Chính sách mã hóa (Encrypt)

- Mã hóa (Encrypt) là biến đổi dữ liệu ban đầu thành dữ liệu khác bằng các thuật toán để che giấu dữ liệu. Là rào cản cuối cùng của kẻ tấn công khi đã vượt qua các cơ chế bảo mật (xác thực người dùng, điều khiển truy cập,...).

- Trong đồ án Mã hóa các thuộc tính của quan hệ:

* NhanVien(luong, phucap)

- Mã hóa bằng thuật toán mã hóa đối xứng AES256 (1 khóa, độ dài khóa là 256 bit). Khóa được tạo cứng từ các kí tự ngẫu nhiên, đảm bảo đủ 256 bit (32 ký tự).

- Chỉ những người dùng có quyền truy xuất dữ liệu của thuộc tính đã được mã hóa mới có thể xem được bản rõ của dữ liệu

- Những người dùng không có quyền truy xuất dữ liệu thì không được xem (kể cả dữ liệu đã mã).  
- Người đảm nhận việc mã hóa là admin.

- Mã hóa dữ liệu ở mức ứng dụng. Bởi vì:

+ Cho phép kiểm soát truy cập và xử lý dữ liệu trực tiếp trong ứng dụng.

+ Đảm bảo rằng chỉ những người có quyền truy cập mới có thể xem và chỉnh sửa dữ liệu lương và phụ cấp.

+ Bảo vệ liệu khỏi các nguy cơ:

• Thiết bị lưu trữ bị đánh cắp

• Chống được tấn công dữ liệu ở mức lưu trữ

• Truy cập dữ liệu bí mật từ người quản trị dữ liệu.

- Thay đổi kiểu dữ liệu: Chuyển đổi kiểu dữ liệu của trường lương và phụ cấp từ số sang dạng chuỗi để lưu trữ dữ liệu đã được mã hóa. Thay cột "LUONG NUMBER(18,2)" bằng cột "LUONG VARCHAR2(2000)".

- Quản lý khóa:

+ Thiết lập khóa: tạo khóa ngẫu nhiên mỗi lần mã hóa.  
+ Lưu trữ khóa: tạo thêm bảng để lưu trữ khóa trong cơ sở dữ liệu.

+ Khôi phục khóa: sao lưu khóa tại một bảng khác mỗi lần thiết lập. Khi bảng lưu khóa chính gặp sự cố, có thể khôi phục khóa từ bản sao lưu

+ Thay khóa đồng loạt sau một thời gian: khóa sẽ được thay sau mỗi lần mã hóa và giải mã. Tức là khi mã hóa khóa sẽ được tạo ngẫu nhiên và lưu trữ lại, sau khi giải mã xong khóa sẽ được xóa đi.