

# **BẢO MẬT CƠ SỞ DỮ LIỆU**

**Lab03 - Mã hóa dữ liệu sử dụng các thuật toán mã hóa  
đối xứng**

Sinh viên:

**Khúc Khánh Đăng – 20120262**

Giảng viên hướng dẫn :

**PSG.TS Nguyễn Đình Thúc**

**TS. Trần Bảo Ngọc**

**ThS. Nguyễn Thị Hương**



Khoa Công nghệ Thông tin  
Đại học Khoa học Tự nhiên TP HCM

## I. Tạo Database QLSV

```
use master
DROP DATABASE IF EXISTS QLSV
go
CREATE DATABASE QLSV
go
```

## II. Tạo các Table

```
USE QLSV

DROP TABLE IF EXISTS NHANVIEN
GO
CREATE TABLE NHANVIEN
(
    MANV VARCHAR(20) NOT NULL,
    HOTEN NVARCHAR(100) NOT NULL,
    EMAIL VARCHAR(20),
    LUONG VARBINARY(max),
    TENDN NVARCHAR(100) NOT NULL,
    MATKHAU VARBINARY(max) NOT NULL,
    CONSTRAINT PK_NV PRIMARY KEY (MANV)
)
DROP TABLE IF EXISTS SINHVIEN
GO
CREATE TABLE SINHVIEN
(
    MASV NVARCHAR(20) NOT NULL,
    HOTEN NVARCHAR(100) NOT NULL,
    NGAYSINH datetime,
    DIACHI NVARCHAR(200),
    MALOP VARCHAR(20),
    TENDN NVARCHAR(100) NOT NULL,
    MATKHAU VARBINARY(max) NOT NULL,
    CONSTRAINT PK_SV PRIMARY KEY (MASV)
)
DROP TABLE IF EXISTS LOP
GO
CREATE TABLE LOP
(
    MALOP VARCHAR(20),
    TEN NVARCHAR(100) NOT NULL,
    MANV VARCHAR(20)
    CONSTRAINT PK_L PRIMARY KEY (MALOP)
)
```

### III. Viết các Stored Procedure

**1.1. Stored dùng để thêm mới dữ liệu (Insert) vào table SINHVIEN, trong đó thuộc tính MATKHAU được mã hóa (HASH) sử dụng MD5.**

#### 1.1.1. Cài đặt

```
DROP PROCEDURE IF EXISTS SP_INS_SINHVIEN;
GO

CREATE PROC SP_INS_SINHVIEN(
    @MASV NVARCHAR(20),
    @HOTEN NVARCHAR(100),
    @NGAYSINH DATETIME,
    @DIACHI NVARCHAR(200),
    @MALOP VARCHAR(20),
    @TENDN NVARCHAR(100),
    @MATKHAU VARCHAR(32)
)
AS
BEGIN
    DECLARE @ENKEY VARBINARY(max);
    SET @ENKEY = CONVERT(VARBINARY, HASHBYTES('MD5', @MATKHAU));
    INSERT INTO SINHVIEN
    VALUES (@MASV, @HOTEN, @NGAYSINH, @DIACHI, @MALOP, @TENDN, @ENKEY)
END;
GO

EXEC SP_INS_SINHVIEN 'SV01', 'NGUYEN VAN A', '1/1/1990', '280 AN DUONG VUONG', 'CNTT-K35', 'NVA', '123456'
select * from SINHVIEN
GO
```

#### 1.1.2. Kết quả chạy

```

77 CREATE PROC SP_INS_SINHVIEN(
78     @MASV NVARCHAR(20),
79     @HOTEN NVARCHAR(100),
80     @NGAYSINH DATETIME,
81     @DIACHI NVARCHAR(200),
82     @MALOP VARCHAR(20),
83     @TENDN NVARCHAR(100),
84     @MATKHAU VARCHAR(32)
85 )
86 AS
87 BEGIN
88     DECLARE @ENKEY VARBINARY(max);
89     SET @ENKEY = CONVERT(VARBINARY, HASHBYTES('MD5', @MATKHAU));
90     INSERT INTO SINHVIEN
91     VALUES (@MASV, @HOTEN, @NGAYSINH, @DIACHI, @MALOP, @TENDN, @ENKEY)
92 END;
93 GO
94 EXEC SP_INS_SINHVIEN 'SV01', 'NGUYEN VAN A', '1/1/1990', '280 AN DUONG VUONG', 'CNTT-K35', 'NVA', '123456'
95 select * from SINHVIEN
96 GO

```

	MASV	HOTEN	NGAYSINH	DIACHI	MALOP	TENDN	MATKHAU
1	SV01	NGUYEN VAN A	1990-01-01 00:00:00.000	280 AN DUONG VUONG	CNTT-K35	NVA	0xE10ADC39436A59ABBE56E057F20F883E

**1.2. Stored dùng để thêm mới dữ liệu (Insert) vào table NHANVIEN, trong đó 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 mã số của sinh viên thực hiện bài Lab này.**

### 1.2.1. Tạo khóa

*Các đối tượng cần khởi tạo là Master key, Certificate và Symmetric key*

```
--tao MASTERKEY
IF NOT EXISTS
(
    SELECT*
    from sys.symmetric_keys
    WHERE symmetric_key_id = 101
)

CREATE MASTER KEY ENCRYPTION by
    PASSWORD = '20120262'
GO

--tao CERTIFICATE
IF NOT EXISTS
(
    SELECT*
    from sys.certificates
    WHERE name = 'MyCert'
)

CREATE CERTIFICATE myCert
    WITH SUBJECT = 'MyCert'
GO

--drop master key
--drop certificate myCert
--tao SYMMETRIC KEY
IF NOT EXISTS
(
    SELECT*
    from sys.symmetric_keys
    WHERE NAME = 'PriKey'
)

CREATE SYMMETRIC KEY PriKey
    WITH ALGORITHM = AES_256
    ENCRYPTION BY CERTIFICATE MyCert;
GO
```

### 1.2.2. Cài đặt

```

drop proc if EXISTS SP_INS_NHANVIEN
go

--SP_INS_NHANVIEN
CREATE PROCEDURE SP_INS_NHANVIEN
(
    @MANV VARCHAR(20),
    @HOTEN NVARCHAR(100),
    @EMAIL VARCHAR(20),
    @LUONG INT,
    @TENDN NVARCHAR(100),
    @MATKHAU VARCHAR(32)
)
AS
BEGIN
    OPEN SYMMETRIC KEY PriKey
    DECRYPTION BY CERTIFICATE MyCert;
    DECLARE @ENPASS varbinary(max);
    DECLARE @ENSAL varbinary(max);
    SET @ENPASS=CONVERT(varbinary, HashBytes('SHA1',@MATKHAU));
    SET @ENSAL = ENCRYPTBYKEY(KEY_GUID('PriKey'), CONVERT(varbinary(MAX), @LUONG))
    insert into NHANVIEN(MANV,HOTEN,EMAIL,LUONG,TENDN,MATKHAU)
    values (@MANV, @HOTEN, @EMAIL, @ENSAL, @TENDN,@ENPASS);
END

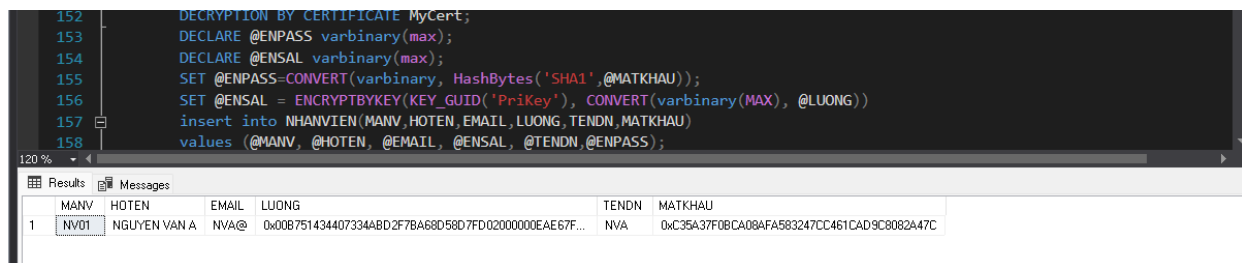
--drop procedure SP_INS_NHANVIEN
GO

GO

EXEC SP_INS_NHANVIEN 'NV01', 'NGUYEN VAN A', 'NVA@', 3000000, 'NVA', 'abcd12'
select * from nhanvien

```

### 1.2.3. Kết quả



	MANV	HOTEN	EMAIL	LUONG	TENDN	MATKHAU
1	NV01	NGUYEN VAN A	NVA@	0x00B751434407334ABD2F7BA68D58D7FD02000000EAE67F...	NVA	0xC35A37F0BCA08AFA583247CC461CAD9C8082A47C

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

### 1.3.1. Cài đặt

```

GO
DROP PROCEDURE IF EXISTS SP_SEL_NHANVIEN;
GO
CREATE PROC SP_SEL_NHANVIEN
AS
BEGIN
    OPEN SYMMETRIC KEY PriKey
    DECRYPTION BY CERTIFICATE MyCert;
    SELECT MANV, HOTEN, EMAIL, CONVERT(int, DECRYPTBYKEY(LUONG)) as LUONGCB
    FROM NHANVIEN
END

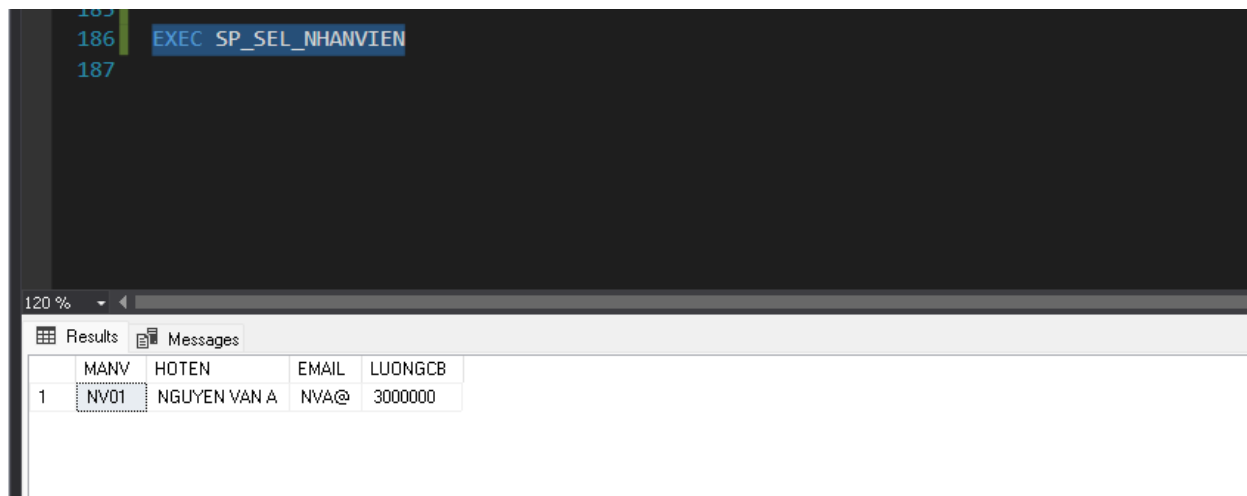
--drop procedure SP_SEL_NHANVIEN

GO

EXEC SP_SEL_NHANVIEN

```

### 1.3.2. Kết quả



	MANV	HOTEN	EMAIL	LUONGCB
1	NV01	NGUYEN VAN A	NVA@	3000000

**1.4. Viết màn hình quản lý đăng nhập hệ thống (sử dụng C#), cho phép nhập vào tên đăng nhập và mật khẩu (giả sử tên đăng nhập của sinh viên và nhân viên là duy nhất, nghĩa là tên đăng nhập của tất cả các sinh viên và tất cả nhân viên là khác nhau).**

#### 1.4.1. Procedure để kết nối và đăng nhập

```

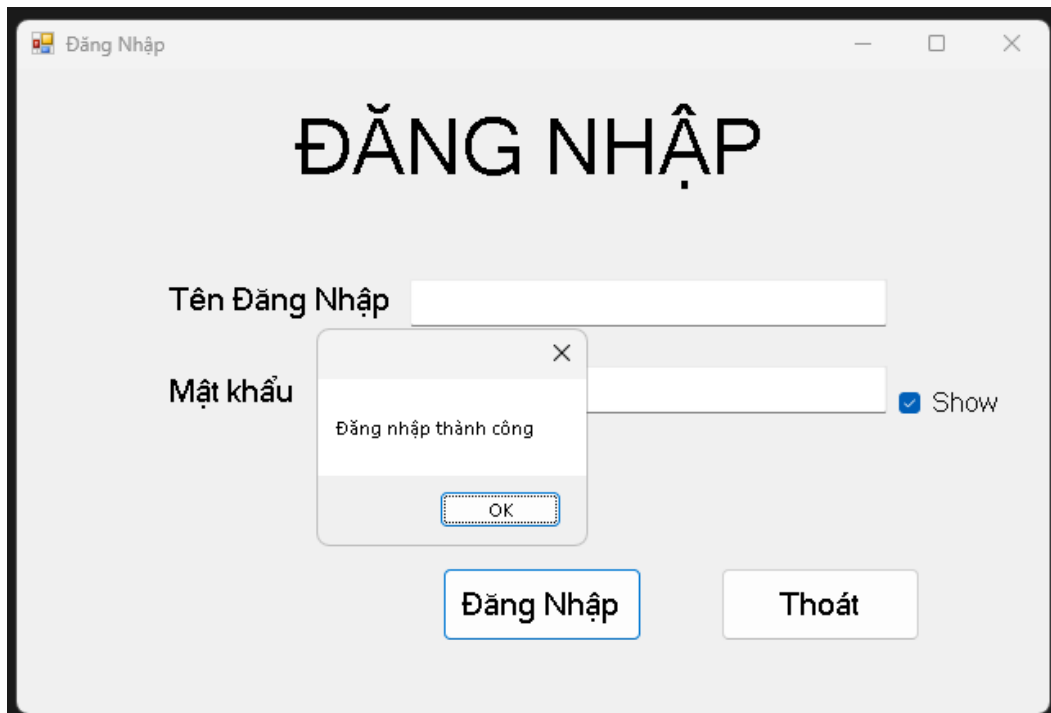
nap.sql - ... (DANG\ dangta (54)) # X
use QLSV
go
DROP PROCEDURE IF EXISTS SP_LOG_IN_
GO
--SP cho màn hình đăng nhập
create proc SP_LOG_IN_
(
    @TENDN nvarchar(100),
    @MATKHAU varchar(32)
)
As
Begin
    DECLARE @EnPassSHA1 varbinary(max);
    DECLARE @EnPassMD5 varbinary(max);
    DECLARE @COUNT INT;
    SET @EnPassSHA1=CONVERT(varbinary, HashBytes('SHA1',@MATKHAU));
    SET @EnPassMD5=CONVERT(varbinary, HashBytes('MD5',@MATKHAU));
    SET @COUNT = (SELECT COUNT(*) FROM NHANVIEN WHERE TENDN = @TENDN and MATKHAU = @EnPassSHA1)
    if @COUNT = 1
        BEGIN SELECT COUNT(*) FROM NHANVIEN WHERE TENDN = @TENDN and MATKHAU = @EnPassSHA1 RETURN END
    ELSE
        BEGIN SELECT COUNT(*) FROM SINHVIEN WHERE TENDN = @TENDN and MATKHAU = @EnPassMD5 END
    END
END
go

```

Khi xây dựng màn hình sẽ sử dụng procedure này để có thể kết nối đến tới database và tìm thông tin theo Username và Password đăng nhập.

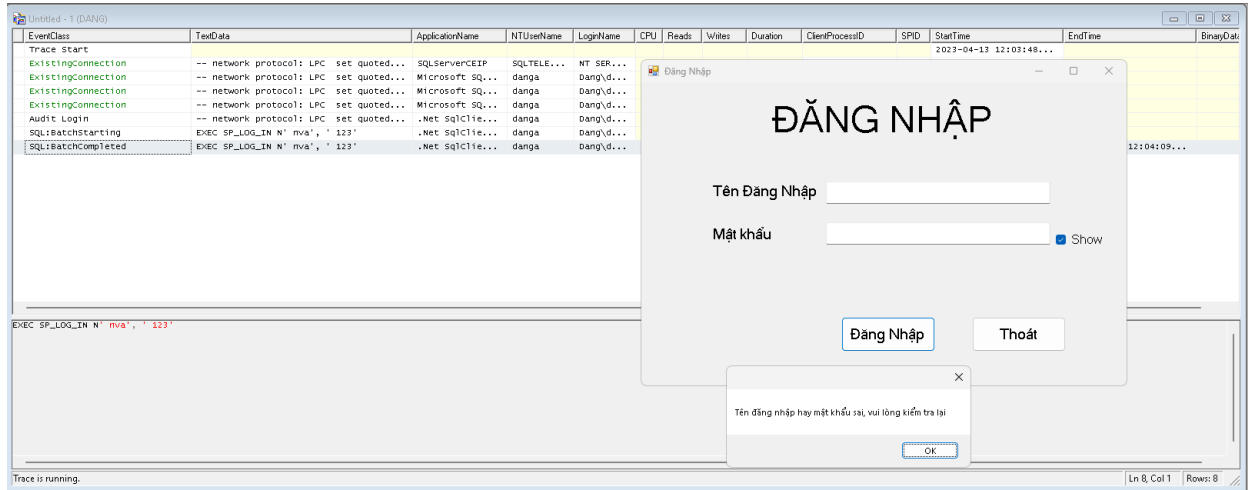
#### 1.4.2. Xây dựng màn hình đăng nhập



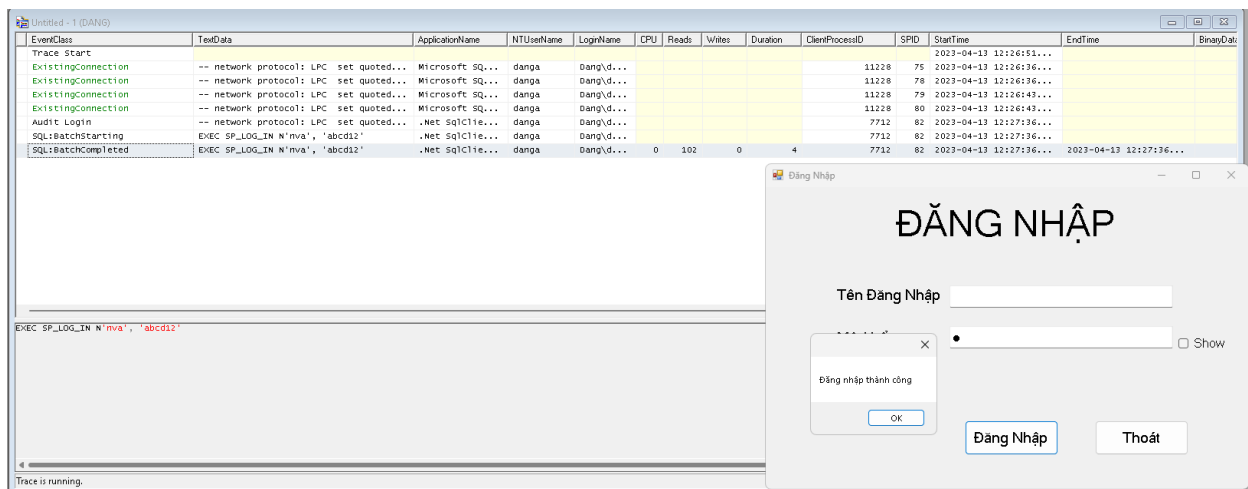


Sử dụng SQL Profile khi đăng nhập

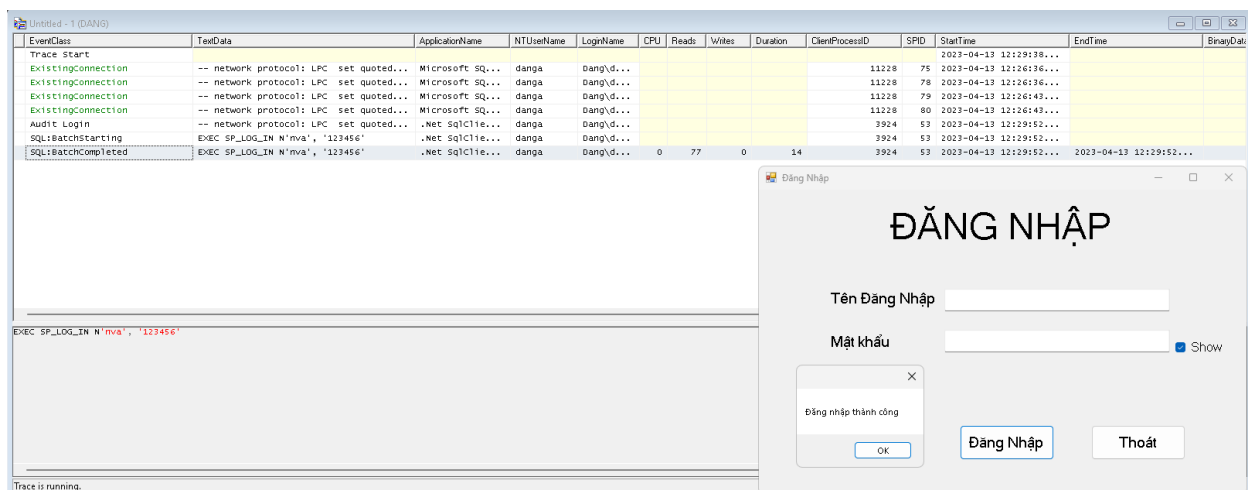
- Tài khoản hay mật khẩu sai



- Đăng nhập với tên đăng nhập và mật khẩu đúng
  - Với Nhân Viên



- Với Sinh Viên



- **Nhận xét:**
  - Người có quyền truy cập tới Tool SQL Server Profiler hoặc nghe trộm có thể thấy dữ liệu rõ giữa client và server gửi với nhau
  - Cần phải mã hóa dữ liệu ở cả hai chiều client và server