

BÀI THỰC HÀNH SỐ 4 (DÀNH CHO NHÓM)

Nội dung yêu cầu:

- Mã hóa dữ liệu từ client trước khi lưu xuống CSDL
- Giải mã dữ liệu ở client sau khi truy vấn dữ liệu từ CSDL

1. Nội dung thực hành

- Tạo bảng và mã hóa dữ liệu sử dụng mã hóa công khai (RSA)
- Tạo stored procedure để truy vấn dữ liệu đã mã hóa

2. Cơ sở dữ liệu “Quản lý sinh viên đơn giản”

- **SINHVIEN (MASV, HOTEN, NGAYSINH, DIACHI, MALOP)**

STT	Thuộc tính	Kiểu dữ liệu	Ghi chú
1	MASV	NVARCHAR(20)	KHÓA CHÍNH
2	HOTEN	NVARCHAR(100)	BẮT BUỘC
3	NGAYSINH	DATETIME	
4	DIACHI	NVARCHAR(200)	
5	MALOP	VARCHAR (20)	
6	TENDN	NVARCHAR(100)	BẮT BUỘC
7	MATKHAU	VARBINARY	BẮT BUỘC

- **NHANVIEN(MANV, HOTEN, EMAIL, LUONG, TENDN, MATKHAU, PUBKEY)**

STT	Thuộc tính	Kiểu dữ liệu	Ghi chú
1	MANV	VARCHAR (20)	KHÓA CHÍNH
2	HOTEN	NVARCHAR(100)	BẮT BUỘC
3	EMAIL	VARCHAR (20)	
4	LUONG	VARBINARY	
5	TENDN	NVARCHAR(100)	BẮT BUỘC
6	MATKHAU	VARBINARY	BẮT BUỘC
7	PUBKEY	VARCHAR(20)	Tên khóa công khai

- **LOP(MALOP, TENLOP, MANV)**

STT	Thuộc tính	Kiểu dữ liệu	Ghi chú
1	MALOP	VARCHAR (20)	KHÓA CHÍNH
2	TENLOP	NVARCHAR(100)	BẮT BUỘC
3	MANV	VARCHAR (20)	

- **HOCPHAN(MAHP, TENHP, SOTC)**

STT	Thuộc tính	Kiểu dữ liệu	Ghi chú
1	MAHP	VARCHAR (20)	KHÓA CHÍNH
2	TENHP	NVARCHAR(100)	BẮT BUỘC
3	SOTC	INT	

- **BANGDIEM(MASV, MAHP, DIEMTHI)**

STT	Thuộc tính	Kiểu dữ liệu	Ghi chú
1	MASV	VARCHAR (20)	KHÓA CHÍNH
2	MAHP	VARCHAR (20)	KHÓA CHÍNH
3	DIEMTHI	VARBINARY	MÃ HÓA

3. Yêu cầu thực hành

- a) Viết script tạo Database có tên **QLSVNhom**.

Đầu file script ghi chú chi tiết như sau:

```

/*-----
MASV:
HO TEN CAC THANH VIEN NHOM:
LAB: 03 - NHOM
NGAY:
-----*/

//CAU LENH TAO DB

```

- b) Viết script tạo mới các Table **SINHVIENT, NHANVIEN, LOP, HOCPHAN, BANGDIEM** như mô tả trên.

Đầu file script ghi chú chi tiết như sau:

```

/*-----
MASV:
HO TEN CAC THANH VIEN NHOM:
LAB: 03 - NHOM
NGAY:
-----*/

//CAC CAU LENH TAO TABLE

```

- c) Viết các Stored procedure sau

Đầu file script ghi chú chi tiết như sau:

```

/*-----
MASV:
HO TEN CAC THANH VIEN NHOM:
LAB: 03 - NHOM
NGAY:
-----*/

// CAU LENH TAO STORED PROCEDURE

```

- i) Stored dùng để thêm mới dữ liệu (Insert) vào table SINHVIEN, trong đó
- Thuộc tính MATKHAU được mã hóa (HASH) sử dụng SHA1
 - Thuộc tính LUONG sẽ được mã hóa từ tham số LUONGCB sử dụng thuật toán RSA 512, với khóa bí mật là tham số MK được truyền vào.
 - Thuộc tính PUBKEY sẽ lưu trữ tên khóa công khai được tạo ra ứng với nhân viên này, giá trị này sẽ lưu thông tin khóa công khai được tạo từ client.

Tên Stored Procedure	SP_INS_PUBLIC_ENCRYPT_NHANVIEN
Danh sách tham số	MANV
	HOTEN
	EMAIL
	LUONG (đã được mã hóa RSA từ client)
	TENDN
	MK (đã được mã hóa SHA1 từ client)
	PUB (Khóa công khai được tạo từ client)

Ví dụ: khi thực thi stored với các tham số

```
EXEC SP_INS_PUBLIC_ENCRYPT_NHANVIEN 'NV01', 'NGUYEN VAN A',
'NVA@', 'LLLLLL', 'NVA', 'MKMKMKMK', 'PUBPUB'
```

Sẽ thêm vào bảng NHANVIEN một dòng trong đó

- Giá trị cột mật khẩu '**MKMKMKMK**' đã được mã hóa sử dụng SHA1.
- Giá trị cột PUBKEY = khóa công khai được tạo từ client.
- Giá trị cột lương '**LLLLLL**' đã được mã hóa sử dụng RSA 512, với khóa công khai Public Key = '**PUBPUB**'

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

Tên Stored Procedure	SP_SEL_PUBLIC_ENCRYPT_NHANVIEN
Danh sách tham số	TENDN MK

Kết quả trả về	Thông tin nhân viên gồm MANV, HOTEN, EMAIL, LUONG, trong đó LUONG là giá trị chưa được giải mã
----------------	--

Ví dụ: khi thực thi stored truy vấn dữ liệu sinh viên

`EXEC SP_SEL_PUBLIC_ENCRYPT_NHANVIEN @MANV, @MK`

Sẽ trả về thông tin nhân viên với dữ liệu lương chưa được giải mã.

d) Viết các stored procedure và chương trình (sử dụng C#) để thực hiện các yêu cầu sau.

Đầu file script ghi chú chi tiết như sau:

`/*-----`

MASV:

HO TEN CAC THANH VIEN NHOM:

LAB: 03 - NHOM

NGAY:

`-----*/`

- 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
- 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)
- 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)

Lưu ý: tất cả các chức năng mã hóa và giải mã đều được thực hiện ở phía client, nghĩa là

- **Mã hóa dữ liệu từ client trước khi lưu xuống CSDL**
- **Giải mã dữ liệu ở client sau khi truy vấn dữ liệu từ CSDL**

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

Lưu ý:

- Chụp lại màn hình các bước thực hiện
- Nộp các file script liên quan đến tất cả các yêu cầu trong phần thực hành