TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN
KHOA CÔNG NGHỆ THÔNG TIN

BÁO CÁO LAB 4
Học Phần: Bảo Mật Cơ Sở Dữ Liệu

Nhóm 3:

222127233 - Trần Hoàng Linh

Ngày 24 Tháng 03 Năm 2025

Mục lục

1 NỘI DUNG

1.1 Câu 3b

1.1.1 Stored dùng để thêm mới dữ liệu (Insert) vào table SINHVIEN

Trong python, thư viện `hashlib` hỗ trợ mã hóa (HASH). Để mã hóa thuộc MATKHAU trước ghi đưa xuống database có thể sử dụng câu lệnh được cung cấp với thuật toán SHA1 như sau:

```
hashlib.sha1(password.encode()).hexdigest().upper()
```

Với thuộc tính LUONG sẽ được mã hóa sử dụng thuật toán `RSA_2048`. Trong python cũng có thử viên `Crypto` hộ trợ cho việc mã hóa RSA

```
from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_OAEP
```

Trong đó `PKCS1_OAEP` là một lược đồ đệm (padding scheme) được sử dụng với mã hóa RSA. Nó giúp tăng cường tính bảo mật của mã hóa RSA bằng cách thêm một lớp ngẫu nhiên vào dữ liệu trước khi mã hóa.

Sinh cặp khóa:

```
key = RSA.generate(2048)
private_key = key
public_key = key.publickey()
```

Mã hóa:

```
cipher_rsa = PKCS1_OAEP.new(public_key)
bytes_encrypted = cipher_rsa.encrypt(data)
```

Giải mã:

```
cipher_rsa = PKCS1_OAEP.new(private_key)
bytes_decrypted = cipher_rsa.decrypt(bytes_encrypted)
```

Lưu trữ cặp khóa sinh được ra file `manv.pem` chứa private_key và public_key được lưu xuống database tương ứng với `manv`.

Mã hóa private_key với password của tương ứng của nhân viên và đưa ra file chứa key `manv.pem`:

```
luong_encrypted = nhanvien.encrypted(public_key, str(luong))
 with open(f'keys/{manv}.pem', 'wb') as f:
     data = key.export_key(passphrase=password,
         pkcs=8,
         protection='PBKDF2WithHMAC-SHA512AndAES256-CBC',
         prot_params={'iteration_count':131072}
     )
     f.write(data)
```

Đưa public_key xuống database:

```
PUB = public_key.export_key() # bytes
cursor.execute("SP_INS_PUBLIC_ENCRYPT_NHANVIEN ?, ?, ?, ?, ?, ?, ? ",
               manv, hoten, email, pyodbc.Binary(luong_encrypted),
               tendn, pyodbc.Binary(mk_encrypted),
               pyodbc.Binary(PUB))
cursor.commit()
```

Stored procedure được triển khai trong SQL-Server như sau:

```
CREATE PROCEDURE SP_INS_PUBLIC_ENCRYPT_NHANVIEN (
    @MANV VARCHAR(20),
    @HOTEN NVARCHAR(100),
    @EMAIL VARCHAR(20),
    @LUONG VARBINARY(MAX),
    @TENDN NVARCHAR(100),
    @MK VARBINARY(MAX),
    @PUB VARBINARY(MAX)
)
AS
BEGIN
INSERT INTO NHANVIEN
(MANV, HOTEN, EMAIL, LUONG, TENDN, MATKHAU, PUBKEY)
VALUES (@MANV, @HOTEN, @EMAIL, @LUONG, @TENDN, @MK, @PUB)
END
GO
```

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

Phía client, thực hiện mã hóa (SHA1) cho mật khẩu và gửi xuống database mật khẩu đã được mã hóa. từ đó phía Server thực hiện so sánh với mật khẩu mã hóa từ client có khớp với mật khẩu mã hóa được lưu khi user đã đăng kí không. nếu khớp thì xác thực đăng nhập thành công.

Thực hiện mã hóa phía client:

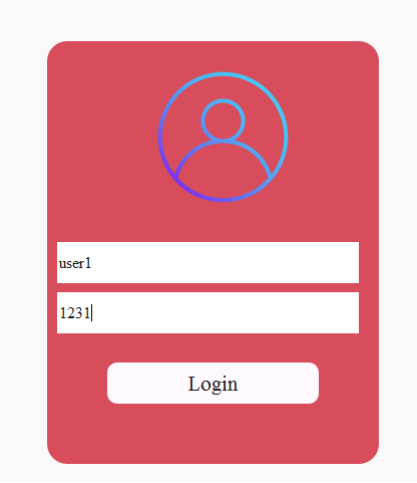
```
    mk_encrypted = crypto.sha1.cipher(MK).encode()

    cursor.execute('EXEC SP_SEL_PUBLIC_ENCRYPT_NHANVIEN ?, ?',
    TENDN, pyodbc.Binary(mk_encrypted))
```

Kiểm tra suy vấn phía Server:

```
CREATE PROCEDURE SP_SEL_PUBLIC_ENCRYPT_NHANVIEN(
     @TENDN NVARCHAR(100),
     @MK VARBINARY(MAX)
)
AS
BEGIN
        SELECT
                MANV,
                HOTEN,
                EMAIL,
                LUONG,
                PUBKEY
        FROM NHANVIEN
        WHERE TENDN = @TENDN AND MATKHAU = @MK
END
GO
```

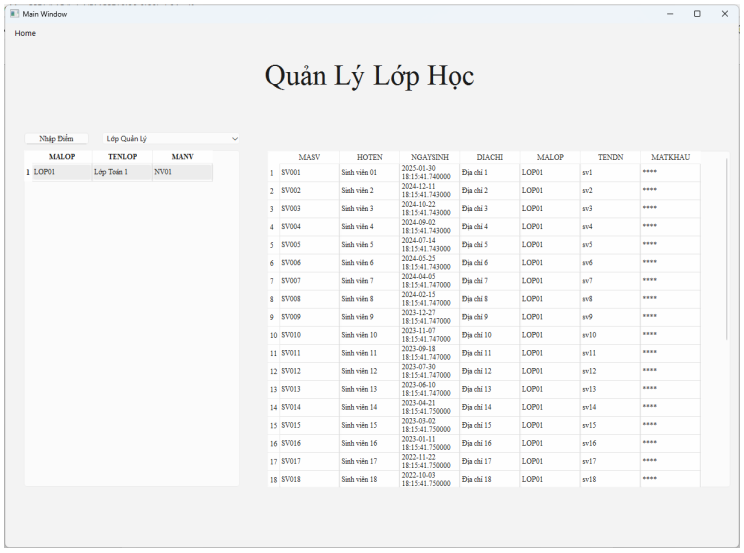
1.2 Câu 3d

- Xây dựng (lập trình) màn hình quản lý đăng nhập như trong bài lab dành cho cá nhân và xử lý đăng nhập với tài khoản là nhân viên (MANV, MATKHAU)

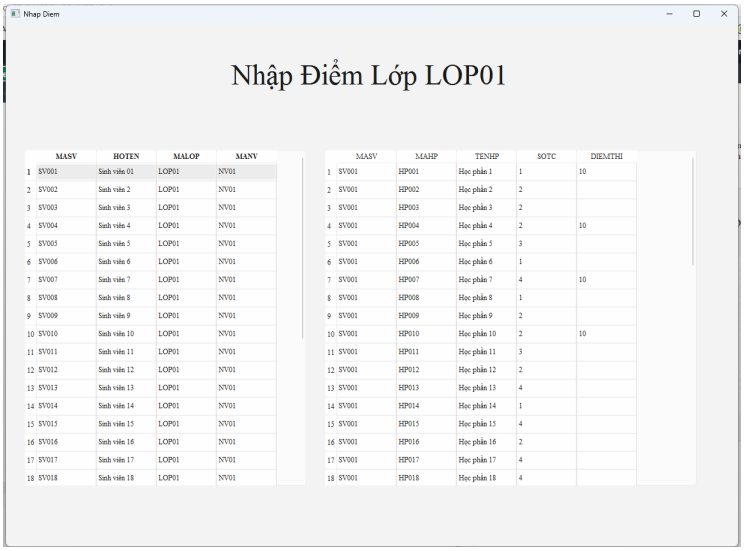


- Xây dựng (lập trình) màn hình quản lý nhân viên

- Xây dựng (lập trình) màn hình quản lý lớp học và 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)

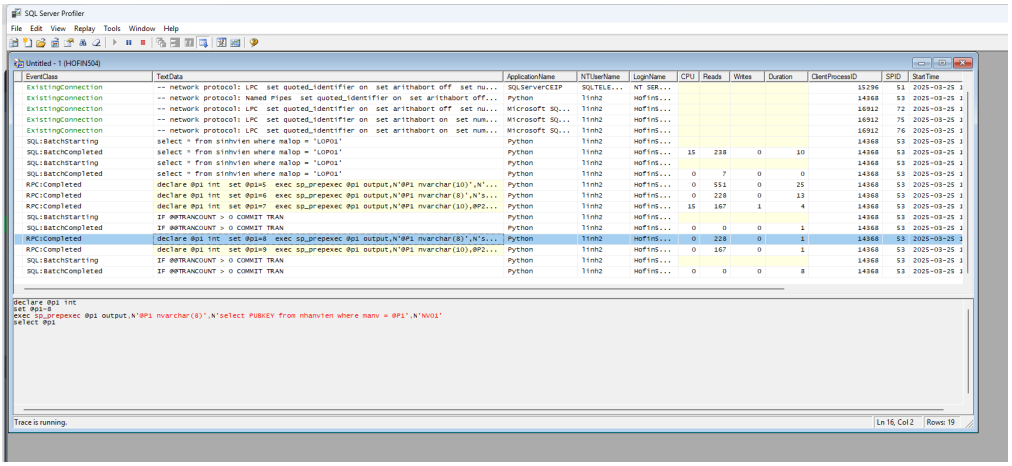


- Xây dựng (lập trình) nhập bảng điểm của từng sinh viên, trong đó cột điểm thi sẽ được mã hóa bằng chính Public Key của nhân viên (đã đăng nhập)

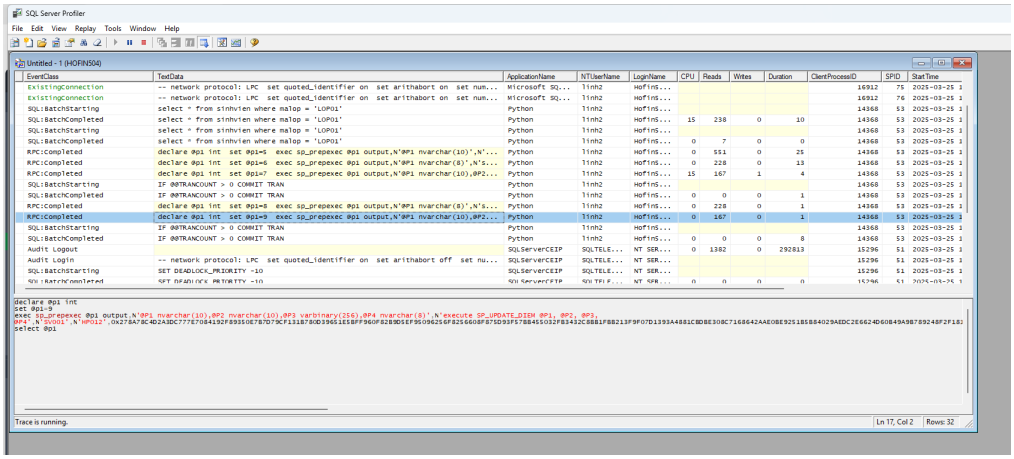


1.3 Câu 3e

Sử dụng công cụ SQL Profile để theo dõi thao tác trong màn hình nhập điểm sinh viên và cho nhận xét.
Để mã hóa điểm ta cần truy vấn `PUBLICKEY` của MANV trong database. từ đó dùng `PUBLICKEY` truy vấn được để mã hóa điểm của Sinh Viên trước khi gửi xuống database:



Khi gửi điểm xuống database ta thấy được rằng điểm của sinh viên `SV001` với học phần `HP012` đã được mã hóa thành 1 chuỗi hex dài là điểm đã mã hóa.


SQL Server Profiler
File Edit View Replay Tools Window Help
Untitled - 1 (HOFIN504)
EventClass TextData ApplicationName NTUserName LoginName CPU Reads Writes Duration ClientProcessID SPID StartTime
ExistingConnection -- network protocol: LPC set quoted_identifier on set arithabort on set num... Microsoft SQ... linh2 HofinS... 16912 75 2025-03-25 1
ExistingConnection -- network protocol: LPC set quoted_identifier on set arithabort on set num... Microsoft SQ... linh2 HofinS... 16912 76 2025-03-25 1
SQL:BatchStarting select * from sinhvien where malop = 'LOP01' Python linh2 HofinS... 14368 53 2025-03-25 1
SQL:BatchCompleted select * from sinhvien where malop = 'LOP01' Python linh2 HofinS... 15 238 0 10 14368 53 2025-03-25 1
SQL:BatchStarting select * from sinhvien where malop = 'LOP01' Python linh2 HofinS... 14368 53 2025-03-25 1
SQL:BatchCompleted select * from sinhvien where malop = 'LOP01' Python linh2 HofinS... 0 7 0 0 14368 53 2025-03-25 1
RPC:Completed declare @p1 int set @p1=5 exec sp_prepexec @p1 output,N'@P1 nvarchar(10)',N'... Python linh2 HofinS... 0 551 0 25 14368 53 2025-03-25 1
RPC:Completed declare @p1 int set @p1=6 exec sp_prepexec @p1 output,N'@P1 nvarchar(8)',N's... Python linh2 HofinS... 0 228 0 13 14368 53 2025-03-25 1
RPC:Completed declare @p1 int set @p1=7 exec sp_prepexec @p1 output,N'@P1 nvarchar(10),@P2... Python linh2 HofinS... 15 167 1 4 14368 53 2025-03-25 1
SQL:BatchStarting IF @@TRANCOUNT > 0 COMMIT TRAN Python linh2 HofinS... 14368 53 2025-03-25 1
SQL:BatchCompleted IF @@TRANCOUNT > 0 COMMIT TRAN Python linh2 HofinS... 0 0 0 1 14368 53 2025-03-25 1
RPC:Completed declare @p1 int set @p1=8 exec sp_prepexec @p1 output,N'@P1 nvarchar(8)',N's... Python linh2 HofinS... 0 228 0 1 14368 53 2025-03-25 1
RPC:Completed declare @p1 int set @p1=9 exec sp_prepexec @p1 output,N'@P1 nvarchar(10),@P2... Python linh2 HofinS... 0 167 0 1 14368 53 2025-03-25 1
SQL:BatchStarting IF @@TRANCOUNT > 0 COMMIT TRAN Python linh2 HofinS... 14368 53 2025-03-25 1
SQL:BatchCompleted IF @@TRANCOUNT > 0 COMMIT TRAN Python linh2 HofinS... 0 0 0 8 14368 53 2025-03-25 1
Audit Logout SQLServerCEIP SQLTELE... NT SER... 0 1382 0 292813 15296 51 2025-03-25 1
Audit Login -- network protocol: LPC set quoted_identifier on set arithabort off set nu... SQLServerCEIP SQLTELE... NT SER... 15296 51 2025-03-25 1
SQL:BatchStarting SET DEADLOCK_PRIORITY -10 SQLServerCEIP SQLTELE... NT SER... 15296 51 2025-03-25 1
declare @p1 int
set @p1=9
exec sp_prepexec @p1 output,N'@P1 nvarchar(10),@P2 nvarchar(10),@P3 varbinary(256),@P4 nvarchar(8)',N'execute SP_UPDATE_DIEM @P1, @P2, @P3,
@P4',N'SV001',N'HP012',0x278A79C4D2A3DC777E7084192F8935DE7B7D79CF131B76CD39651E58FF960F82B8D5EF95D9625F825608F875D93F57BB45503 2F83432C88B1FBB213F9F07D1393A481CBDBE308C7168642AAE0BE925185B84029AEDC2E6624D60B49A9B789248F2F183
select @p1
Trace is running.
Ln 17, Col 2
Rows: 32