

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

KHOA CÔNG NGHỆ THÔNG TIN



# BÁO CÁO LAB 3: MÃ HÓA DỮ LIỆU SỬ DỤNG CÁC THUẬT TOÁN MÃ HÓA ĐỐI XỨNG

**MÔN BẢO MẬT CƠ SỞ DỮ LIỆU**

SINH VIÊN THỰC HIỆN:

20120335 – CÁI HỮU NGHĨA

Thành phố Hồ Chí Minh, tháng 4 năm 2023

# Mục lục

<b>I.</b>	<b>Thông tin chung.....</b>	<b>3</b>
	a/ Thông tin sinh viên.....	3
	b/ Đánh giá mức độ hoàn thành.....	3
<b>II.</b>	<b>Nội dung.....</b>	<b>4</b>
	1. Tạo cơ sở dữ liệu quản lý sinh viên: .....	4
	2. Tạo table cho cơ sở dữ liệu: .....	4
	3. Tạo stored procedure: .....	5
	4. Tạo màn hình đăng nhập:.....	8
<b>III.</b>	<b>Tài liệu tham khảo .....</b>	<b>13</b>

## I. Thông tin chung

a/ Thông tin sinh viên

Họ và tên	Mã số sinh viên
Cái Hữu Nghĩa	20120335

b/ Đánh giá mức độ hoàn thành

Mã số sinh viên	Họ và tên	Công việc	Mức độ hoàn thành
20120335	Cái Hữu Nghĩa	Tạo database quản lý sinh viên	100%
		Tạo table	100%
		Viết các stored procedure	100%
		Viết màn hình đăng nhập	100%
		Viết báo cáo	100%

## II. Nội dung

### 1. Tạo cơ sở dữ liệu quản lý sinh viên:

```
QLSV_20120335.sql...9AAA6\Admin (62))
/*--
Ma so sinh vien: 20120335
Ten: Cai Huu Nghia
Lab: 03
--*/
use master
go

if DB_ID('QLSV') IS NOT NULL
    drop database QLSV
go

create database QLSV
go

use QLSV
go
```

### 2. Tạo table cho cơ sở dữ liệu:

- Table SinhVien:

```
create table SINHVIEN
(
    MASV varchar(20) NOT NULL,
    HOTEN nvarchar(100) NOT NULL,
    NGAYSINH datetime,
    DIACHI nvarchar(200),
    MALOP varchar(20),
    TENDN nvarchar(100) NOT NULL,
    MATKHAU varbinary(100) NOT NULL,
    primary key(MASV)
)
go
```

- Table NhanVien:

```

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(100) NOT NULL,
    PUBKEY varchar(20),
    primary key(MANV)
)
go

```

- Table Lop:

```

create table LOP(
    MALOP varchar(20) NOT NULL,
    TENLOP nvarchar(100) NOT NULL,
    MANV varchar(20),
    primary key(MALOP)
)
go

```

### 3. Tạo stored procedure:

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

```

--stored procedure
/*SP_INS_NHANVIEN*/
IF OBJECT_ID('dbo.SP_INS_NHANVIEN','P') IS NOT NULL
    EXEC('DROP PROCEDURE SP_INS_NHANVIEN')
GO

CREATE PROCEDURE SP_INS_NHANVIEN(@MANV VARCHAR(20),
    @HOTEN NVARCHAR(100), @EMAIL VARCHAR(20), @LUONG VARCHAR(20),
    @TENDN nvarchar(100), @MATKHAU VARCHAR(20))
AS
BEGIN
    INSERT INTO NHANVIEN(MANV,HOTEN,EMAIL,LUONG,TENDN,MATKHAU)
    VALUES (@MANV, @HOTEN,@EMAIL,(select ENCRYPTBYKEY(KEY_GUID('PriKey'),@LUONG)),
    @TENDN,(select HASHBYTES ('SHA1',@MATKHAU)))
END;
GO

EXEC SP_INS_NHANVIEN 'NV01', 'NGUYEN VAN A', 'NVA@', '3000000', 'NVA', 'abcd12'
EXEC SP_INS_NHANVIEN 'NV02', 'NGUYEN VAN B', 'NVB@', '3000000', 'NVB', 'abcdef'
EXEC SP_INS_NHANVIEN 'NV03', 'NGUYEN VAN C', 'NVC@', '3000000', 'NVC', '123456'

select * from NHANVIEN

```

100 %

Results Messages

	MANV	HOTEN	EMAIL	LUONG	TENDN	MATKHAU	PUBKEY
1	NV01	NGUYEN VAN A	NVA@	0x00F3A4EA9978C74CB6472790F296E92B020000004DC9E7...	NVA	0xC35A37F0BCA08AFA583247CC461CAD9C8082A47C	NULL
2	NV02	NGUYEN VAN B	NVB@	0x00F3A4EA9978C74CB6472790F296E92B020000009E7439D...	NVB	0x1F8AC10F23C5B5BC1167BDA84B833E5C057A77D2	NULL
3	NV03	NGUYEN VAN C	NVC@	0x00F3A4EA9978C74CB6472790F296E92B020000001B7B6C...	NVC	0x7C4A8D09CA3762AF61E59520943DC26494F8941B	NULL

⇒ Kết quả: MATKHAU đã được mã hóa thành công.

- 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.

```

/* .SP_INS_SINHVIEN*/
IF OBJECT_ID('dbo.SP_INS_SINHVIEN','P') IS NOT NULL
    EXEC('DROP PROCEDURE SP_INS_SINHVIEN')
GO

CREATE PROCEDURE SP_INS_SINHVIEN(@MASV NVARCHAR(20),
    @HOTEN NVARCHAR(100),
    @NGAYSINH DATETIME,
    @DIACHI NVARCHAR(200),
    @MALOP VARCHAR(20),
    @TENDN NVARCHAR(100),
    @MATKHAU NVARCHAR(20))
AS
BEGIN
    INSERT INTO SINHVIEN(MASV,HOTEN,NGAYSINH,DIACHI,MALOP,TENDN,MATKHAU)
    VALUES (@MASV, @HOTEN,@NGAYSINH,@DIACHI,@MALOP,@TENDN,
    (SELECT HASHBYTES ('MD5',@MATKHAU)))
END;
GO

EXEC SP_INS_SINHVIEN 'SV01', 'NGUYEN VAN A', '1/1/1990', '280 AN
DUONG VUONG', 'CNTT-K35', 'NVA', '123456'

select* from SINHVIEN

```

⇒ Kết quả thu được: MATKHAU được mã hóa thành công.

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

```

/*SP_SEL_NHANVIEN*/
IF OBJECT_ID('dbo.SP_SEL_NHANVIEN','P') IS NOT NULL
    EXEC('DROP PROCEDURE SP_SEL_NHANVIEN')
GO
CREATE PROCEDURE SP_SEL_NHANVIEN
AS
BEGIN
    SELECT MANV,HOTEN,EMAIL, convert(varchar, DECRYPTBYKEY(LUONG))
    FROM NHANVIEN
END;
GO

EXEC SP_SEL_NHANVIEN

```

100 %

Results

Messages

	MANV	HOTEN	EMAIL	(No column name)
1	NV01	NGUYEN VAN A	NVA@	3000000
2	NV02	NGUYEN VAN B	NVB@	3000000
3	NV03	NGUYEN VAN C	NVC@	3000000

- Tạo master key, certificate, private key AES\_256 cho các thao tác trên:

```

--create master key
if NOT EXISTS
(
    select*
    from sys.symmetric_keys
    where symmetric_key_id = 101
)
create master key encryption by
    password = '123456'
go

--create certificates
if NOT EXISTS
(
    select *
    from sys.certificates
    WHERE name = 'MyCert'
)
create certificate MyCert
    with subject = 'MyCert'
go

--create private key aes_256
if NOT EXISTS
(
    select*
    from sys.symmetric_keys
    where name = 'PriKey'
)
create symmetric key PriKey
    with algorithm = AES_256,
    key_source = '20120335'
    encryption by certificate MyCert;
go

```

#### 4. Tạo màn hình đăng nhập:

- Kết nối với database quản lý sinh viên.



Add Connection?×

Enter information to connect to the selected data source or click "Change" to choose a different data source and/or provider.

Data source:

Microsoft SQL Server (SqlClient)Change...

Server name:

DESKTOP-A79AAA6\MSSQLSERVER01▼Refresh

Log on to the server

Authentication:

Windows Authentication▼

User name:

Password:

☐ Save my password

Connect to a database

☒ Select or enter a database name:

QLSV▼

☐ Attach a database file:

Browse...

Logical name:

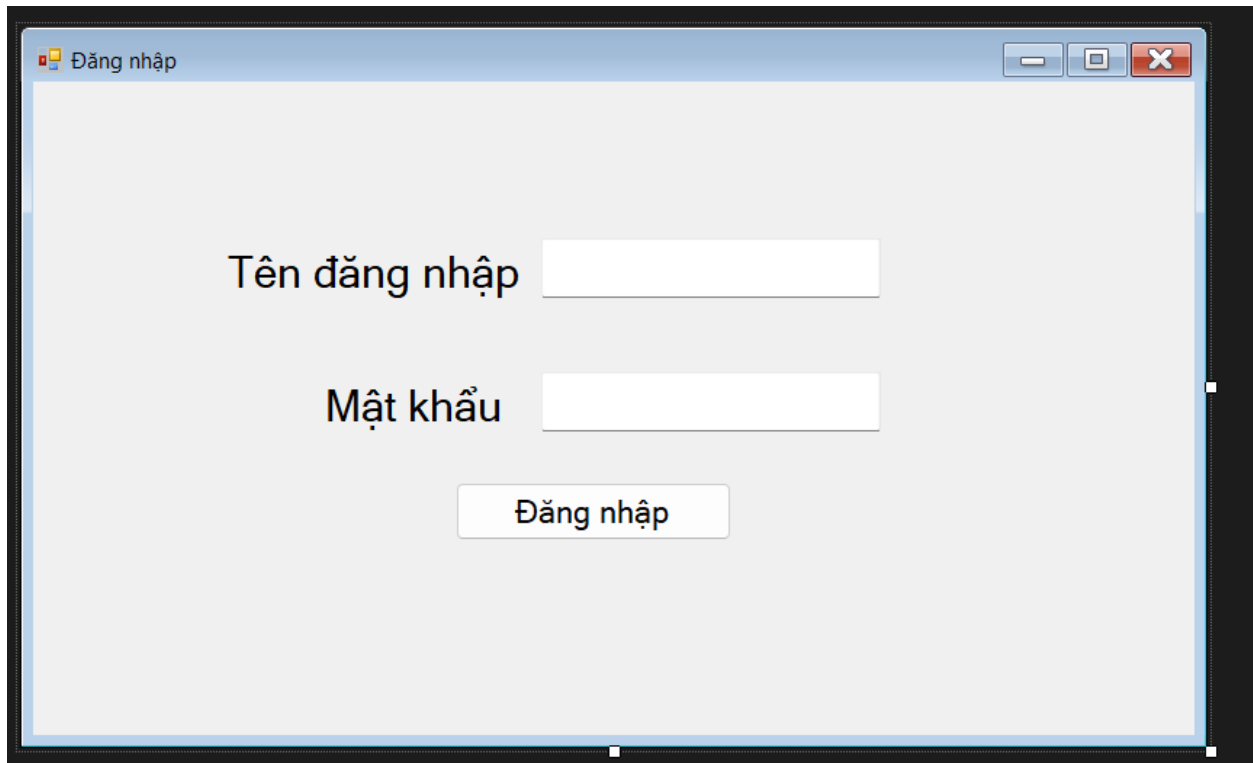
Advanced...

Test Connection

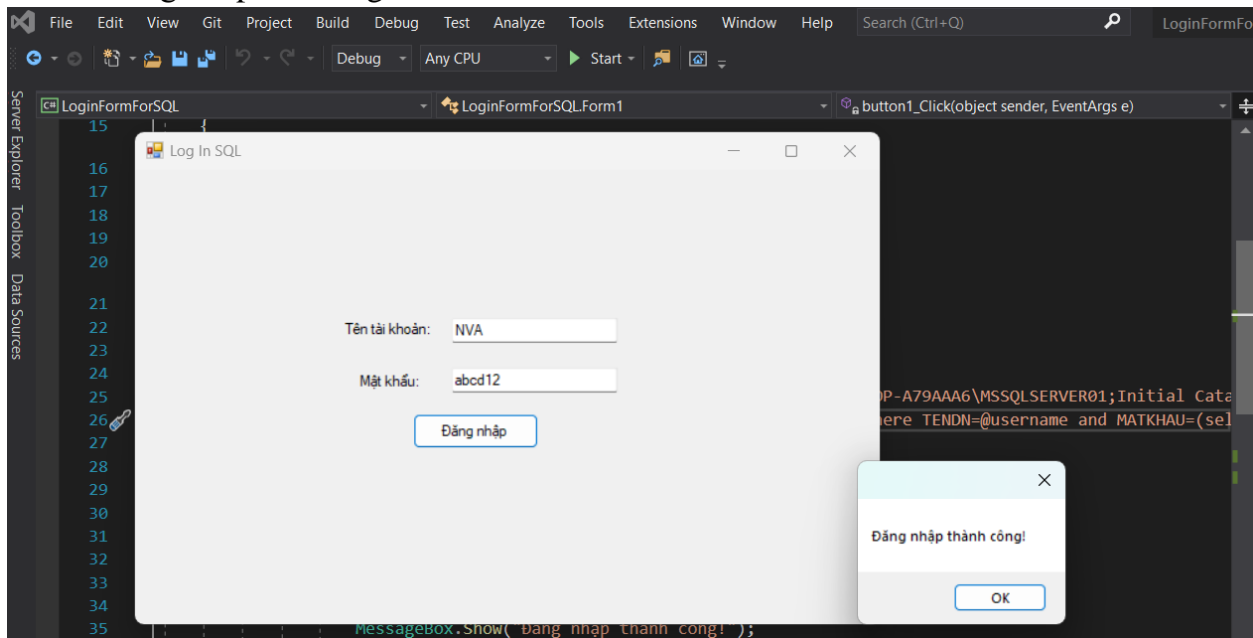
OK

Cancel

- Tạo form đăng nhập.



- Đăng nhập thử bằng tài khoản NVA.



- Kết quả SQL Profiler:

Untitled - 1 (DESKTOP-A79AAA6\MSSQLSERVER01)

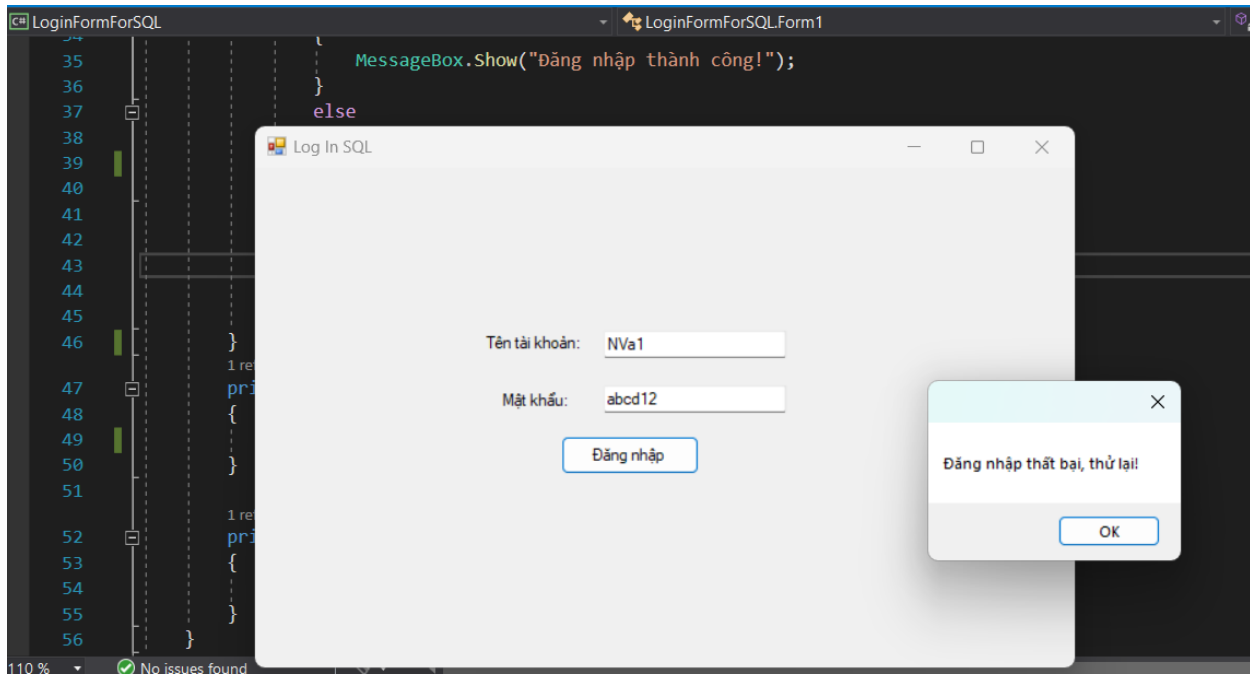
EventClass	TextData	ApplicationName	NTUserName	LoginName	CPU	Reads	Writes	Duration	ClientProcessID
Trace Start									
ExistingConnection	-- network protocol: LPC set quoted_identifier on set arith...	SQLServerCEIP	SQLTELE...	NT SER...					
ExistingConnection	-- network protocol: LPC set quoted_identifier on set arith...	Microsoft SQ...	Admin	DESKTO...					
ExistingConnection	-- network protocol: LPC set quoted_identifier on set arith...	Microsoft SQ...	Admin	DESKTO...					
ExistingConnection	-- network protocol: LPC set quoted_identifier on set arith...	Microsoft SQ...	Admin	DESKTO...					
ExistingConnection	-- network protocol: LPC set quoted_identifier on set arith...	.Net SqlClie...	Admin	DESKTO...					
Audit Login	-- network protocol: LPC set quoted_identifier on set arith...	.Net SqlClie...	Admin	DESKTO...					
RPC:Completed	exec sp_executesql N'select * from NHANVIEN where TENDN=@user...	.Net SqlClie...	Admin	DESKTO...	0	242	0	18	

exec sp\_executesql N'select \* from NHANVIEN where TENDN=@username and MATKHAU=(select HASHBYTES('SHA1',convert(varchar,@password)))',N'@username nvarchar(3),@password nvarchar(6)',@username=N'NVA',@password=N'abcd12'

Trace is running. Ln 8, Col 1 Rows: 8

⇒ Nhận xét: Khi đăng nhập thành công, server sẽ trace được gói là có người dùng nào đăng nhập vào hệ thống.

- Đăng nhập thử với tài khoản NVA1.



- Khi đăng nhập sai vào hệ thống, kết quả SQL Profiler:

Untitled - 1 (DESKTOP-A79AAA6\MSSQLSERVER01)

EventClass	TextData	ApplicationName	NTUserName	LoginName	CPU	Reads	Writes	Duration	ClientProcessID	SPID	StartTime
Trace Start											
ExistingConnection	-- network protocol: LPC set quoted...	SQLServerCEIP	SQLTELE...	NT SER...					11256	51	2023-04-1
ExistingConnection	-- network protocol: LPC set quoted...	Microsoft SQ...	Admin	DESKTO...					19792	58	2023-04-1
ExistingConnection	-- network protocol: LPC set quoted...	Microsoft SQ...	Admin	DESKTO...					19792	59	2023-04-1
ExistingConnection	-- network protocol: LPC set quoted...	.Net SqlClie...	Admin	DESKTO...					15892	61	2023-04-1
Audit Login	-- network protocol: LPC set quoted...	.Net SqlClie...	Admin	DESKTO...					10364	63	2023-04-1
RPC:Completed	exec sp_executesql N'select * from N...	.Net SqlClie...	Admin	DESKTO...	0	242	0	16	10364	63	2023-04-1

exec sp\_executesql N'select \* from NHANVIEN where TENDN=@username and MATKHAU=(select HASHBYTES('SHA1',convert(varchar,@password)))',N'@username nvarchar(4),@password nvarchar(6)',@username=N'NVA1',@password=N'abcd12'

Trace is running. Ln 7, Col 1 Rows: 7

⇒ Nhận xét: Khi đăng nhập thất bại, server vẫn sẽ trace được gói là có người dùng nào đăng nhập vào hệ thống.

### III. Tài liệu tham khảo

- Slide BMCSDL.
- Hướng dẫn thực hành lab 3.
- How to Create a Login Form with SQL Server in C# Form – TK code:  
<https://www.youtube.com/watch?v=OJOJacdiUBY>