

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

KHOA CÔNG NGHỆ THÔNG TIN



BÁO CÁO LAB 4: MÃ HÓA DỮ LIỆU TỪ CLIENT 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

I.	Thông tin chung.....	3
	a/ Thông tin sinh viên.....	3
	b/ Đánh giá mức độ hoàn thành.....	3
II.	Nội dung.....	4
	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:.....	6
III.	Tài liệu tham khảo	13

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 từ client

```

/*TAO STORED PROCEDURE*/
---c.i---
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

```

- 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.

```

---c.ii---
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

```

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

```

---c.iii---
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
    from NHANVIEN NV
end
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:

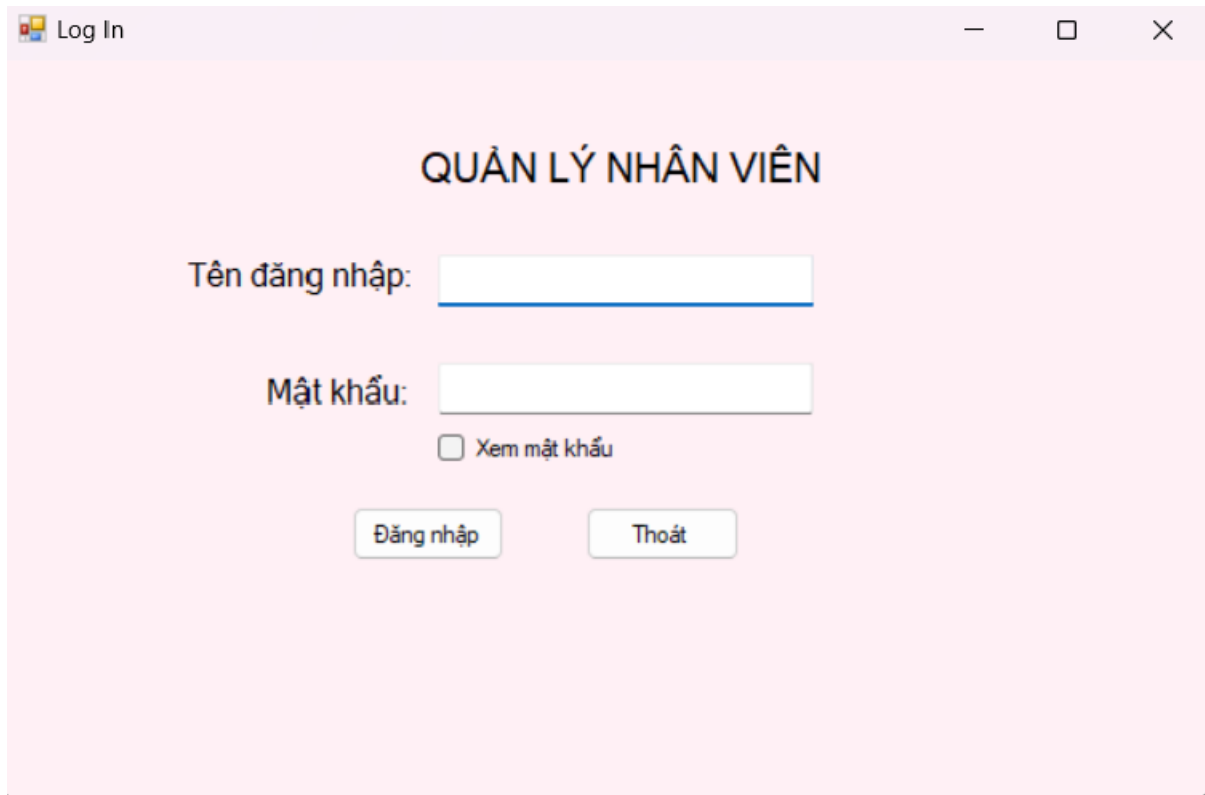
Advanced...

Test Connection

OK

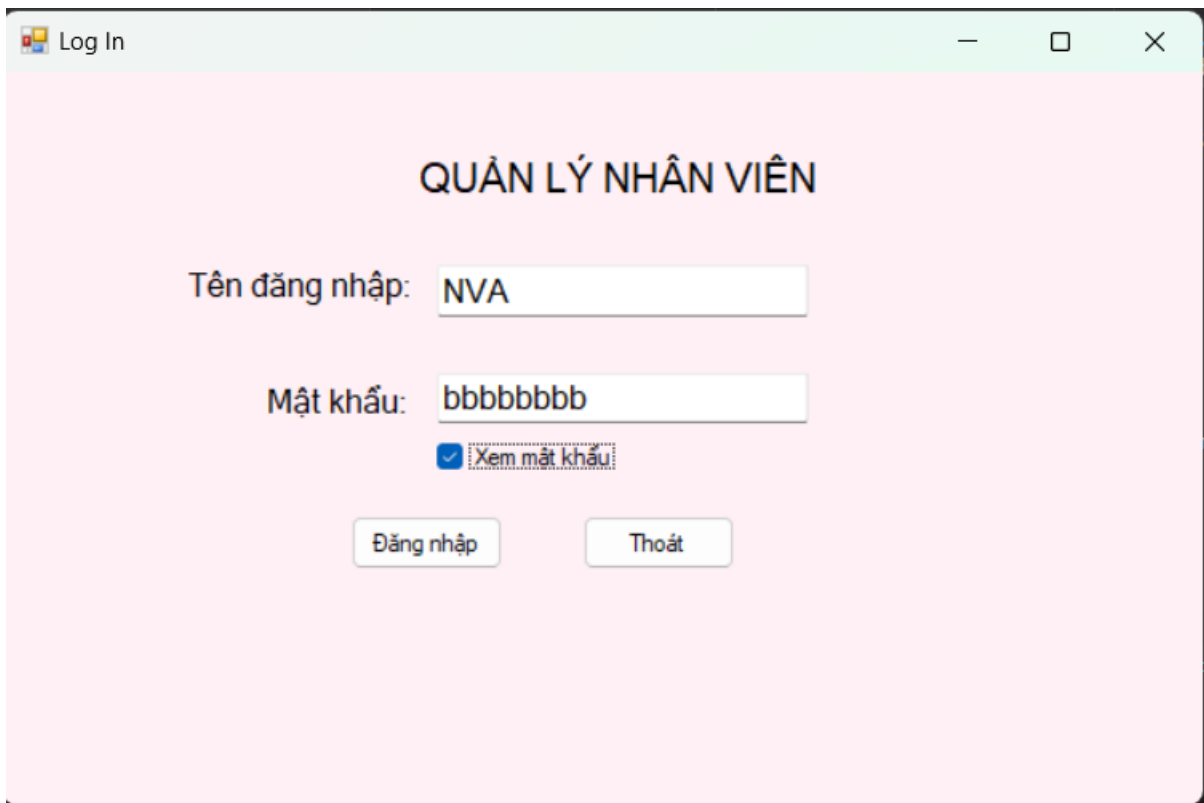
Cancel

- Tạo form đăng nhập.



The image shows a screenshot of a Windows-style application window titled "Log In". The window has a light pink background. At the top center, the text "QUẢN LÝ NHÂN VIÊN" is displayed in a bold, black, sans-serif font. Below this, there are two input fields. The first is labeled "Tên đăng nhập:" and the second is labeled "Mật khẩu:". Below the password field, there is a checkbox labeled "Xem mật khẩu". At the bottom of the form, there are two buttons: "Đăng nhập" and "Thoát". The window's title bar includes standard Windows window controls (minimize, maximize, close) on the right side.

- Đăng nhập thử bằng tài khoản NVA.



- Kết quả SQL Profiler:

EventClass	TextData	ApplicationName	NTUserName	LoginName	CPU	Reads	Writes	Dur
Trace Start								
ExistingConnection	-- network protocol: LPC set quoted_identifier on set arithabort off set numeric_roundabort off set a...	SQLServerCEIP	SQLTELE...	NT SER...				
ExistingConnection	-- network protocol: LPC set quoted_identifier on set arithabort on set numeric_roundabort off set an...	Microsoft SQ...	Admin	DESKTO...				
ExistingConnection	-- network protocol: LPC set quoted_identifier on set arithabort off set numeric_roundabort off set a...	Microsoft SQ...	Admin	DESKTO...				
ExistingConnection	-- network protocol: LPC set quoted_identifier on set arithabort on set numeric_roundabort off set an...	Microsoft SQ...	Admin	DESKTO...				
ExistingConnection	-- network protocol: LPC set quoted_identifier on set arithabort off set numeric_roundabort off set a...	.Net SqlClie...	Admin	DESKTO...				
Audit Login	-- network protocol: LPC set quoted_identifier on set arithabort off set numeric_roundabort off set a...	.Net SqlClie...	Admin	DESKTO...				
RPC:Completed	exec sp_executesql N'SELECT NV,MANV, NV.TENDN FROM NHANVIEN AS NV where NV.TENDN = @username and NV.MATKH...	.Net SqlClie...	Admin	DESKTO...	0	314	0	
Audit Login	-- network protocol: LPC set quoted_identifier on set arithabort off set numeric_roundabort off set a...	.Net SqlClie...	Admin	DESKTO...				
SQL:BatchStarting	exec SP_SEL_ENCRYPT_NHANVIEN	.Net SqlClie...	Admin	DESKTO...				
SQL:BatchCompleted	exec SP_SEL_ENCRYPT_NHANVIEN	.Net SqlClie...	Admin	DESKTO...	0	45	0	
Trace Pause								

```

exec sp_executesql N'SELECT NV,MANV, NV.TENDN FROM NHANVIEN AS NV where NV.TENDN = @username and NV.MATKHAIU = @password',N'@username nvarchar(3),@password
varbinary(32)',@username='NVA',@password=0xFB398CC690E15DDDBA43EE811B6C0D3EC190901AD3DF377FEC9A1F9004B919A06

```

⇒ Nhận xét: Khi đăng nhập thành công, server sẽ trace được gói là có người dùng nào đăng nhập vào hệ thống với username là NVA và password là 0xFB398CC690E15DDDBA43EE811B6C0D3EC190901AD3DF377FEC9A1F9004B919A06 là password được mã hóa từ bbbbbbbb.

- Đăng nhập thử với tài khoản NVA1.

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

EventClass	TextData	ApplicationName	NTUserName	LoginName	CPU	Reads	Writes	Duration	ClientProcessID	SPID	StartTime
Trace Start											2023-04-30 15:07:57...
ExistingConnection	-- network protocol: LPC set quoted...	SQLServerCEIP	SQLTELE...	NT SER...					14016	56	2023-04-30 15:04:18...
ExistingConnection	-- network protocol: LPC set quoted...	Microsoft SQ...	Admin	DESKTO...					19876	57	2023-04-30 12:55:29...
ExistingConnection	-- network protocol: LPC set quoted...	Microsoft SQ...	Admin	DESKTO...					19876	58	2023-04-30 12:55:31...
ExistingConnection	-- network protocol: LPC set quoted...	Microsoft SQ...	Admin	DESKTO...					19876	61	2023-04-30 14:18:00...
ExistingConnection	-- network protocol: LPC set quoted...	.Net SqlClie...	Admin	DESKTO...					13816	64	2023-04-30 13:32:03...
Audit Login	-- network protocol: LPC set quoted...	.Net SqlClie...	Admin	DESKTO...					4776	62	2023-04-30 15:08:07...
RPC:completed	exec sp_executesql N'SELECT NV,MANV,...	.Net SqlClie...	Admin	DESKTO...	0	233	0	1	4776	62	2023-04-30 15:08:16...
Trace Pause											2023-04-30 15:08:16...

```
exec sp_executesql N'SELECT NV,MANV, NV.TENDN FROM NHANVIEN AS NV where nv.TENDN = @username and NV.MATKHAU = @password',N'@username nvarchar(4),@password
varbinary(32)',@username=N'NV1',@password=0xF8396CC690E15DD8A43EE81186C0D3EC190901AD3DF377FEC9A1F90048919A06
```

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

```

where MANV = @MANV
END
GO

exec sp_executesql N'SELECT NV,MANV, NV.TENDN FROM NHANVIEN AS NV where nv.TENDN = @username and NV.MATKHAU = @password',N'@username nvarch

```

00 %

Results Messages

	MANV	TENDN
1	NV01	NVA

- Thực thi câu lệnh trong SQL server với câu lệnh ở SQL profiler.
- ⇒ Nhận xét: Hệ thống dữ liệu sẽ biết được ai đăng nhập vào vì biết được mã nhân viên và tên đăng nhập của nhân viên.

• Thêm nhân viên:

- Sau khi nhập các thông tin cần thêm mới của nhân viên mới vào, ta nhấn nút Thêm sau đó nhấn vào nút Ghi/Lưu để lưu xuống database.

QLNV

DANH MỤC NHÂN VIÊN

Thông tin nhân viên

Mã NV: NV03 Họ tên: NGUYEN VAN C

Email: NVC@ Lương: 2200

Tên đăng nhập: NVC Mật khẩu: 12345678

	MANV	HOTEN	EMAIL	LUONGNV
▶	NV01	NGUYEN VAN A	NVA@	20000
	NV02	NGUYEN VAN B	NVB@	21000
	NV03	NGUYEN VAN C	NVC@	2200
*				

- Kết quả trong SQL Profiler

EventClass	TextData	ApplicationName	NTUserName	LoginName	CPU	Reads	Writes	Duration	ClientProcessID	SPID	StartTime	EndTime
Trace Start											2023-04-30 15:16:41...	
ExistingConnection	-- network protocol: LPC set quoted...	SQLServerCEIP	SQLTELE...	NT SER...					14016	56	2023-04-30 15:14:19...	
ExistingConnection	-- network protocol: LPC set quoted...	Microsoft SQ...	Admin	DESKTO...					19876	57	2023-04-30 12:55:29...	
ExistingConnection	-- network protocol: LPC set quoted...	Microsoft SQ...	Admin	DESKTO...					19876	58	2023-04-30 12:55:31...	
ExistingConnection	-- network protocol: LPC set quoted...	Microsoft SQ...	Admin	DESKTO...					19876	61	2023-04-30 14:18:00...	
ExistingConnection	-- network protocol: LPC set quoted...	.Net SqlClie...	Admin	DESKTO...					13816	64	2023-04-30 13:32:03...	
Audit Login	-- network protocol: LPC set quoted...	.Net SqlClie...	Admin	DESKTO...					20960	55	2023-04-30 15:17:01...	
RPC:Completed	exec sp_executesql N'SELECT NV,MANV,...	.Net SqlClie...	Admin	DESKTO...	0	233	0	1	20960	55	2023-04-30 15:17:01...	2023-04-30 15:
Audit Login	-- network protocol: LPC set quoted...	.Net SqlClie...	Admin	DESKTO...					20960	65	2023-04-30 15:17:02...	
SQL:BatchStarting	exec SP_SEL_ENCRYPT_NHANVIEN	.Net SqlClie...	Admin	DESKTO...					20960	65	2023-04-30 15:17:02...	
SQL:BatchCompleted	exec SP_SEL_ENCRYPT_NHANVIEN	.Net SqlClie...	Admin	DESKTO...	0	45	0	1	20960	65	2023-04-30 15:17:02...	2023-04-30 15:
Audit Logout	-- network protocol: LPC set quoted...	.Net SqlClie...	Admin	DESKTO...	0	233	0	47957	20960	55	2023-04-30 15:17:01...	2023-04-30 15:
RPC:Completed	exec sp_reset_connection	.Net SqlClie...	Admin	DESKTO...	0	0	0	0	20960	55	2023-04-30 15:17:49...	2023-04-30 15:
Audit Login	-- network protocol: LPC set quoted...	.Net SqlClie...	Admin	DESKTO...					20960	55	2023-04-30 15:17:49...	
RPC:Completed	exec sp_executesql N'exec SP_INS_ENC...	.Net SqlClie...	Admin	DESKTO...	0	275	0	2	20960	55	2023-04-30 15:17:49...	2023-04-30 15:
Audit Logout	-- network protocol: LPC set quoted...	.Net SqlClie...	Admin	DESKTO...	0	508	0	34953	20960	55	2023-04-30 15:17:49...	2023-04-30 15:
RPC:Completed	exec sp_reset_connection	.Net SqlClie...	Admin	DESKTO...	0	0	0	0	20960	55	2023-04-30 15:18:23...	2023-04-30 15:
Audit Login	-- network protocol: LPC set quoted...	.Net SqlClie...	Admin	DESKTO...					20960	55	2023-04-30 15:18:23...	
SQL:BatchStarting	exec SP_SEL_ENCRYPT_NHANVIEN	.Net SqlClie...	Admin	DESKTO...					20960	55	2023-04-30 15:18:23...	
SQL:BatchCompleted	exec SP_SEL_ENCRYPT_NHANVIEN	.Net SqlClie...	Admin	DESKTO...	0	257	0	1	20960	55	2023-04-30 15:18:23...	2023-04-30 15:
Trace Pause											2023-04-30 15:18:41...	

```

exec sp_executesql N'exec SP_INS_ENCRYPT_NHANVIEN @manv, @hoten, @email, @luong, @tendn, @matkhau',N'@manv nvarchar(4),@email nvarchar(4),@tendn nvarchar(3),@hoten nvarchar(12),@luong varbinary(16),@matkhau varbinary(32)',@manv=N'NV03',@email=N'NVC@',@tendn=N'NVC',@hoten=N'nguyen Van C',@luong=0x9336CCEB0440CD14502B1896EC96C6,@matkhau=0xEF797C8118F02DFB649607D0503F8C7623048C9C06D032CC95CD7A898A64F

```

- Lệnh SP_INS_ENCRYPT_NHANVIEN trong SQL profiler: exec sp_executesql N'exec SP_INS_ENCRYPT_NHANVIEN @manv, @hoten, @email, @luong, @tendn, @matkhau',N'@manv nvarchar(4),@email nvarchar(4),@tendn

nvarchar(3),@hoten nvarchar(12),@luong varbinary(16),@matkhau
varbinary(32)',@manv=N'NV03',@email=N'NVC@',@tendn=N'NVC',@hoten=N
'Nguyen Van
C',@luong=0x9336CCEBE0440CD14502B1B96EC9E6C6,@matkhau=0xEF797
C8118F02DFB649607DD5D3F8C7623048C9C063D532CC95C5ED7A898A64F

⇒ Nhận xét: khi ta thêm bản rõ của mật khẩu và lương của nhân viên Nguyen Van C
trên client, client sẽ mã hóa lương, mật khẩu của Nguyen Van C sau đó mới lưu
lương và mật khẩu đã được mã hóa vào database.

III. Tài liệu tham khảo

- Slide BMCSDL.
- Hướng dẫn thực hành lab 4.
- How to Create a Login Form with SQL Server in C# Form – TK code:
<https://www.youtube.com/watch?v=OJOJacdiUBY>
-