

**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN
KHOA CÔNG NGHỆ THÔNG TIN**



**BÁI CÁO LAB 3
HỌC PHẦN: BẢO MẬT CƠ SỞ DỮ LIỆU**

Nhóm 3: 22127233 – Trần Hoàng Linh

Lớp: 22CLC05

Hồ Chí Minh, Ngày 11 Tháng 03 Năm 2025

3b. Viết Stored procedure

i. SP_INS_PUBLIC_NHANVIEN

Stored procedure dùng để thêm nhân viên mới, trong đó:

- Nếu chưa có khóa tương ứng với MANV, tạo mới bằng thuật toán RSA_2048
- Khóa này được bảo vệ bằng mật khẩu MK
- Lương được chuyển đổi thành dạng VARBINARY trước khi lưu vào cột LUONG
- Mật khẩu của nhân viên không lưu trực tiếp mà được băm bằng SHA1 để đảm bảo bảo mật
- Chèn dữ liệu vào bảng NHANVIEN bao gồm MANV, HOTEN, EMAIL, LUONG (RSA), TENDN, MATKHAU (SHA1), PUBKEY

```
CREATE PROCEDURE SP_INS_PUBLIC_NHANVIEN (
    @MANV VARCHAR(20),
    @HOTEN NVARCHAR(100),
    @EMAIL VARCHAR(20),
    @LUONGCB INT,
    @TENDN NVARCHAR(100),
    @MK NVARCHAR(100)
)
AS
BEGIN

    IF NOT EXISTS (SELECT * FROM sys.asymmetric_keys WHERE NAME
= @MANV)
    BEGIN
        DECLARE @SSQL NVARCHAR(100) = N'CREATE ASYMMETRIC KEY '
+ QUOTENAME(@MANV) +
        N' WITH ALGORITHM = RSA_2048 ENCRYPTION BY PASSWORD =
''' + @MK + ''''

        EXEC sp_executesql @SSQL
    END

    DECLARE @LUONG_BINARY VARBINARY(MAX);
    SET @LUONG_BINARY = ENCRYPTBYASYMKEY(ASYMKEY_ID(@MANV),
convert(varbinary(MAX), @LUONGCB));

    INSERT INTO NHANVIEN(MANV, HOTEN, EMAIL, LUONG, TENDN,
MATKHAU, PUBKEY) VALUES (@MANV, @HOTEN, @EMAIL, @LUONG_BINARY,
@TENDN, HASHBYTES('SHA1', @MK), @MANV)
END
GO
```

Sau khi thực hiện lệnh mã hóa bằng table sẽ có định dạng như sau:

```
EXECUTE SP_INS_PUBLIC_NHANVIEN 'NV11', N'Nguyễn Văn Mười Một',
'vanmuoimot@gmail.com', 11000, N'user11', '12311';
select * from nhanvien
```

	MANV	HOTEN	EMAIL	LUONG	TENDN	MATKHAU	PUBKEY
1	NV01	Nguyễn Văn Một	vanmot@gmail.com	0x49D4A4310BF59080A971A348DDC2CAA514E4938DF82BF6...	user1	0xDCA1B603094D2AF5E304C17B1F0DA47DFE41C6A5	NV01
2	NV02	Nguyễn Văn Hai	vanhai@gmail.com	0xF3A8F1B7FCB12DEE63CC33542EF254E6E4EEA13B37517FE...	user2	0x8DDFA1CDD5313642FF75C6771AA251D5E469EB36	NV02
3	NV03	Nguyễn Văn Ba	vanba@gmail.com	0xFE86CB1A38B8B6413CAE6959690F02C03DF8AD0729C3EAE...	user3	0x97D2B84F97A9AAB202195ABE8BDDAE5690BC5C3	NV03
4	NV04	Nguyễn Văn Tư	vantu@gmail.com	0xB3018BBA2FDA495927FE105326329EFC3A393C8ECD54DE8...	user4	0x139F69C93C042496A8E958EC5930662C6CCCAFBF	NV04
5	NV05	Nguyễn Văn Năm	vannam@gmail.com	0x4A29A9AFF715C92FAB6B3B5616B458BD23058C887523E35...	user5	0xF77054A52C29352ED21BF2F8C6D2D4481C1B7847	NV05
6	NV06	Nguyễn Văn Sáu	vansau@gmail.com	0x3525694E57E9F962E676BE7328BC5E647C4CF38C7DFAF5...	user6	0x3A7396C228C7820FB9C42313282F38DAA3E5EC66	NV06
7	NV07	Nguyễn Văn Bảy	vanbay@gmail.com	0x2435251DE213FC20B0B0584AA6ACDC7FE039E7D449BAA7...	user7	0x1D38E07723D49DC76293EFD83051DAF17304AA3C	NV07
8	NV08	Nguyễn Văn Tám	vantam@gmail.com	0xBD1E18B7A36A9D974EC2123800D26E3DBB92E122652E12...	user8	0x7CB9C405902EB81040BBFB5015ABED07FE46A7F2	NV08
9	NV09	Nguyễn Văn Chín	vanchin@gmail.com	0x925EADBD201AC55F7B733C18354110120E3574112A90F6...	user9	0x7E504CF1DD96733CF97B309921749C8A12A17F10	NV09
10	NV10	Nguyễn Văn Mười	vanmuoi@gmail.com	0x96636EEAD133997BF40E1E6B2C8680A1B16EE0BC97F0ECF...	user10	0x2F21B8D2AAA4425793FFDAA401E57470883F10A4	NV10
11	NV11	Nguyễn Văn Mười Một	vanmuoi1@gmail.com	0x3B13ACBDB8ABD94166819401B13E329D126C9129FBB95B4...	user11	0xFB85A05FE101546178CD19AF168D6D0ECBE943E	NV11

ii. SP_SEL_PUBLIC_NHANVIEN

Stored procedure dùng để truy vấn nhân viên, trong đó:

- Truy vấn nhân viên có TENDN tương ứng.
- Giải mã LUONG bằng RSA
 - Sử dụng khóa bất đối xứng ứng với MANV để giải mã dữ liệu LUONG.
 - Sử dụng mật khẩu MK để mở khóa giải mã.
 - MK được giải mã bằng SHA1

```
CREATE PROCEDURE SP_SEL_PUBLIC_NHANVIEN(
    @TENDN NVARCHAR(100),
    @MK NVARCHAR(100)
)
AS
BEGIN

    SELECT
        MANV,
        HOTEN,
        EMAIL,
        CONVERT(INT, DECRYPTBYASYMKEY( ASYMKEY_ID(MANV), LUONG,
@MK))) AS LUONGCB FROM NHANVIEN
        WHERE TENDN = @TENDN AND MATKHAU = HASHBYTES('SHA1', @MK)

END
GO
```

Sau khi thực hiện lệnh truy vấn trên table nhanvien sẽ có định dạng như sau:

Execute 'user11', '12311'

	MANV	HOTEN	EMAIL	LUONGCB
1	NV01	Nguyễn Văn Một	vanmot@gmail.com	1000

- 3d)
- Xây dựng (lập trình) màn hình quản lý đăng nhập xử lý đăng nhập với tài khoản là nhân viên (MANV, MATKHAU)

A login form with a red background. At the top is a blue circular icon representing a user. Below it are two white input fields: the first contains 'user1' and the second contains '1231'. At the bottom is a white 'Login' button.

- Xây dựng (lập trình) màn hình quản lý lớp học: Người dùng có thể chọn ở thanh chọn gồm “Lớp Quản lý”, “tất cả các lớp học” và xem thông tin về sinh viên đó trong lớp học đó.

The screenshot shows a 'Main Window' titled 'Quản Lý Lớp Học'. The window has a 'Home' tab. On the left is a sidebar with a dropdown menu labeled 'Nhập Điểm' and 'Lớp Quản Lý'. Below the dropdown is a table with columns 'MALOP', 'TENLOP', and 'MANV'. The main area displays a table with columns: MASV, HOTEN, NGAYSINH, DIACHI, MALOP, TENDN, and MATKHAU. The table contains 18 rows of student data.

	MALOP	TENLOP	MANV
1	LOP01	Lớp Toán 1	NV01

	MASV	HOTEN	NGAYSINH	DIACHI	MALOP	TENDN	MATKHAU
1	SV001	Sinh viên 1	2025-01-14 15:24:41.507000	Địa chỉ 1	LOP01	sv1	****
2	SV002	Sinh viên 2	2024-11-25 15:24:41.507000	Địa chỉ 2	LOP01	sv2	****
3	SV003	Sinh viên 3	2024-10-06 15:24:41.507000	Địa chỉ 3	LOP01	sv3	****
4	SV004	Sinh viên 4	2024-08-17 15:24:41.510000	Địa chỉ 4	LOP01	sv4	****
5	SV005	Sinh viên 5	2024-06-28 15:24:41.510000	Địa chỉ 5	LOP01	sv5	****
6	SV006	Sinh viên 6	2024-05-09 15:24:41.510000	Địa chỉ 6	LOP01	sv6	****
7	SV007	Sinh viên 7	2024-03-20 15:24:41.510000	Địa chỉ 7	LOP01	sv7	****
8	SV008	Sinh viên 8	2024-01-30 15:24:41.510000	Địa chỉ 8	LOP01	sv8	****
9	SV009	Sinh viên 9	2023-12-11 15:24:41.510000	Địa chỉ 9	LOP01	sv9	****
10	SV010	Sinh viên 10	2023-10-22 15:24:41.510000	Địa chỉ 10	LOP01	sv10	****
11	SV011	Sinh viên 11	2023-09-02 15:24:41.510000	Địa chỉ 11	LOP01	sv11	****
12	SV012	Sinh viên 12	2023-07-14 15:24:41.510000	Địa chỉ 12	LOP01	sv12	****
13	SV013	Sinh viên 13	2023-05-25 15:24:41.510000	Địa chỉ 13	LOP01	sv13	****
14	SV014	Sinh viên 14	2023-04-05 15:24:41.510000	Địa chỉ 14	LOP01	sv14	****
15	SV015	Sinh viên 15	2023-02-14 15:24:41.510000	Địa chỉ 15	LOP01	sv15	****
16	SV016	Sinh viên 16	2022-12-26 15:24:41.510000	Địa chỉ 16	LOP01	sv16	****
17	SV017	Sinh viên 17	2022-11-06 15:24:41.510000	Địa chỉ 17	LOP01	sv17	****
18	SV018	Sinh viên 18	2022-09-17 15:24:41.510000	Địa chỉ 18	LOP01	sv18	****

- Xây dựng (lập trình) màn hình sinh viên của từng lớp (lưu ý chỉ được phép thay đổi thông tin của những sinh viên thuộc lớp mà nhân viên đó quản lý):
 - o Khi nhân viên quản lý lớp học thì có quyền chỉnh sửa thông tin của sinh viên ở cột thông tin HOTEN, DIACHI.
- Xây dựng (lập trình) nhập bảng điểm của từng sinh viên, trong đó cột điểm thi sẽ được mã hóa bằng chính Public Key của nhân viên (đã đăng nhập):
 - o Với bảng của từng sinh viên chứa thông tin học phần mà sinh viên đó có và đã được mã hóa điểm số bằng public key của nhân viên đó quản lý

```
CREATE PROCEDURE SP_UPDATE_DIEM(
    @MASV VARCHAR(20),
    @MAHP VARCHAR(20),
    @DIEM INT,
    @MANV VARCHAR(20)
)
AS BEGIN
    UPDATE BANGDIEM
    SET DIEMTHI = ENCRYPTBYASYMKEY (ASYMKEY_ID(@MANV),
    CONVERT(varbinary(MAX), @DIEM))
    WHERE @MASV = MASV AND @MAHP = MAHP
END
```

Nhap Diem

Nhập Điểm Lớp LOP01

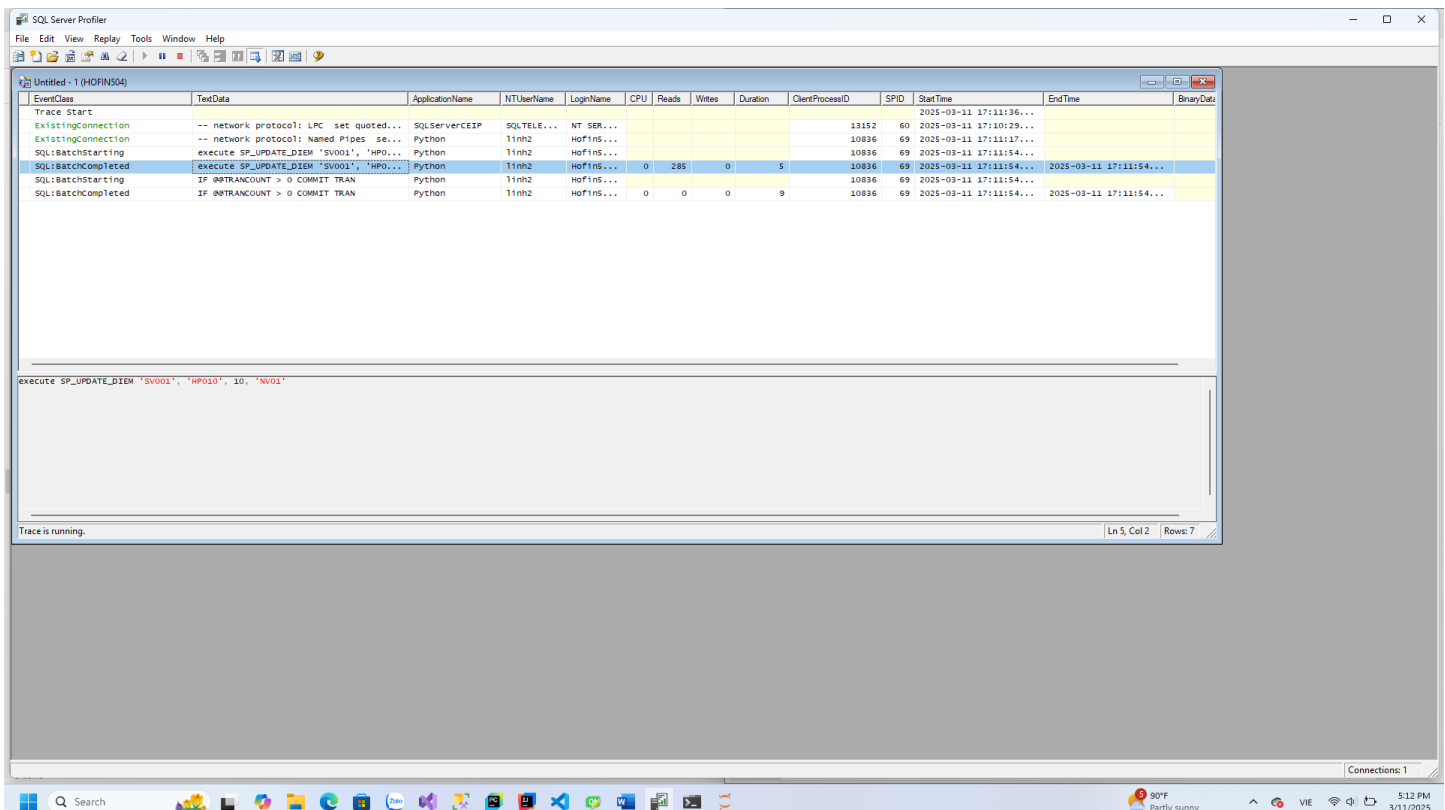
	MASV	HOTEN	MALOP	MANV
1	SV001	Sinh viên 1	LOP01	NV01
2	SV002	Sinh viên 2	LOP01	NV01
3	SV003	Sinh viên 3	LOP01	NV01
4	SV004	Sinh viên 4	LOP01	NV01
5	SV005	Sinh viên 5	LOP01	NV01
6	SV006	Sinh viên 6	LOP01	NV01
7	SV007	Sinh viên 7	LOP01	NV01
8	SV008	Sinh viên 8	LOP01	NV01
9	SV009	Sinh viên 9	LOP01	NV01
10	SV010	Sinh viên 10	LOP01	NV01
11	SV011	Sinh viên 11	LOP01	NV01
12	SV012	Sinh viên 12	LOP01	NV01
13	SV013	Sinh viên 13	LOP01	NV01
14	SV014	Sinh viên 14	LOP01	NV01
15	SV015	Sinh viên 15	LOP01	NV01
16	SV016	Sinh viên 16	LOP01	NV01
17	SV017	Sinh viên 17	LOP01	NV01
18	SV018	Sinh viên 18	LOP01	NV01

	MASV	MAHP	TENHP	SOTC	DIEMTHI
1	SV001	HP001	Học phần 1	1	10
2	SV001	HP002	Học phần 2	4	
3	SV001	HP003	Học phần 3	2	
4	SV001	HP004	Học phần 4	3	
5	SV001	HP005	Học phần 5	1	
6	SV001	HP006	Học phần 6	2	10
7	SV001	HP007	Học phần 7	3	
8	SV001	HP008	Học phần 8	4	
9	SV001	HP009	Học phần 9	3	
10	SV001	HP010	Học phần 10	3	
11	SV001	HP011	Học phần 11	4	
12	SV001	HP012	Học phần 12	2	
13	SV001	HP013	Học phần 13	2	
14	SV001	HP014	Học phần 14	3	
15	SV001	HP015	Học phần 15	4	
16	SV001	HP016	Học phần 16	4	
17	SV001	HP017	Học phần 17	3	
18	SV001	HP018	Học phần 18	2	

- Sử dụng công cụ SQL Profile để theo dõi thao tác trong màn hình nhập điểm sinh viên và cho nhận xét

Nhận xét:

- Đầu tiên, khi ta đăng nhập, sẽ có dữ liệu của client được đưa đến server báo có người dùng với username và password đăng nhập vào hệ thống.
- Sau khi ta nhập điểm, dữ liệu cũng được đưa đến server từ client dưới dạng bản rõ.
- Sau đó, dữ liệu sẽ được server lưu về, mã hóa rồi lưu vào database.
- Chỉ có những người nhân viên có chức năng quản lý sinh viên mới nhìn thấy được bản rõ của điểm sinh viên
- Các sự kiện của profiler:
 - o SQL:BatchStarting & SQL:BatchCompleted: Xác nhận rằng StoredProcedure được thực thi mà không có lỗi.
 - o CPU Time = 285 ms cho thấy quá trình xử lý mất một lượng thời gian CPU đáng kể.
 - o Duration = 5 ms tổng thời gian thực thi khá nhanh, không có dấu hiệu chậm trễ đáng kể.
- Không có dấu hiệu lỗi trong quá trình thực thi SP_UPDATE_DIEM.
- Kết thúc COMMIT TRAN được ghi nhận trong SQL Profiler cho thấy dữ liệu đã được cập nhật thành công.



EventClass	TextData	ApplicationName	NTUserName	LoginName	CPU	Reads	Writes	Duration	ClientProcessID	SPID	StartTime	EndTime	BinaryData
Trace start											2025-03-11 17:11:36...		
ExistingConnection	-- network protocol: LPC set quoted...	SQLServerCE2P	SQLTELE...	NT SER...					13152	60	2025-03-11 17:10:29...		
ExistingConnection	-- network protocol: Named Pipes se...	Python	11nh2	HOflns...					10836	69	2025-03-11 17:11:17...		
SQL:BatchStarting	execute SP_UPDATE_DIEM 'SV001', 'HP0...	Python	11nh2	HOflns...					10836	69	2025-03-11 17:11:54...		
SQL:BatchCompleted	execute SP_UPDATE_DIEM 'SV001', 'HP0...	Python	11nh2	HOflns...	0	285	0	5	10836	69	2025-03-11 17:11:54...	2025-03-11 17:11:54...	
SQL:BatchStarting	IF @@TRANCOUNT > 0 COMMIT TRAN	Python	11nh2	HOflns...					10836	69	2025-03-11 17:11:54...		
SQL:BatchCompleted	IF @@TRANCOUNT > 0 COMMIT TRAN	Python	11nh2	HOflns...	0	0	0	9	10836	69	2025-03-11 17:11:54...	2025-03-11 17:11:54...	

execute SP_UPDATE_DIEM 'SV001', 'HP010', 10, 'NV01'

Trace is running. Ln 5, Col 2 Rows 7

Connections: 1