

## BÀI THỰC HÀNH SỐ 3 (DÀNH CHO CÁ NHÂN)

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

### 1. Nội dung thực hành

- Tạo và quản lý khóa
- Tạo bảng và mã hóa mật khẩu sử dụng các hàm HASH.
- Mã hóa dữ liệu sử dụng các hệ mã đối xứng (DES, 3DES, AES,...)
- 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	<b>MASV</b>	NVARCHAR(20)	KHÓA CHÍNH
2	<b>HOTEN</b>	NVARCHAR(100)	BẮT BUỘC
3	<b>NGAYSINH</b>	DATETIME	
4	<b>DIACHI</b>	NVARCHAR(200)	
5	<b>MALOP</b>	VARCHAR (20)	
6	<b>TENDN</b>	NVARCHAR(100)	BẮT BUỘC
7	<b>MATKHAU</b>	VARBINARY	BẮT BUỘC

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

STT	Thuộc tính	Kiểu dữ liệu	Ghi chú
1	<b>MANV</b>	VARCHAR (20)	KHÓA CHÍNH
2	<b>HOTEN</b>	NVARCHAR(100)	BẮT BUỘC
3	<b>EMAIL</b>	VARCHAR (20)	
4	<b>LUONG</b>	VARBINARY	
5	<b>TENDN</b>	NVARCHAR(100)	BẮT BUỘC
6	<b>MATKHAU</b>	VARBINARY	BẮT BUỘC

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

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

---

### 3. Yêu cầu thực hành

a) Viết script tạo Database có tên **QLSV**.

Đầu file script ghi chú chi tiết như sau:

```
/*-----  
MASV:  
HO TEN:  
LAB: 03  
NGAY:  
-----*/  
  
//CAU LENH TAO DB
```

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

Đầu file script ghi chú chi tiết như sau:

```
/*-----  
MASV:  
HO TEN:  
LAB: 03  
NGAY:  
-----*/  
  
//CAC CAU LENH TAO TABLE
```

c) Viết các Stored procedure sau

Đầu file script ghi chú chi tiết như sau:

```
/*-----  
MASV:  
HO TEN:  
LAB: 03  
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 MD5

Tên Stored Procedure	SP_INS_SINHVIEN
Danh sách tham số	<b>MASV</b>

	<b>HOTEN</b>
	<b>NGAYSINH</b>
	<b>DIACHI</b>
	<b>MALOP</b>
	<b>TENDN</b>
	<b>MATKHAU</b>

Ví dụ: khi thực thi stored với các tham số

**EXEC SP\_INS\_SINHVIEN 'SV01', 'NGUYEN VAN A', '1/1/1990', '280 AN DUONG VUONG', 'CNTT-K35', 'NVA', '123456'**

Sẽ thêm vào bảng SINHVIEN một dòng trong đó giá trị cột mật khẩu (**123456**) sẽ được mã hóa sử dụng MD5.

- ii) Stored dùng để thêm mới dữ liệu (Insert) vào table NHANVIEN, trong đó thuộc tính MATKHAU được mã hóa (HASH) sử dụng SHA1 và thuộc tính LUONG sẽ được mã hóa sử dụng thuật toán AES 256, với khóa mã hóa là mã số của sinh viên thực hiện bài Lab này.

Tên Stored Procedure	SP_INS_NHANVIEN
Danh sách tham số	<b>MANV</b>
	<b>HOTEN</b>
	<b>EMAIL</b>
	<b>LUONG</b>
	<b>TENDN</b>
	<b>MATKHAU</b>

Ví dụ: khi thực thi stored với các tham số

**EXEC SP\_INS\_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 lương (3000000) sẽ được mã hóa sử dụng AES 256 với khóa dùng để mã hóa là mã số của sinh viên tham gia bài LAB (giả sử sinh viên có mã số 1100234 thì khóa dùng để mã hóa sẽ là **'1100234'**)

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

Tên Stored Procedure	SP_SEL_NHANVIEN
Danh sách tham số	<b>Không có</b>

Kết quả trả về	<b>Danh sách nhân viên gồm MANV, HOTEN, EMAIL, LUONGCB</b> , trong đó LUONGCB là giá trị đã được giải mã từ thuộc tính LUONG sử dụng khóa đã mã hóa
----------------	---

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

**EXEC SP\_SEL\_NHANVIEN**

Sẽ trả về danh sách nhân viên với dữ liệu lương đã được giải mã.

- d) Viết màn hình quản lý đăng nhập hệ thống (sử dụng C#), cho phép nhập vào tên đăng nhập và mật khẩu (giả sử tên đăng nhập của sinh viên và nhân viên là duy nhất, nghĩa là tên đăng nhập của tất cả các sinh viên và tất cả nhân viên là khác nhau).

Kiểm tra nếu tên đăng nhập và mật khẩu tồn tại trong bảng SINHVIEN hoặc NHANVIEN thì hiển thị hộp thông báo thành công

Ngược lại hiển thị hộp thông báo “tên đăng nhập và mật khẩu không hợp lệ”

- e) Sử dụng công cụ SQL Profile để theo dõi thao tác đăng nhập từ màn hình quản lý đăng nhập trên, nhận xét.
- Mở màn hình quản lý đăng nhập
  - Nhập tên đăng nhập và mật khẩu
  - Nhấn nút đăng nhập
  - Chuyển sang màn hình SQL Profile, xem kết quả và viết 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