|  |  |
| --- | --- |
| **ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH**  **TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN**  **KHOA CÔNG NGHỆ THÔNG TIN** | |
| A blue and white logo  Description automatically generated | |
| **BÁI CÁO LAB 3**  **HỌC PHẦN: BẢO MẬT CƠ SỞ DỮ LIỆU** | |
| **Nhóm 3:** | 22127233 – Trần Hoàng Linh |
| **Lớp:** | 22CLC05 |
| ***Hồ Chí Minh, Ngày 11 Tháng 03 Năm 2025***  3b. Viết Stored procedure   1. SP\_INS\_PUBLIC\_NHANVIEN   Stored procedure dùng để thêm nhân viên mới, trong đó:   * Nêu chưa có khóa tương ứng với MANV, tạo mới bằng thuật toán RSA\_2048 * Khóa này được bảo vệ bằng mật khẩu MK * Lương được chuyển đổi thành dạng VARBINARY trước khi lưu vào cột LUONG * Mật khẩu của nhân viên không lưu trực tiếp mà được băm bằng SHA1 để đảm bảo bảo mật * Chèn dữ liệu vào bảng NHANVIEN bao gồm MANV, HOTEN, EMAIL, LUONG (RSA), TENDN, MATKHAU (SHA1), PUBKEY  |  | | --- | | CREATE PROCEDURE SP\_INS\_PUBLIC\_NHANVIEN (  @MANV VARCHAR(20),  @HOTEN NVARCHAR(100),  @EMAIL VARCHAR(20),  @LUONGCB INT,  @TENDN NVARCHAR(100),  @MK NVARCHAR(100)  )  AS  BEGIN  IF NOT EXISTS (SELECT \* FROM sys.asymmetric\_keys WHERE NAME = @MANV)  BEGIN  DECLARE @SSQL NVARCHAR(100) = N'CREATE ASYMMETRIC KEY ' + QUOTENAME(@MANV) +  N' WITH ALGORITHM = RSA\_2048 ENCRYPTION BY PASSWORD = ''' + @MK + ''''  EXEC sp\_executesql @SSQL  END    DECLARE @LUONG\_BINARY VARBINARY(MAX);  SET @LUONG\_BINARY = ENCRYPTBYASYMKEY(ASYMKEY\_ID(@MANV), convert(varbinary(MAX), @LUONGCB));    INSERT INTO NHANVIEN(MANV, HOTEN, EMAIL, LUONG, TENDN, MATKHAU, PUBKEY) VALUES (@MANV, @HOTEN, @EMAIL, @LUONG\_BINARY, @TENDN, HASHBYTES('SHA1', @MK), @MANV)  END  GO |   Sau khi thực hiện lệnh mã hóa bằng table sẽ có định dạng như sau:   |  | | --- | | EXECUTE SP\_INS\_PUBLIC\_NHANVIEN 'NV11', N'Nguyễn Văn Mười Một', 'vanmuoimot@gmail.com', 11000, N'user11', '12311';  select \* from nhanvien |      1. SP\_SEL\_PUBLIC\_NHANVIEN   Stored procedure dùng để truy vấn nhân viên, trong đó:   * Truy vấn nhân viên có TENDN tương ứng. * Giải mã LUONG bằng RSA   + Sử dụng khóa bất đối xứng ứng với MANV để giải mã dữ liệu LUONG.   + Sử dụng mật khẩu MK để mở khóa giải mã.   + MK được giải mã bằng SHA1  |  | | --- | | CREATE PROCEDURE SP\_SEL\_PUBLIC\_NHANVIEN(  @TENDN NVARCHAR(100),  @MK NVARCHAR(100)  )  AS  BEGIN  SELECT  MANV,  HOTEN,  EMAIL,  CONVERT(INT, DECRYPTBYASYMKEY( ASYMKEY\_ID(MANV), LUONG, @MK)) AS LUONGCB FROM NHANVIEN  WHERE TENDN = @TENDN AND MATKHAU = HASHBYTES('SHA1', @MK)  END  GO |   Sau khi thực hiện lệnh truy vấn trên table nhanvien sẽ có định dạng như sau:   |  | | --- | | Execute ‘user11’, ‘12311’ |   **A screenshot of a computer  AI-generated content may be incorrect.**    3d)   * 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: Người dùng có thể chọn ở thanh chọn gồm “Lớp Quản lý”, “tất cả các lớp học” và xem thông tin về sinh viên đó trong lớp học đó.      * 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):   + Khi nhân viên quản lý lớp học thì có quyền chỉnh sửa thông tin của sinh viên ở cột thông tin HOTEN, DIACHI. * 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):   + Với bảng của từng sinh viên chứa thông tin học phần mà sinh viên đó có và đã được mã hóa điểm số bằng public key của nhân viên đó quản lý  |  | | --- | | CREATE PROCEDURE SP\_UPDATE\_DIEM(  @MASV VARCHAR(20),  @MAHP VARCHAR(20),  @DIEM INT,  @MANV VARCHAR(20)  )  AS BEGIN  UPDATE BANGDIEM  SET DIEMTHI = ENCRYPTBYASYMKEY (ASYMKEY\_ID(@MANV), CONVERT(varbinary(MAX), @DIEM))  WHERE @MASV = MASV AND @MAHP = MAHP  END | | |

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

Nhận xét:

* Đầu tiên, khi ta đăng nhập, sẽ có dữ liệu của client được đưa đến server báo có người dùng với username và password đăng nhập vào hệ thống.
* Sau khi ta nhập điểm, dữ liệu cũng được đưa đến server từ client dưới dạng bản rõ.
* Sau đó, dữ liệu sẽ được server lưu về, mã hóa rồi lưu vào database.
* Chỉ có những người nhân viên có chức năng quản lý sinh viên mới nhìn thấy được bản rõ của điểm sinh viên
* Các sự kiện của profiler:
  + SQL:BatchStarting & SQL:BatchCompleted: Xác nhận rằng Sture procedure được thực thi mà không có lỗi.
  + CPU Time = 285 ms cho thấy quá trình xử lý mất một lượng thời gian CPU đáng kể.
  + Duảtion = 5 ms tông thời gian thực thi khá nhanh, không có dấu hiện chậm trễ đáng kể.
* Không có dấu hiệu lỗi trong quá trình thực thi SP\_UPDATE\_DIEM.
* Kết thúc COMMIT TRAN được ghi nhận trong SQL Profiler cho thấy dữ liệu đã được cập nhật thành công.

**A screenshot of a computer

AI-generated content may be incorrect.**