

**TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN TP.HCM**

**KHOA CÔNG NGHỆ THÔNG TIN**

**BÁO CÁO BÀI TẬP**

**MÔN: AN TOÀN VÀ BẢO MẬT DỮ LIỆU**

**TRONG HỆ THỐNG THÔNG TIN**

**Bài tập thực hành nhóm 02: Mã hóa**

Giáo viên hướng dẫn: Lương Vĩ Minh

Nhóm ISS2-10:

1612064 – Nguyễn Thị Thu Cúc

1612682 – Nguyễn Thị Thúy

1612894 – Phạm Quỳnh Thi

**Mục lục**

Bảng phân công thực hiện 3

Phần 1: 4

Tạo CSDL và nhập liệu

Tạo user và role

Phần 2:

Câu 1

Câu 2

Câu 3

Câu 4

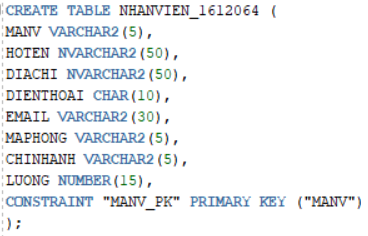
**BẢNG PHÂN CÔNG THỰC HIỆN**

|  |  |  |
| --- | --- | --- |
| **Thành viên thực hiện** | **Công việc** | **Mức độ hoàn thành** |
| 1612064 – Nguyễn Thị Thu Cúc | Cài đặt cấu trúc của cơ sở dữ liệu theo lược đồ | 100% |
| Tạo tài khoản (user) cho các nhân viên | 100% |
| Áp dụng giải pháp DAC phân quyền theo yêu cầu câu 2c | 100% |
| Áp dụng giải pháp VPD và DAC phân quyền theo yêu cầu câu 2e | 100% |
| Áp dụng giải pháp OLS phân quyền theo yêu cầu câu 2f | 0% |
| 1612682 – Nguyễn Thị Thúy |  |  |
| 1612894 – Phạm Quỳnh Thi | Nhập dữ liệu vào cơ sở dữ liệu | 100% |
| Áp dụng giải pháp DAC tạo các vai trò (role) cho các vị trí trong công ty theo yêu cầu câu 2b | 100% |
| Áp dụng giải pháp DAC phân quyền theo yêu cầu câu 2d | 100% |
| Áp dụng giải pháp OLS phân quyền theo yêu cầu câu 2g | 0% |
| Áp dụng giải pháp VPD phân quyền theo yêu cầu câu 2h | 100% |
| Tổng kết mức độ hoàn thành: | | 80% |

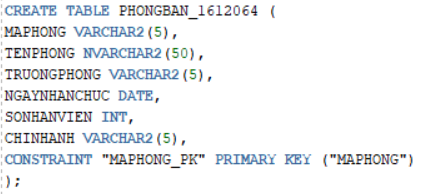
**PHẦN 1**

* Cài đặt cấu trúc của cơ sở dữ liệu theo lược đồ và nhập liệu cho các bảng:

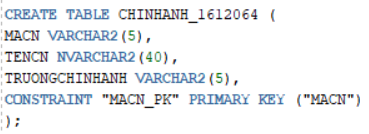
Bảng NHANVIEN:



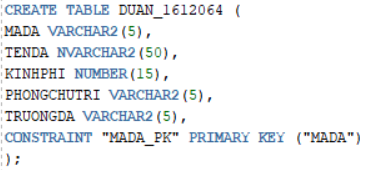
Bảng PHONGBAN:



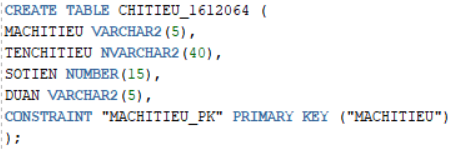
Bảng CHINHANH:



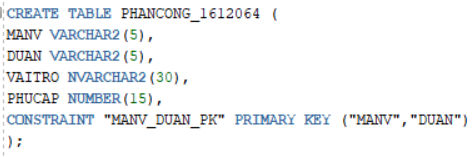
Bảng DUAN:



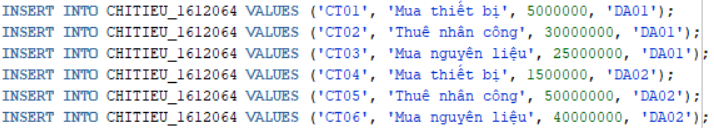
Bảng CHITIEU:

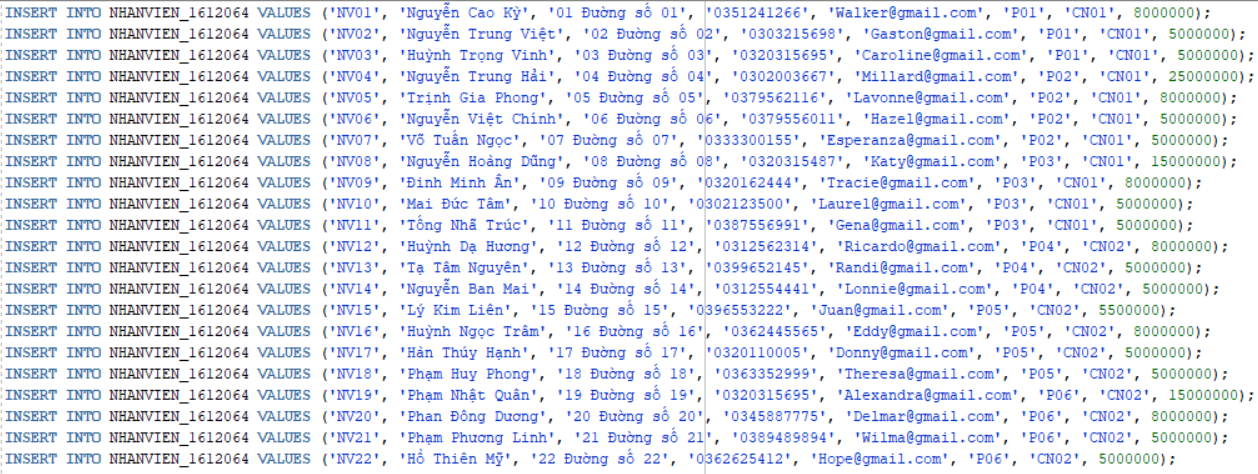


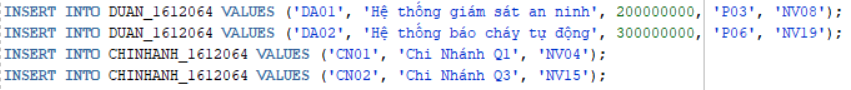
Bảng PHANCONG:

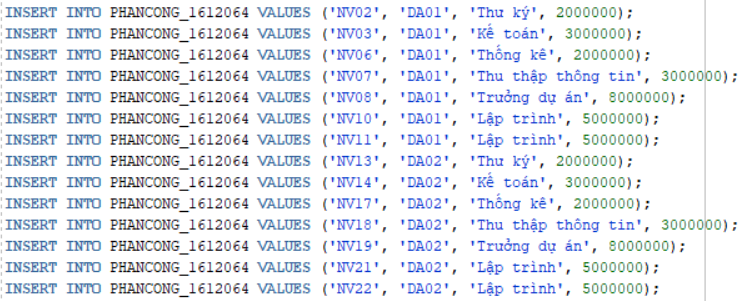


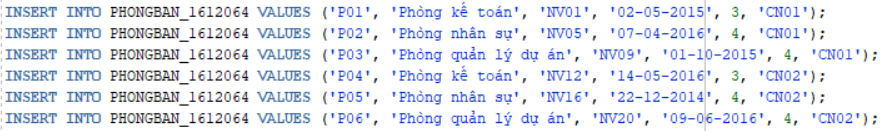
* Nhập dữ liệu:



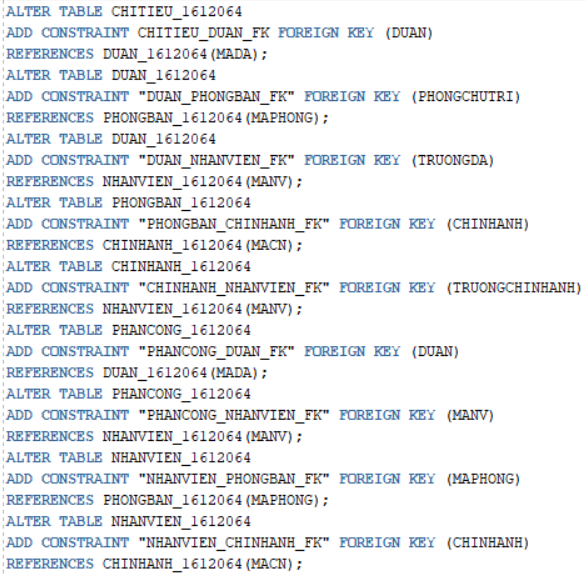




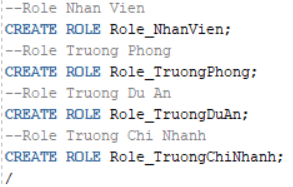




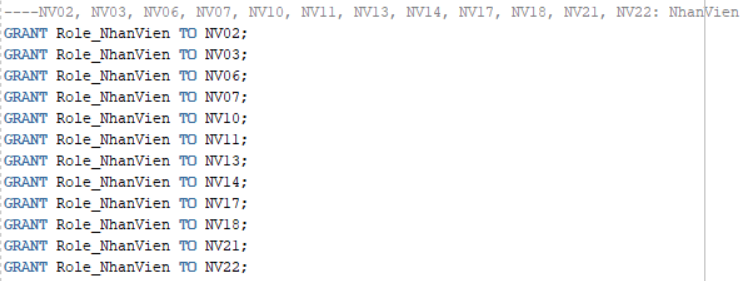
* Tạo khóa ngoại:

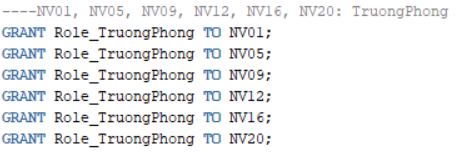


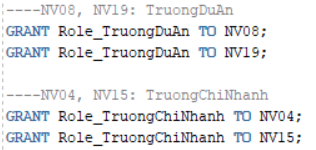
* Tạo các role: nhân viên, trưởng phòng, trưởng dự án, trưởng chi nhánh



* Tạo user tự động bằng thủ tục:
* Truyền vào 2 giá trị số thứ tự user bắt đầu và kết thúc.
* Lặp câu lệnh thực thi tạo user có mã nhân viên là NV + số thứ tự và câu lệnh cấp quyền đăng nhập ‘GRANT CREATE SESSION’ cho user đó.
* Thực thi tạo tự động 22 user ứng với 22 nhân viên:
* Gán role cho các user:







**PHẦN 2**

*Câu 1: Với nhóm người dùng là Nhân viên, thông tin lương của Nhân viên là nhạy cảm và  
chỉ Nhân viên đó mới đươc xem thông tin đó. Vì vậy, thông tin lương cần được mã  
hóa sao cho chỉ Nhân viên được phép xem thông tin lương của mình. Sinh viên cần  
thiết kế giải pháp sử dụng mã hóa đối xứng (cần lựa chọn thuật toán, padding,  
scheme,…) hoặc mã hóa bất đối xứng (thuật toán,...) để bảo vệ thông tin này*

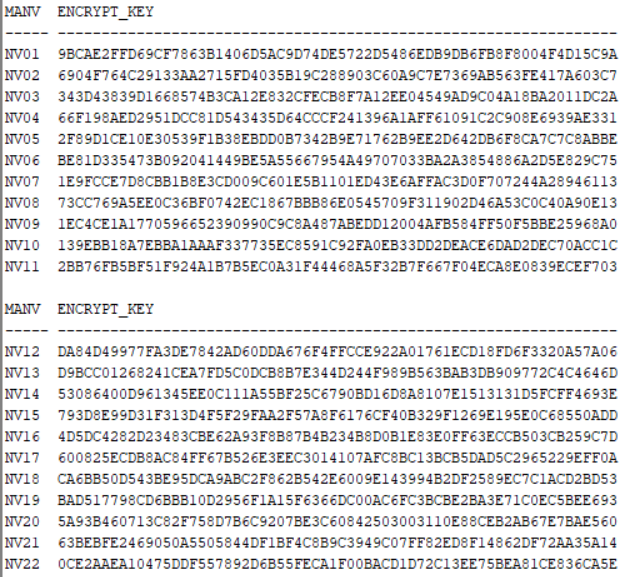
* **Mã hóa thông tin lương:**

1. Trong bảng NHANVIEN, tạo cột mới ENCRYPTED\_LUONG kiểu RAW chứa dữ liệu lương sau khi được mã hóa:
2. Trong bảng NHANVIEN, tạo cột mới ENCRYPT\_KEY kiểu RAW 32 bytes chứa khóa dùng để mã hóa và giải mã lương của một nhân viên:



1. Phát sinh khóa ngẫu nhiên độ dài 32 bytes bằng hàm DBMS\_CRYPTO.RANDOMBYTES, lưu vào cột ENCRYPT\_KEY:





*(Mã nhân viên và khóa ngẫu nhiên tương ứng của nhân viên đó)*

1. Thủ tục mã hóa cột lương trong bảng NHANVIEN bằng khóa của nhân viên đó. Trước khi mã hóa, thực hiện phép XOR lương với số điện thoại của nhân viên.

* Duyệt bảng NHANVIEN bằng con trỏ (NV\_CUR), đọc các thuộc tính: mã nhân viên, số điện thoại, lương, khóa

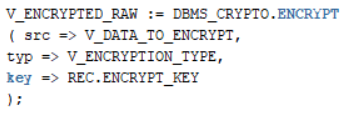


* Đối với từng bộ dữ liệu con trỏ (REC), thực hiện phép XOR lương với số điện thoại của nhân viên (sau khi chuyển sang kiểu RAW bằng hàm UTL\_RAW.CAST\_TO\_RAW) và lưu vào biến V\_DATA\_TO\_ENCRYPT kiểu RAW bằng hàm UTL\_RAW.BIT\_XOR:

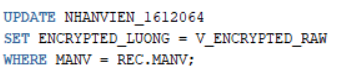


* Thực hiện mã hóa V\_DATA\_TO\_ENCRYPT bằng hàm DBMS\_CRYPTO.ENCRYPT, với kiểu mã hóa (typ) là tổ hợp của thuật toán ENCRYPT\_AES256, kiểu chain CHAIN\_CBC và kiểu padding PAD\_PKCS5 và khóa (key) là khóa ENCRYPT\_KEY của nhân viên đó:



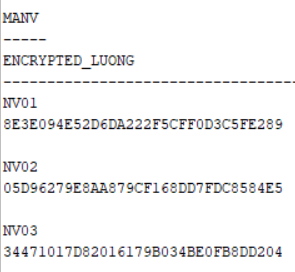


* Cập nhật thông tin mã hóa vào cột ENCRYPTED\_LUONG:



1. Sau khi mã hóa ta được chuỗi mã ENCRYPTED\_LUONG (của 3 nhân viên đầu tiên):

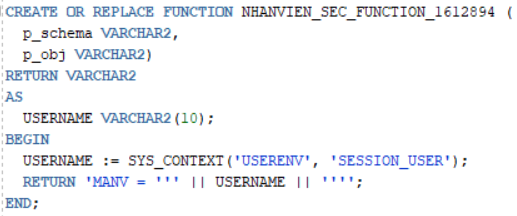




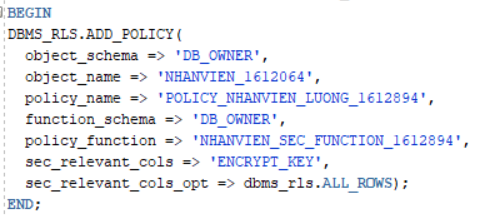
* **Phân quyền truy cập thông tin lương:**

1. Sau khi mã hóa cột lương, ta có thể bỏ đi cột LUONG trong bảng NHANVIEN.
2. Phân quyền: các Nhân viên chỉ được xem khóa mã hóa của chính mình

* Dùng VPD:
* Tạo hàm chính sách trả về vị từ là tên đăng nhập (mã nhân viên) của user đang đăng nhập.

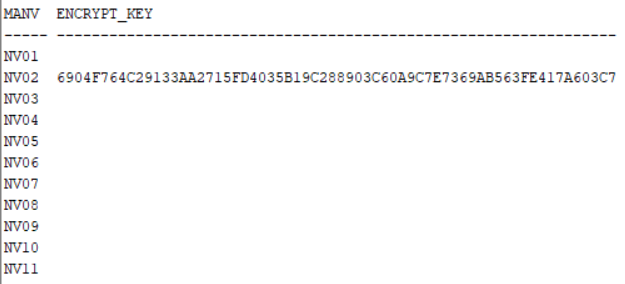


* Gán hàm chính sách vào bảng NHANVIEN, cho phép xem ENCRYPT\_KEY của chính mình, còn của user khác thì null:



* Kiểm tra sự phân quyền dưới tên user NV02 thuộc role Nhân viên:

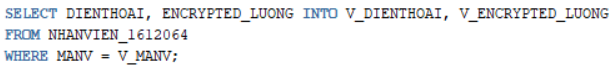




* **Giải mã thông tin lương:** Thủ tục giải mã cột lương trong bảng NHANVIEN bằng khóa của nhân viên đó
* Input: mã nhân viên (V\_MANV), khóa mã hóa của nhân viên (V\_KEY).
* Output: lương của nhân viên đã được giải mã (V\_DECRYPTED\_LUONG) (dạng chuỗi).

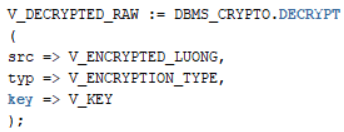
1. Kiểm tra nếu mã nhân viên và khóa nhập vào không khớp với dữ liệu trong bảng NHANVIEN thì trả về chuỗi rỗng.
2. Nếu trùng khớp khóa thì bắt đầu giải mã:

* Lấy thông tin số điện thoại và ENCRYPT\_LUONG của nhân viên này:



* Giải mã ENCRYPT\_LUONG bằng hàm DBMS\_CRYPTO.DECRYPT, với kiểu giải mã (typ) là tổ hợp của thuật toán ENCRYPT\_AES256, kiểu chain CHAIN\_CBC và kiểu padding PAD\_PKCS5 và khóa (key) là khóa ENCRYPT\_KEY của nhân viên đó:





* Kết quả của hàm giải mã trên (V\_DECRYPTED\_RAW) cũng là kết quả XOR lương với số điện thoại của nhân viên, do đó muốn tìm ra lương của nhân viên ta thực hiện lại phép XOR V\_DECRYPTED\_RAW với số điện thoại của nhân viên bằng hàm UTL\_RAW.BIT\_XOR:



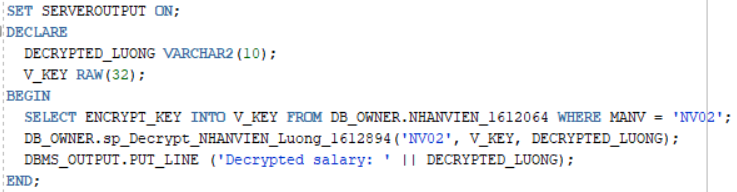
* Trả về giá trị lương (V\_DECRYPTED\_LUONG) sau khi chuyển đổi kết quả XOR sang kiểu chuỗi:



1. Cấp quyền thực thi thủ tục giải mã cho role Nhân viên:



1. Đăng nhập vào user NV02 và thực hiện giải mã:



1. Kết quả:

