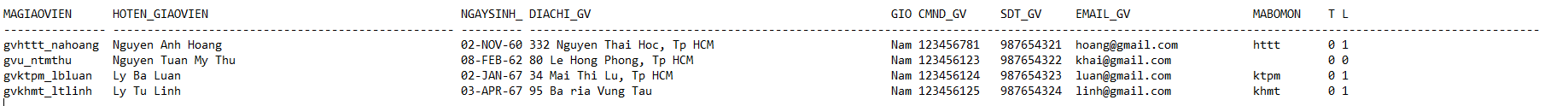
Cột dữ liệu được đem ra làm mẫu để mã hóa dữ liệu trên cột là cột EMAIL\_GV của bảng giảng viên, đây không phải là cột dữ liệu quan trọng nhưng mà vì độ dài của dữ liệu thỏa mãn chuỗi kí tự sau khi mã hóa lưu vào trong database.

Bảng dữ liệu thô ban đầu khi chưa mã hóa là



Loại mã hóa nhóm em sử dụng là mã hóa theo thuật toán mã hóa(PLS\_INTEGER), kiểu dữ liệu là RAW.

Trước khi tạo hàm mã hóa thì cần tạo một package để chứa các thành phần như key, hàm mã hóa, hàm giải mã.

CREATE OR REPLACE EDITIONABLE PACKAGE NV\_ENCRYPT IS

FUNCTION ENCRYPT\_(inputData IN VARCHAR2) RETURN RAW DETERMINISTIC;

FUNCTION DECRYPT\_(inputEncryptData IN RAW) RETURN VARCHAR2 DETERMINISTIC;

END;

/

DETERMINISTIC là dùng để xác định kiểu trả về đó là thuộc vòa trong function đó.

Tiếp theo là khởi tạo thuật toán mã hóa, ở đây dùng các thuật toán có sẵn mà ORACLE có cung cấp cho là:

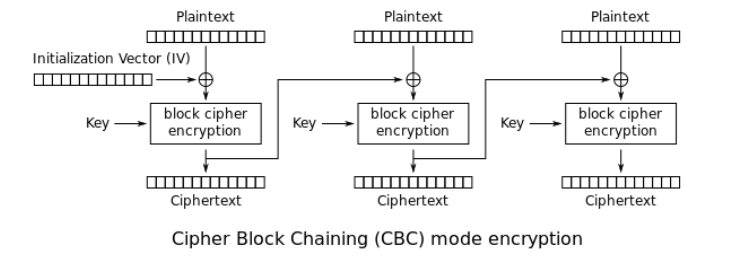
encrypt\_Type PLS\_INTEGER :=DBMS\_CRYPTO.ENCRYPT\_DES

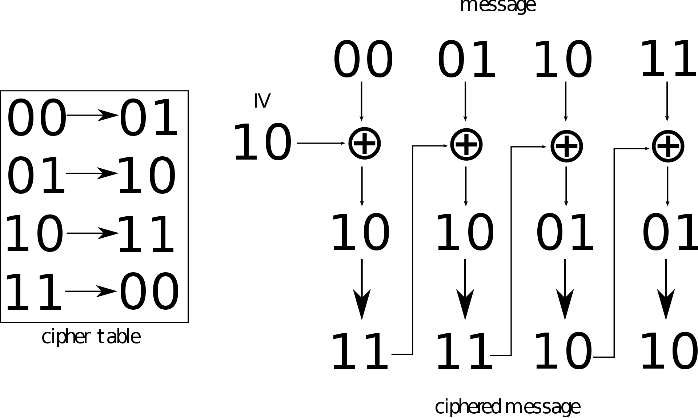
+DBMS\_CRYPTO.CHAIN\_CBC

+DBMS\_CRYPTO.PAD\_PKCS5;

DBMS\_CRYPTO.ENCRYPT\_DES: dùng chuẩn mã hóa cơ bản của phương pháp mã hóa bằng mật mã, chỉ sử dụng 1 key có độ dài là 7 bytes.

DBMS\_CRYPTO.CHAIN\_CBC: khi mã hóa thì dữ liệu sẽ bị chia thành các khối(block) được XOR với block ciphertext trước(key mã hóa) để tạo ra được một block ciphertext.

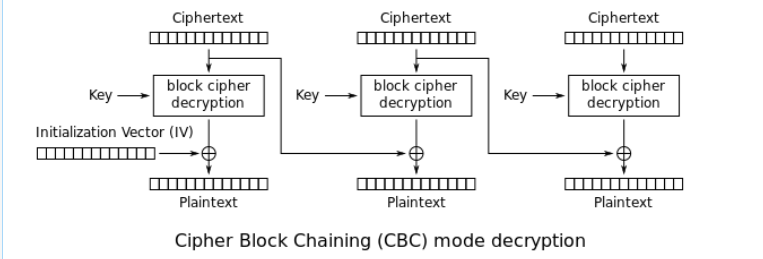




DBMS\_CRYPTO.PAD\_PKCS5: các cipher block được tạo ra cần có kích thước, ở đây không có tạo size cho cipher block nên cần có thuật toan đệm padding cho block.

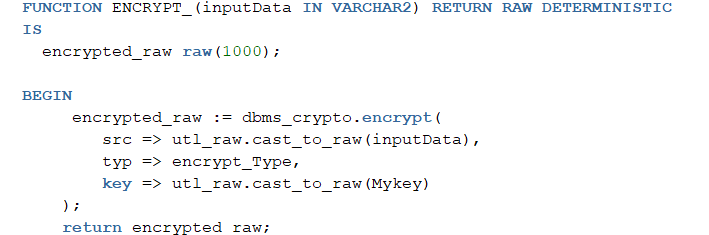
Sau khi mã hóa sử dụng thuật toán mã hóa thì sẽ được chuỗi có độ dài là 32 bytes.

Hàm giải mã được nằm trong cùng một block nên thuật toán giải mã sẽ được áp dụng giống với khi mã hóa nhưng theo chiều ngược lại:

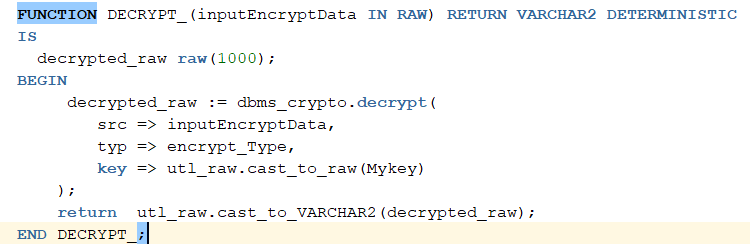


Cần có khởi tạo key mã hóa phía bên trong của package để tạo sự đồng nhất về key của mã hóa và giải mã.

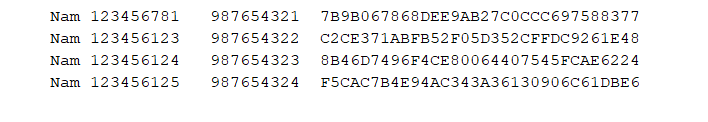
Hàm mã hóa là:



Hàm giải mã là:



Sau khi thực hiện mã hóa chuỗi EMAIL\_GV của bảng GIAOVIEN thì ta được kết quả là:



Sau khi thực hiện phép chọn trên bảng giáo viên và chỉ chọn giải mã dữ liệu đọc lên chứ không giải mã dữ liệu gốc thì được kết quả là:

