## Giới thiệu

# Thành viên

|  |  |  |  |
| --- | --- | --- | --- |
| NO | Họ và Tên | MSSV | Email |
| 1 | Võ Minh Khôi | 22127213 | [Vmkhoi22@clc.fitus.edu.vn](mailto:Vmkhoi22@clc.fitus.edu.vn) |
| 2 | Từ Chí Tiến | 22127414 | [Tctien22@clc.fitus.edu.vn](mailto:Tctien22@clc.fitus.edu.vn) |

# Bảng phân công công việc

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **NO.** | | **Công việc** | **Người phụ trách** | **Thời gian hoàn thành** |
| 1 | Thực hiện yêu cầu | A | Tiến | 27/02 – 28/03 |
| 2 | B | Tiến | 27/02 – 28/02 |
| 3 | C | Tiến | 01/03 – 03/03 |
| 4 | D | Khôi | 04/03 – 08/03 |
| 5 | E | Tiến | 09/03 - 09/03 |
| 6 | Kiểm tra và kiểm thử script | | Tiến – Khôi | 09/03 – 10/03 |
| 7 | Viết báo cáo | | Tiến - Khôi | 10/03 - 11/03 |

## Thực hiện

# Tạo database và tạo các bảng

# Viết các Stored Procedure

## Stored Procedure SP\_INS\_PUBLIC\_ENCRYPT\_NHANVIEN

Stored Procedure **SP\_INS\_PUBLIC\_ENCRYPT\_NHANVIEN** được thiết kế để thêm một bản ghi mới vào bảng **NHANVIEN** trong cơ sở dữ liệu **QLSVNhom** với cơ chế mã hóa dữ liệu nhạy cảm từ phía client trước khi lưu trữ.

Các tham số đầu vào: MANV, HOTEN, EMAIL, LUONGCB (VARCHAR), TENDN, MK.

**SP\_INS\_PUBLIC\_NHANVIEN** thực hiện các nhiệm vụ sau:

* **Mã hóa mật khẩu**: Mật khẩu nhận từ client (đã được hash SHA1) sẽ được chuyển đổi sang dạng binary để lưu trữ. Sử dụng hàm **HASHBYTES('SHA1', @MK)** để mã hóa mật khẩu.
* **Xử lý dữ liệu lương:** Thông tin lương đã được mã hóa RSA từ phía client và truyền vào dưới dạng chuỗi. Stored procedure chuyển đổi chuỗi lương đã mã hóa sang dạng varbinary bằng hàm CONVERT(VARBINARY(MAX), @LUONG).
* **Lưu trữ khóa công khai**: Khóa công khai (public key) được lưu trữ nguyên bản dưới dạng chuỗi vào cột PUBKEY. Khóa này sẽ được sử dụng sau này cho các giao dịch mã hóa từ phía server.
* **Thêm dữ liệu**: Thực hiện lệnh INSERT INTO để thêm thông tin nhân viên vào bảng NHANVIEN. Các trường dữ liệu nhạy cảm đều được lưu ở dạng đã mã hóa. Đảm bảo ràng buộc UNIQUE cho trường TENDN (tên đăng nhập).

**Kết quả trả về của Stored Procedure khi thực thi:**

EXEC SP\_INS\_PUBLIC\_ENCRYPT\_NHANVIEN

'NV01',

'NGUYEN VAN A',

'NVA@',

'LLLLLL', -- Lương đã mã hóa RSA

'NVA',

'MKMKMKMK', -- Mật khẩu đã hash SHA1

A screenshot of a computer

AI-generated content may be incorrect. 'PUBPUB'; -- Public key

## Stored Procedure SP\_SEL\_PUBLIC\_ENCRYPT\_NHANVIEN

Stored Procedure **SP\_SEL\_PUBLIC\_ENCRYPT\_NHANVIEN** được thiết kế để truy vấn thông tin nhân viên từ bảng **NHANVIEN** trong cơ sở dữ liệu **QLSVNhom** với cơ chế xác thực và bảo mật dữ liệu nhạy cảm.

Các tham số đầu vào: TENDN, MK.

**SP\_SEL\_PUBLIC\_NHANVIEN** thực hiện các công việc sau:

* **Xác thực thông tin đăng nhập**: Mật khẩu đầu vào được mã hóa SHA1 bằng hàm HASHBYTES('SHA1', @MK) so sánh với giá trị đã lưu trong cơ sở dữ liệu để xác thực.
* **Truy vấn thông tin nhân viên**: Nếu xác thực thành công, procedure trả về các thông tin: MANV, HOTEN, EMAIL, LUONG\_ENCRYTED, PUBKEY.
* **Bảo mật dữ liệu**: Thông tin lương được giữ nguyên ở dạng đã mã hóa (varbinary). Việc giải mã lương phải được thực hiện ở phía client bằng private key tương ứng, chỉ trả về dữ liệu khi thông tin đăng nhập chính xác.

**Kết quả trả về của Stored Procedure khi thực thi:**

A screenshot of a computer

AI-generated content may be incorrect.EXEC SP\_SEL\_PUBLIC\_ENCRYPT\_NHANVIEN 'NVA', 'MKMKMKMK';

# 

# Viết các stored procedure và chương trình để thực hiện các yêu cầu

## Xây dựng màn hình quản lý đăng và xử lý đăng nhập với tài khoản là nhân viên

1. **SP\_SEL\_PUBLIC\_NHANVIEN**

* **Mục đích:** Lấy thông tin của nhân viên, phục vụ cho việc xác thực.
* **Các tham số đầu vào:**
  + **@TENDN**: Tên đăng nhập.
  + **@MK**: Mật khẩu.
* **Công việc chính:**
  + Kiểm tra xem tên đăng nhập và mật khẩu có khớp với bất kỳ bản ghi nào trong bảng **NHANVIEN** hay không.
  + Trả về kết quả xác thực **(@AUTHENTICATED**) và mã nhân viên **(@MANV)** nếu thành công.
* A screenshot of a computer

  AI-generated content may be incorrect.A screenshot of a computer

  AI-generated content may be incorrect.**UI:**

Giao diện của hệ thống sao khi đăng nhập thành công

Màn hình đăng nhập của hệ thống

## Xây dựng màn hình quản lý nhân viên

**1. SP\_INS\_PUBLIC\_ENCRYPT\_NHANVIEN**

**Mục đích**: Thêm nhân viên mới với dữ liệu đã được mã hóa từ client  
**Tham số**:

* @MANV, @HOTEN, @EMAIL, @TENDN (thông tin cơ bản)
* @LUONG (dạng varbinary đã mã hóa)
* @MK (mật khẩu gốc)
* @PUB (khóa công khai)

**Công việc**:

* Chèn dữ liệu đã mã hóa vào bảng NHANVIEN
* Lưu trữ nguyên bản dữ liệu mã hóa từ client

**2. SP\_SEL\_PUBLIC\_ENCRYPT\_NHANVIEN**

**Mục đích**: Truy vấn thông tin nhân viên  
**Tham số**:

* @TENDN (tên đăng nhập)
* @MK (mật khẩu đã hash)  
  **Công việc**:
* Xác thực bằng mật khẩu đã hash
* Trả về thông tin với lương ở dạng mã hóa

**3. SP\_UPD\_ENCRYPTED\_BANGDIEM**

**Mục đích**: Cập nhật điểm đã mã hóa  
**Tham số**:

* @MASV, @MAHP (khóa)
* @DIEMTHI\_ENCRYPTED (điểm đã mã hóa)  
  **Công việc**:
* Cập nhật điểm mà không giải mã trên server

**4. SP\_INS\_ENCRYPTED\_BANGDIEM**

**Mục đích**: Thêm điểm đã mã hóa  
**Tham số**:

* @MASV, @MAHP (khóa)
* @DIEMTHI\_ENCRYPTED (điểm đã mã hóa)  
  **Công việc**:
* Chèn dữ liệu điểm đã mã hóa vào bảng

**5. UI:**