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

MAGIAOVIEN	HOTEN_GIAOVIEN	NGAYSINH_ DIACHI_GV	GIO CMND_GV	SDT_GV	EMAIL_GV	MABOMON	
	Nguyen Anh Hoang	02-NOV-60 332 Nguyen Thai Hoc, Tp HCM			hoang@gmail.com	httt	0 1
gvu_ntmthu	Nguyen Tuan My Thu	08-FEB-62 80 Le Hong Phong, Tp HCM	Nam 123456123	987654322	khai@gmail.com		0 0
gvktpm_lbluan	Ly Ba Luan	02-JAN-67 34 Mai Thi Lu, Tp HCM	Nam 123456124	987654323	luan@gmail.com	ktpm	0 1
gvkhmt_ltlinh	Ly Tu Linh	03-APR-67 95 Ba ria Vung Tau	Nam 123456125	987654324	linh@gmail.com	khmt	0 1

Loại mã hóa nhóm em sử dụng là mã hóa theo thuật toán mã hóa(PLS\_INTEGER), kiểu dữ liêu 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:

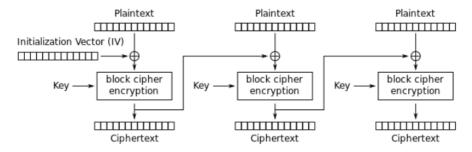
```
encrypt_Type PLS_INTEGER :=DBMS_CRYPTO.ENCRYPT_DES

+DBMS_CRYPTO.CHAIN_CBC

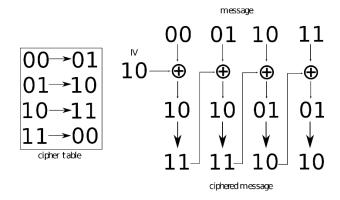
+DBMS_CRYPTO.PAD_PKCS5;
```

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.



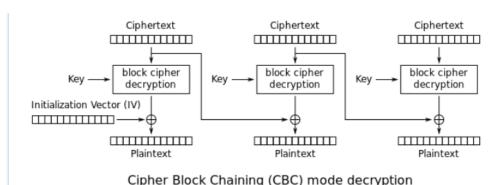
Cipher Block Chaining (CBC) mode encryption



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:

END DECRYPT ;

```
FUNCTION ENCRYPT (inputData IN VARCHAR2) RETURN RAW DETERMINISTIC
    encrypted raw raw(1000);
  BEGIN
       encrypted_raw := dbms_crypto.encrypt(
          src => utl raw.cast to raw(inputData),
          typ => encrypt_Type,
          key => utl raw.cast to raw(Mykey)
      );
      return encrypted raw;
Hàm giải mã là:
 FUNCTION DECRYPT (inputEncryptData IN RAW) RETURN VARCHAR2 DETERMINISTIC
   decrypted raw raw(1000);
 BEGIN
      decrypted raw := dbms crypto.decrypt(
         src => inputEncryptData,
         typ => encrypt_Type,
         key => utl raw.cast to raw(Mykey)
     );
```

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

return utl raw.cast\_to\_VARCHAR2(decrypted\_raw);

```
Nam 123456781 987654321 7B9B067868DEE9AB27C0CCC697588377
Nam 123456123 987654322 C2CE371ABFB52F05D352CFFDC9261E48
Nam 123456124 987654323 8B46D7496F4CE80064407545FCAE6224
Nam 123456125 987654324 F5CAC7B4E94AC343A36130906C61DBE6
```

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:

##