

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN TP.HCM
KHOA CÔNG NGHỆ THÔNG TIN

~0~



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

20120313 – Phan Tấn Kiệt

TP Hồ Chí Minh, ngày 6 tháng 4 năm 2023

Mục lục

Câu a, b: Tạo CSDL	3
Câu c: Tạo các stored procedure	4
1. Stored procedure SP_INS_SINHVIEN	4
2. Stored procedure SP_SEL_NHANVIEN.....	5
3. Stored procedure SP_SEL_NHANVIEN.....	6
Câu d: Viết màn hình quản lý đăng nhập hệ thống	6
Câu e: Sử dụng công cụ SQL Profile để theo dõi thao tác đăng nhập và nhận xét ...	7
• Nhận xét:	9

Câu a, b: Tạo CSDL

```
IF DB_ID('QLSV') IS NOT NULL
    DROP DATABASE QLSV
GO
CREATE DATABASE QLSV
GO
USE QLSV
GO
-- CREATE TABLES

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(100) NOT NULL,
    PRIMARY KEY(MASV)
)
GO
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) NOT NULL,
    PRIMARY KEY(MANV)
)
GO
CREATE TABLE LOP(
    MALOP VARCHAR(20) NOT NULL,
    TENLOP NVARCHAR(100) NOT NULL,
    MANV VARCHAR(20),
    PRIMARY KEY(MALOP)
)
GO
```

Câu c: Tạo các stored procedure

1. Stored procedure SP_INS_SINHVIEN

Sử dụng mã hoá MD5 để mã thuộc tính MATKHAU

```
IF OBJECT_ID('dbo.SP_INS_SINHVIEN','P') IS NOT NULL
DROP PROCEDURE dbo.SP_INS_SINHVIEN
GO
CREATE PROCEDURE dbo.SP_INS_SINHVIEN
    @MASV NVARCHAR(20),
    @HOTEN NVARCHAR(100),
    @NGAYSINH DATETIME,
    @DIACHI NVARCHAR(200),
    @MALOP VARCHAR(20),
    @TENDN NVARCHAR(100),
    @MATKHAU NVARCHAR(50)
AS
BEGIN
    INSERT INTO SINHVIEN(MASV, HOTEN, NGAYSINH, DIACHI, MALOP, TENDN, MATKHAU)
    VALUES (@MASV, @HOTEN, @NGAYSINH, @DIACHI, @MALOP, @TENDN,
    HASHBYTES('MD5',@MATKHAU))
END
GO
--EXEC dbo.SP_INS_SINHVIEN 'SV01', 'NGUYEN VAN A', '1990-01-01', '280 AN DUONG
VUONG', 'CNTT-K35', 'SVA', '123456' -- Fix date format
```

2. Stored procedure SP_SEL_NHANVIEN

Sử dụng AES 256 với khóa dùng để mã hóa là public key là 20120313 để mã thuộc tính LUONG.

Sử dụng mã hoá SHA1 để mã thuộc tính MATKHAU

```
--Buoc 1
IF NOT EXISTS
(
    SELECT * FROM sys.symmetric_keys WHERE symmetric_key_id = 101
)
CREATE MASTER KEY ENCRYPTION BY
PASSWORD= '20120313'
GO
-- Buoc 2
IF NOT EXISTS
(
    SELECT * FROM sys.certificates WHERE name = 'Cert'
)
CREATE CERTIFICATE Cert
WITH SUBJECT = 'Cert';
GO
-- Buoc 3
IF NOT EXISTS
(
    SELECT * FROM sys.symmetric_keys WHERE name = 'Prikey'
)
CREATE SYMMETRIC KEY Prikey
WITH ALGORITHM = AES_256
ENCRYPTION BY CERTIFICATE Cert;
GO
-- Buoc 4
IF OBJECT_ID('SP_INS_NHANVIEN','P') IS NOT NULL
DROP PROCEDURE SP_INS_NHANVIEN
GO
CREATE PROCEDURE SP_INS_NHANVIEN
    @MANV VARCHAR(20),
    @HOTEN NVARCHAR(100),
    @EMAIL VARCHAR(20),
    @LUONG INT,
    @TENDN NVARCHAR(100),
    @MATKHAU NVARCHAR(100)
AS
BEGIN
    OPEN SYMMETRIC KEY Prikey
    DECRYPTION BY CERTIFICATE Cert;
    DECLARE @LUONG_VARBINARY VARBINARY(100) = CONVERT(VARBINARY(100), @LUONG)
    INSERT INTO NHANVIEN (MANV, HOTEN, EMAIL, LUONG, TENDN, MATKHAU)
    VALUES (@MANV, @HOTEN, @EMAIL, ENCRYPTBYKEY(KEY_GUID('Prikey'),
@LUONG_VARBINARY), @TENDN, HASHBYTES('SHA1', @MATKHAU));
    CLOSE SYMMETRIC KEY Prikey
END
GO
--EXEC SP_INS_NHANVIEN 'NV01', 'NGUYEN VAN A', 'NVA@', 3000000,'NVA', 'abcd12'
```

3. Stored procedure SP_SEL_NHANVIEN

Truy vấn dữ liệu từ bảng nhân viên

```
IF OBJECT_ID('SP_SEL_NHANVIEN','P') IS NOT NULL
DROP PROCEDURE SP_SEL_NHANVIEN
GO
CREATE PROCEDURE SP_SEL_NHANVIEN
AS
BEGIN
    OPEN SYMMETRIC KEY Prikey
    DECRYPTION BY CERTIFICATE Cert;
    SELECT NV.MANV, NV.HOTEN,
    NV.EMAIL, CONVERT(INT, DECRYPTBYKEY(NV.LUONG)) as
    LUONGCB
    FROM NHANVIEN AS NV
    CLOSE SYMMETRIC KEY Prikey
END
GO
--exec SP_SEL_NHANVIEN
```

Câu d: Viết màn hình quản lý đăng nhập hệ thống

Xem thư mục 20120313lab3

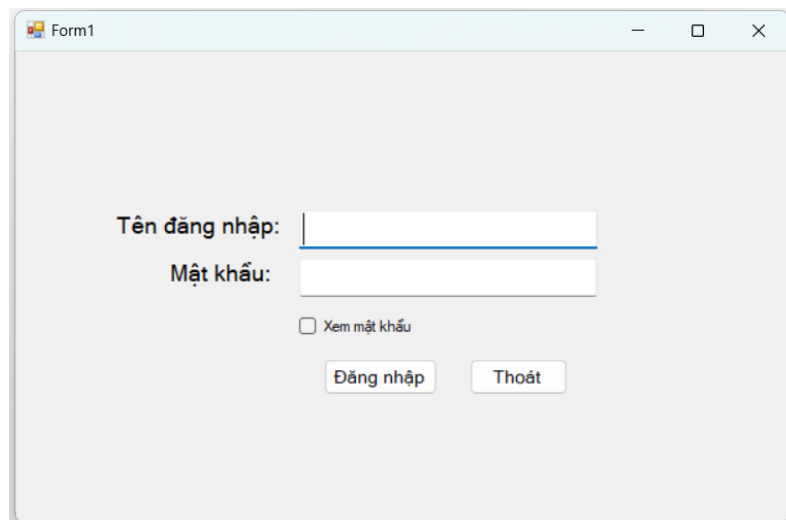
```
private void btnLogIn_Click(object sender, EventArgs e)
{
    string u, p;
    u = txtUser.Text;
    p = txtPass.Text;
    cmd1 = new SqlCommand("select * from sinhvien where
tendn=@username and matkhau=HASHBYTES('MD5',@userpass)", con);
    cmd1.Parameters.AddWithValue("@username", u);
    cmd1.Parameters.AddWithValue("@userpass", p);

    cmd2 = new SqlCommand("select * from nhanvien where
tendn=@username and matkhau=HASHBYTES('SHA1',@userpass)", con);
    cmd2.Parameters.AddWithValue("@username", u);
    cmd2.Parameters.AddWithValue("@userpass", p);

    con.Open();
    rd1 = cmd1.ExecuteReader();
    rd2 = cmd2.ExecuteReader();
    if (rd1.HasRows || rd2.HasRows)
    {
        MessageBox.Show("Đăng nhập thành công");
    }
    else
    {
        MessageBox.Show("tên đăng nhập và mật khẩu không hợp lệ!");
    }
    con.Close();
}
```

Câu e: Sử dụng công cụ SQL Profile để theo dõi thao tác đăng nhập và nhận xét

Bước 1: Mở màn hình đăng nhập



Form1

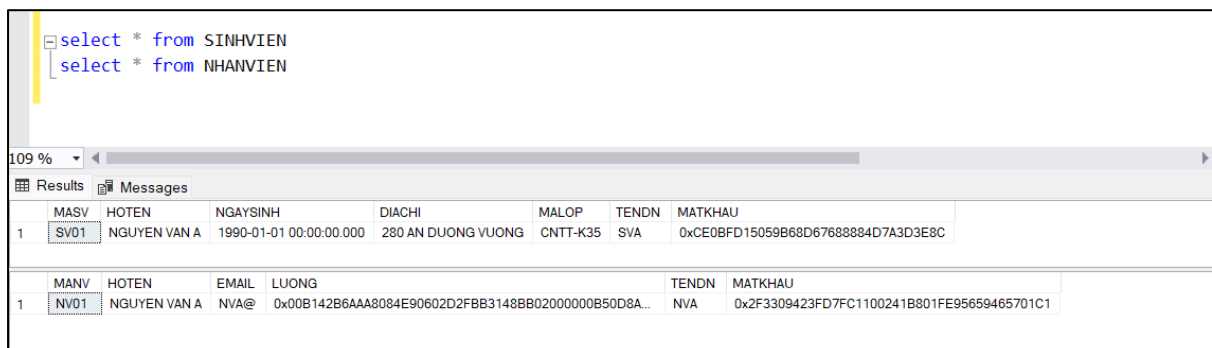
Tên đăng nhập:

Mật khẩu:

☐ Xem mật khẩu

Hình 1: Bảng đăng nhập

Bước 2: Đăng nhập sử dụng tài khoản và mật khẩu:

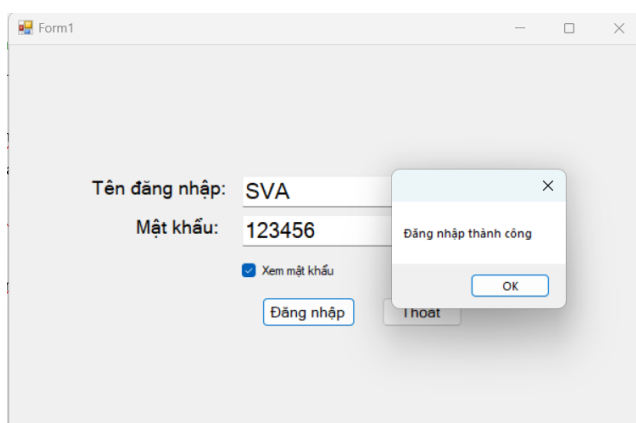


```
select * from SINHVIEN
select * from NHANVIEN
```

	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	SVA	0xCE0BFD15059B68D67688884D7A3D3E8C

	MANV	HOTEN	EMAIL	LUONG	TENDN	MATKHAU
1	NV01	NGUYEN VAN A	NVA@	0x00B142B6AAA8084E90602D2FBB3148BB02000000B50D8A...	NVA	0x2F3309423FD7FC1100241B801FE95659465701C1

Hình 2: Thông tin bảng học sinh và nhân viên



Form1

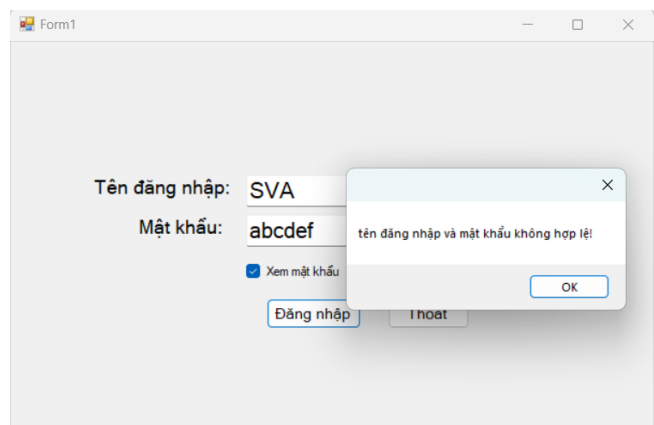
Tên đăng nhập: SVA

Mật khẩu: 123456

☒ Xem mật khẩu

Đăng nhập thành công

OK



Form1

Tên đăng nhập: SVA

Mật khẩu: abcdef

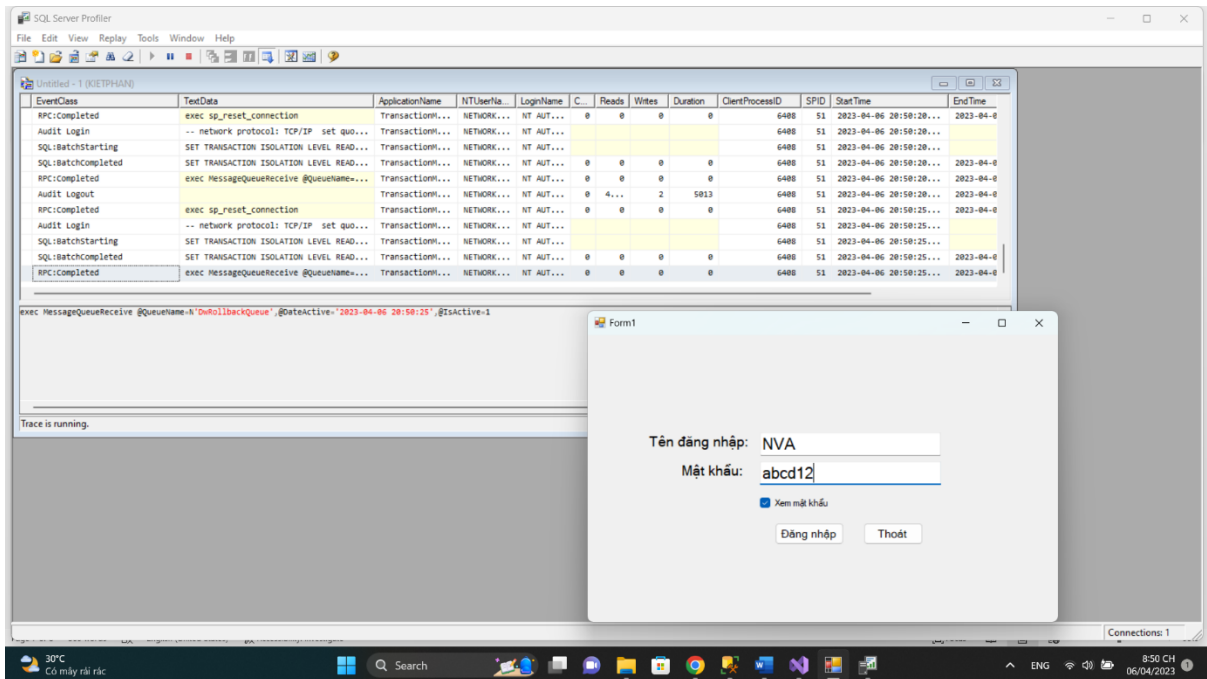
☒ Xem mật khẩu

tên đăng nhập và mật khẩu không hợp lệ!

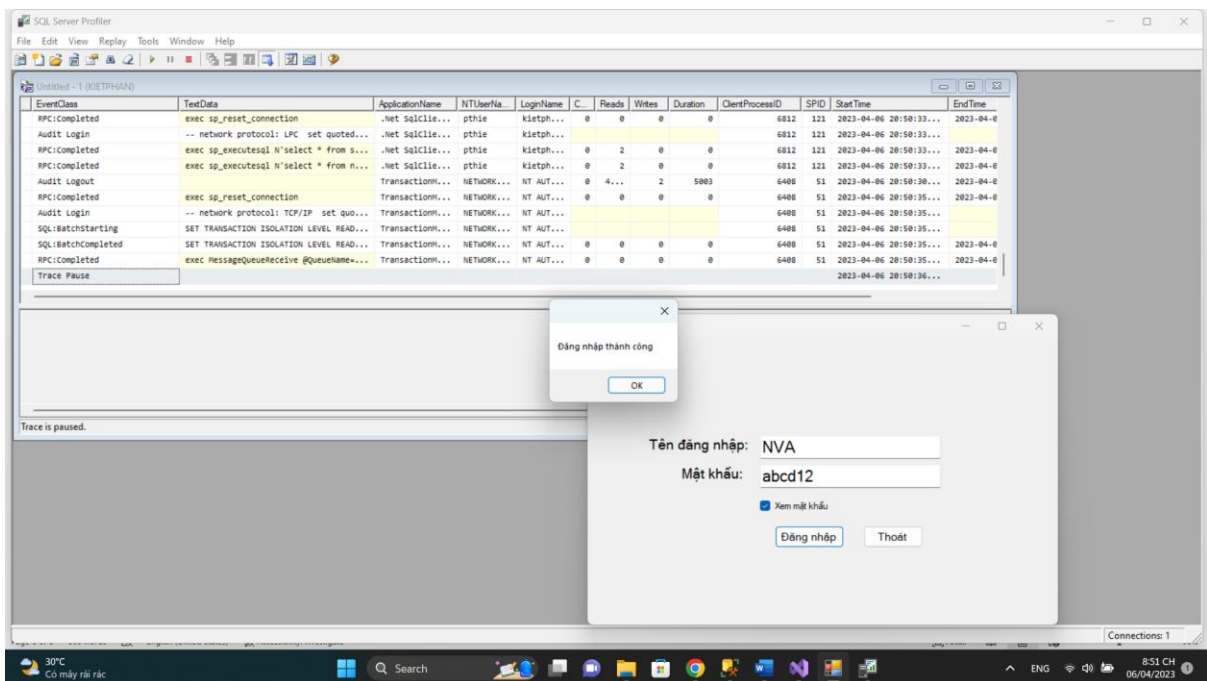
OK

Hình 3: Đăng nhập đúng và sai thông tin

Bước 3: Đăng nhập và sử dụng SQL Profile để theo dõi



Hình 4: Trước khi theo dõi



Hình 5: Sau khi đăng nhập

EventClass	TextData	ApplicationName	NTUserName	LoginName	C...	Reads	Writes	Duration	ClientProcessID	SPID	StartTime	EndTime
RPC:Completed	exec sp_reset_connection	.Net SqlClie...	pthie	kietph...	0	0	0	0	6812	121	2023-04-06 20:50:33...	2023-04-06
Audit Login	-- network protocol: LPC set quoted...	.Net SqlClie...	pthie	kietph...					6812	121	2023-04-06 20:50:33...	
RPC:Completed	exec sp_executesql N'select * from s...	.Net SqlClie...	pthie	kietph...	0	2	0	0	6812	121	2023-04-06 20:50:33...	2023-04-06
RPC:Completed	exec sp_executesql N'select * from n...	.Net SqlClie...	pthie	kietph...	0	2	0	0	6812	121	2023-04-06 20:50:33...	2023-04-06
Audit Logout		TransactionM...	NETWORK...	NT AUT...	0	4...	2	5003	6408	51	2023-04-06 20:50:30...	2023-04-06
RPC:Completed	exec sp_reset_connection	TransactionM...	NETWORK...	NT AUT...	0	0	0	0	6408	51	2023-04-06 20:50:35...	2023-04-06
Audit Login	-- network protocol: TCP/IP set quo...	TransactionM...	NETWORK...	NT AUT...					6408	51	2023-04-06 20:50:35...	
SQL:BatchStarting	SET TRANSACTION ISOLATION LEVEL READ...	TransactionM...	NETWORK...	NT AUT...					6408	51	2023-04-06 20:50:35...	
SQL:BatchCompleted	SET TRANSACTION ISOLATION LEVEL READ...	TransactionM...	NETWORK...	NT AUT...	0	0	0	0	6408	51	2023-04-06 20:50:35...	2023-04-06
RPC:Completed	exec MessageQueueReceive @QueueName=...	TransactionM...	NETWORK...	NT AUT...	0	0	0	0	6408	51	2023-04-06 20:50:35...	2023-04-06
Trace Pause											2023-04-06 20:50:36...	

exec sp_executesql N'select * from sinhvien where tendn=@username and mathau=HASHBYTES('MD5',@userpass)',N'@username nvarchar(3),@userpass nvarchar(6)',@username=N'NVA',@userpass=N'abcd12'

Trace is paused. Ln 73, Col 2 Rows: 81

Hình 6: Query trên bảng sinh viên

EventClass	TextData	ApplicationName	NTUserName	LoginName	C...	Reads	Writes	Duration	ClientProcessID	SPID	StartTime	EndTime
RPC:Completed	exec sp_reset_connection	.Net SqlClie...	pthie	kietph...	0	0	0	0	6812	121	2023-04-06 20:50:33...	2023-04-06
Audit Login	-- network protocol: LPC set quoted...	.Net SqlClie...	pthie	kietph...					6812	121	2023-04-06 20:50:33...	
RPC:Completed	exec sp_executesql N'select * from s...	.Net SqlClie...	pthie	kietph...	0	2	0	0	6812	121	2023-04-06 20:50:33...	2023-04-06
RPC:Completed	exec sp_executesql N'select * from n...	.Net SqlClie...	pthie	kietph...	0	2	0	0	6812	121	2023-04-06 20:50:33...	2023-04-06
Audit Logout		TransactionM...	NETWORK...	NT AUT...	0	4...	2	5003	6408	51	2023-04-06 20:50:30...	2023-04-06
RPC:Completed	exec sp_reset_connection	TransactionM...	NETWORK...	NT AUT...	0	0	0	0	6408	51	2023-04-06 20:50:35...	2023-04-06
Audit Login	-- network protocol: TCP/IP set quo...	TransactionM...	NETWORK...	NT AUT...					6408	51	2023-04-06 20:50:35...	
SQL:BatchStarting	SET TRANSACTION ISOLATION LEVEL READ...	TransactionM...	NETWORK...	NT AUT...					6408	51	2023-04-06 20:50:35...	
SQL:BatchCompleted	SET TRANSACTION ISOLATION LEVEL READ...	TransactionM...	NETWORK...	NT AUT...	0	0	0	0	6408	51	2023-04-06 20:50:35...	2023-04-06
RPC:Completed	exec MessageQueueReceive @QueueName=...	TransactionM...	NETWORK...	NT AUT...	0	0	0	0	6408	51	2023-04-06 20:50:35...	2023-04-06
Trace Pause											2023-04-06 20:50:36...	

exec sp_executesql N'select * from nhanvien where tendn=@username and mathau=HASHBYTES('SHA1',@userpass)',N'@username nvarchar(3),@userpass nvarchar(6)',@username=N'NVA',@userpass=N'abcd12'

Trace is paused. Ln 74, Col 2 Rows: 81

Hình 7: Query trên bảng nhân viên

(Giải thích: Có hai lệnh query là vì trong source code có hai lệnh query để kiểm tra tài khoản trên cả hai bảng)

• Nhận xét:

Phần Textdata ghi lại thông tin của câu lệnh được yêu cầu thực hiện, cũng như các tham số.

Sau khi click vào nút đăng nhập, câu lệnh query được thực hiện, với tham số đầu vào là @username = N'NVA' và @password = N'abcd123'. Hai tham số này được gửi đến server mà không được mã hoá do thuật toán mã hoá chỉ được cài đặt ở phía server.

Mỗi hành động đều ghi lại thông tin user, thời gian thực hiện câu lệnh.