TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN TP.HCM

KHOA CNTT

http://www.fit.hcmus.edu.vn

BÀI THỰC HÀNH SỐ 3

Nội dung yêu cầu: **Mã hóa dữ liệu sử dụng các thuật toán mã hóa công khai**

1. Nội dung thực hành

- Tạo và quản lý khóa

- 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, TENDN, MATKHAU**)**

Bảng sinh viên lưu các thông tin của sinh viên

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**	~~NVARCHAR(200)~~ varchar(20)	
6	TENDN	NVARCHAR(100)	BẮT BUỘC - Unique
7	MATKHAU	VARBINARY	BẮT BUỘC

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

Bảng nhân viên lưu các thông tin liên quan tới nhân viên. Nhân viên bao gồm cả giáo viên giảng dạy và các công nhân viên chức trong trường.

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 - Unique
6	MATKHAU	VARBINARY	BẮT BUỘC
7	PUBKEY	VARCHAR(20)	Tên khóa công khai

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

Lớp lưu các thông tin về lớp, giảng viên chủ nhiệm lớp.

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)**

Table học phần lưu các thông tin liên quan tới học phần gồm tên học phần và số tín chỉ của học phần đó.

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)**

Bảng điểm lưu thông tin nào học môn gì và được bao nhiêu điểm.

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**.

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

c) Viết các Stored procedure sau:

i. Stored dùng để thêm mới dữ liệu (Insert) vào table NHANVIEN, 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 = với mã nhân viên.

Tên Stored Procedure	SP_INS_PUBLIC_NHANVIEN
Danh sách tham số	**MANV** **HOTEN** **EMAIL** **LUONGCB** (trước khi mã hóa) **TENDN** **MK** (giá trị trước khi mã hóa)

Ví dụ: khi thực thi stored với các tham số

EXEC SP_INS_PUBLIC_NHANVIEN 'NV01', 'NGUYEN VAN A', 'NVA@', 3000000, 'NVA', 'abcd12'

Sẽ thêm vào bảng NHANVIEN một dòng trong đó

- Giá trị cột mật khẩu **(abcd12)** sẽ được mã hóa sử dụng SHA1.
- Giá trị cột PUBKEY = 'NV01'
- Giá trị cột lương (3000000) sẽ được mã hóa sử dụng RSA 512, với khóa công khai Public Key sẽ được tạo với tên là 'NV01' và khóa bí mật dùng để tạo khóa công khai là MK

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

Tên Stored Procedure	SP_SEL_PUBLIC_NHANVIEN
Danh sách tham số	**TENDN** **MK**
Kết quả trả về	**Thông tin nhân viên gồm MANV, HOTEN, EMAIL, LUONGCB,** trong đó LUONGCB là giá trị đã được giải mã từ thuộc tính LUONG sử dụng khóa bí mật là mật khẩu MK

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

EXEC SP_SEL_PUBLIC_NHANVIEN ‘NV01’, ‘abcd12’

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

d) Viết các stored procedure và chương trình (Java, Python, C#) để thực hiện các yêu cầu sau.

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

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