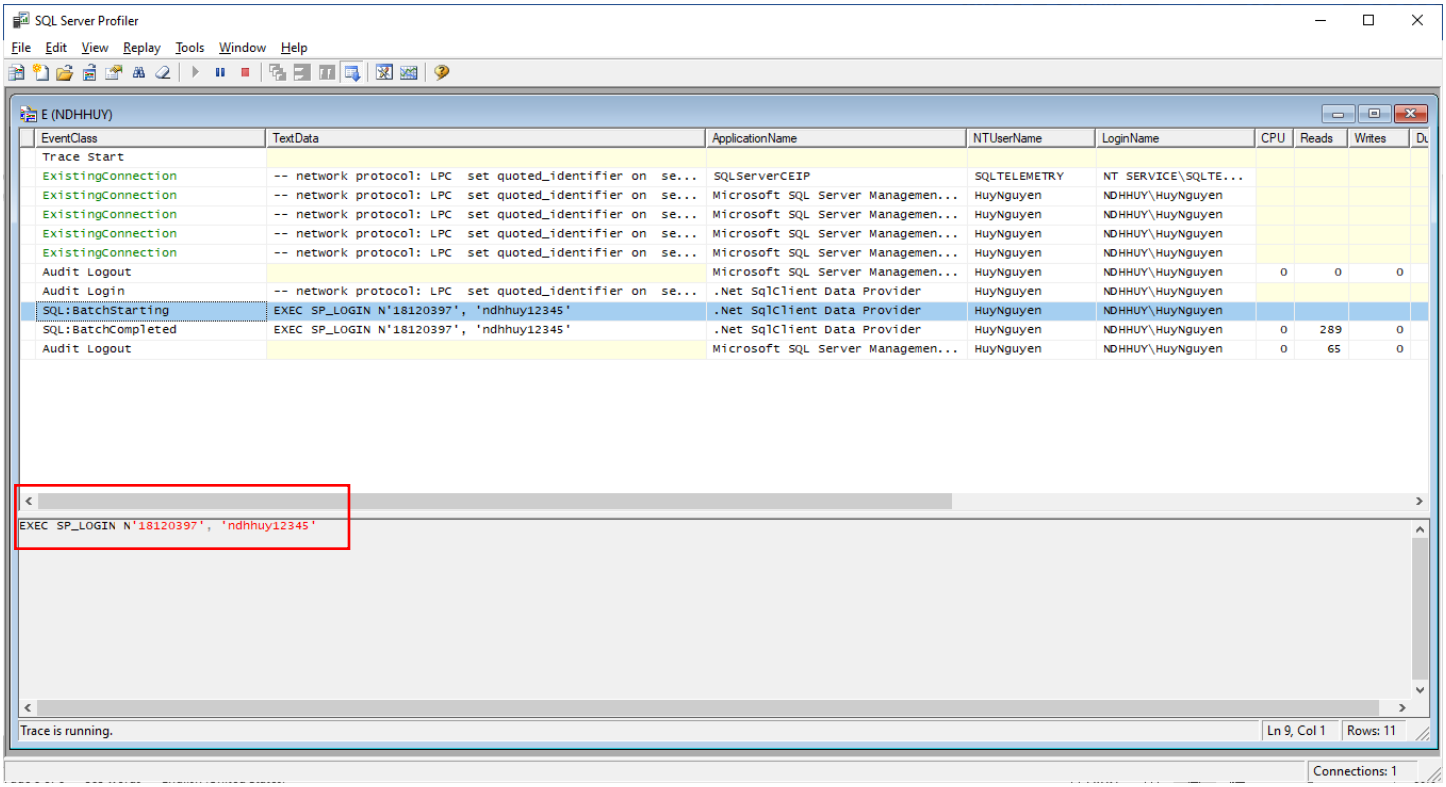
Bước 2: Đăng nhập **SQL Server**



Bước 3: Nhập **Tên đăng nhập – Mật khẩu** → Nhấn **Đăng nhập**



Bước 4: Quan sát



Nhận xét:

- Ghi nhật ký các truy cập vào cơ sở dữ liệu
- Thể hiện các thông tin:
  - Text data
  - Ứng dụng truy cập (.Net SqlClient Data Provider)
  - LonginName
  - Đọc/ghi dữ liệu, thời gian bắt đầu/kết thúc

- Tuy nhiên lại làm lộ thông tin đăng nhập của người dùng, do câu truy vấn không được mã hóa.