Tóm tắt nội dung thuật toán AES

Tổng quan.

* AES (viết tắt của từ tiếng anh: Advanced Encryption Standard, hay Tiêu chuẩn mã hóa nâng cao) là một thuật toán mã hóa khối được chính phủ Hoa Kỳ áp dụng làm tiêu chuẩn mã hóa.
* Thuật toán được xây dựng dựa trên Rijndael Cipher phát triển bởi 2 nhà mật mã học người Bỉ: Joan Daemen và Vincent Rijmen.
* AES làm việc với các khối dữ liệu 128bit và độ dài khóa 128bit, 192bit hoặc 256bit. Các khóa mở rộng sử dụng trong chu trình được tạo ra bởi thủ tục sinh khóa Rijndael.
* Hầu hết các phép toán trong thuật toán AES đều thực hiện trong một trường hữu hạn của các byte. Mỗi khối dữ liệu đầu vào 128bit được chia thành 16byte, có thể xếp thành 4 cột, mỗi cột 4 phần tử hay một ma trận 4×4 của các byte, nó gọi là ma trận trạng thái.
* Tùy thuộc vào độ dài của khóa khi sử dụng 128bit, 192bit hay 256bit mà thuật toán được thực hiện với số lần lặp khác nhau.

Các bước xử lý chính.

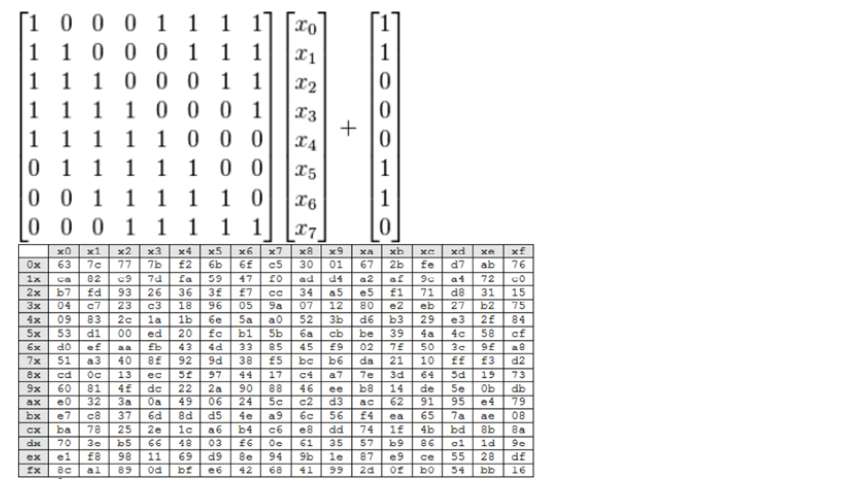
* Quá trình mở rộng khóa sử dụng thủ tục sinh khóa Rijndael.
* Quá trình mã hóa.

# Xây dựng thuật toán.

## 1. Xây dựng bảng S-box.

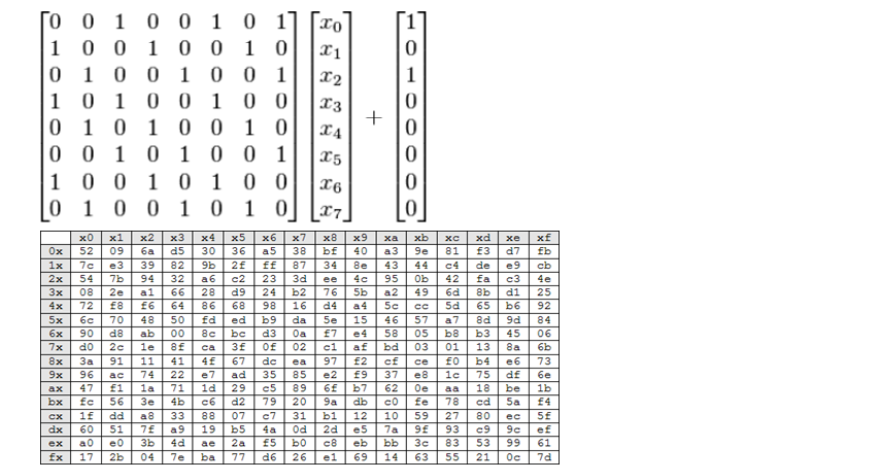
### a. Bảng S – box thuận.

* Bảng S-box thuận được sinh ra bằng việc xác định nghịch đảo cho một giá trị nhất định trên GF(28) = GF(2)[x] / (x8+x4+x3+x+1) (trường hữu hạn Rijindael). Giá trị 0 không có nghịch đảo thì được ánh xạ với 0. Những nghịch đảo được chuyển đổi thông qua phép biến đổi affine.
* Công thức tính các giá trị bảng S-box và bảng S- box tương ứng:



### b. Bảng S-box nghịch đảo.

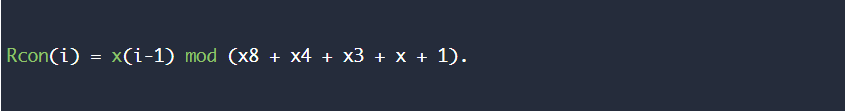
* S-box nghịch đảo chỉ đơn giản là S-box chạy ngược. Nó được tính bằng phép biến đổi affine nghịch đảo các giá trị đầu vào. Phép biến đổi affine nghịch đảo được biểu diễn như sau:



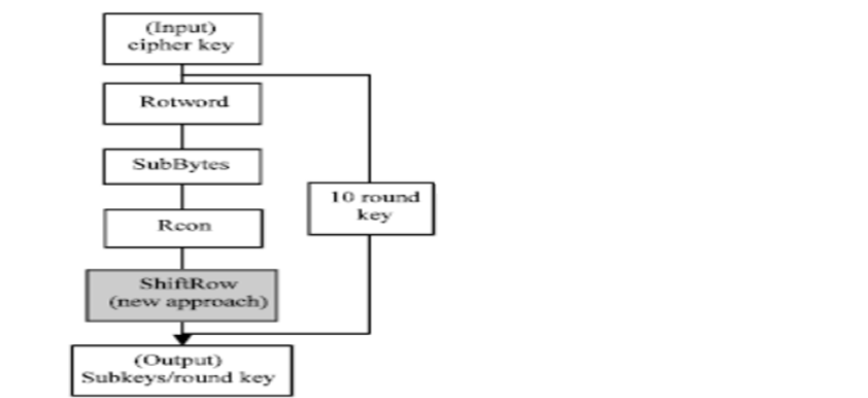
2. Giải thuật sinh khóa phụ.

Quá trình sinh khóa gồm 4 bước:

* Rotword: quay trái 8 bít
* SubBytes
* Rcon: tính giá trị Rcon(i) Trong đó :

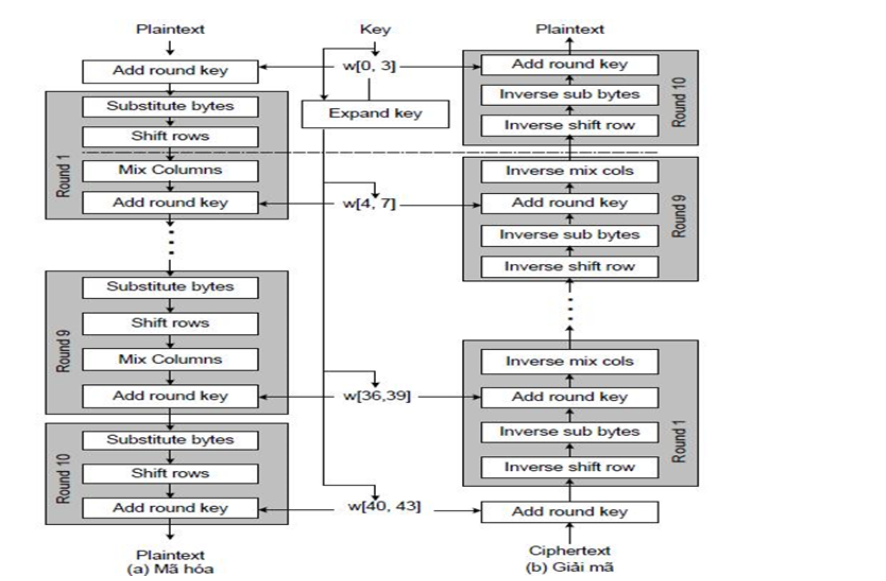


* ShiftRow



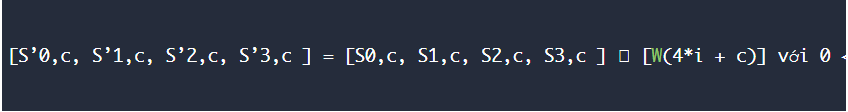
## 3. Quá trình mã hóa.

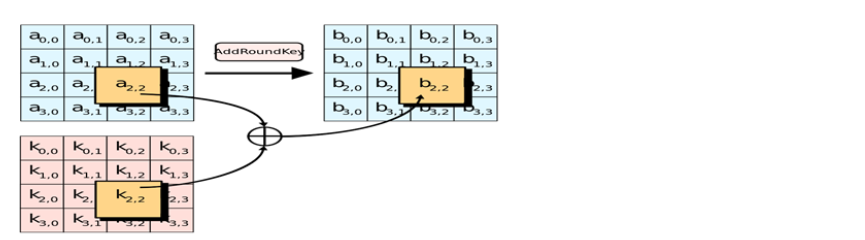
## a. Sơ đồ tổng quát.



### b. Hàm AddRoundKey.

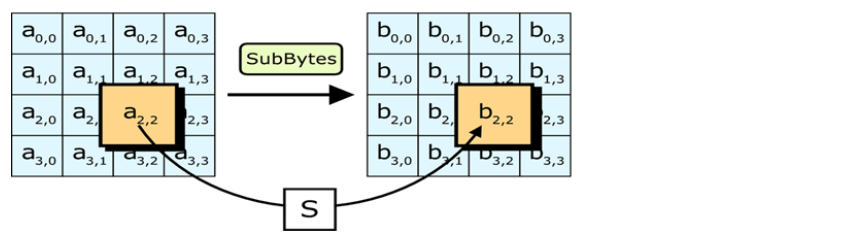
* Được áp dụng từ vòng lặp thứ 1 tới vòng lặp Nr
* Trong biến đổi Addroundkey(), một khóa vòng được cộng với state bằng một phép XOR theo từng bit đơn giản.
* Mỗi khóa vòng gồm có 4 từ (128 bit) được lấy từ lịch trình khóa. 4 từ đó được cộng vào mỗi cột của state, sao cho:





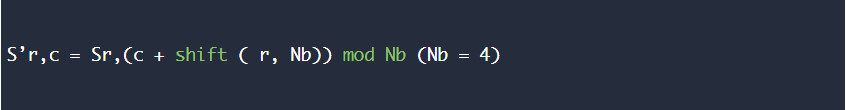
### c. Hàm SubBytes.

* Biến đổi SubBytes() thay thế mỗi byte riêng rẽ của state Sr,c bằng một giá trị mới S’ r,c sử dụng bảng thay thế (S – box) được xây dựng ở trên.

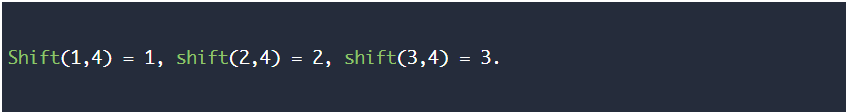


### d. Hàm ShiftRow.

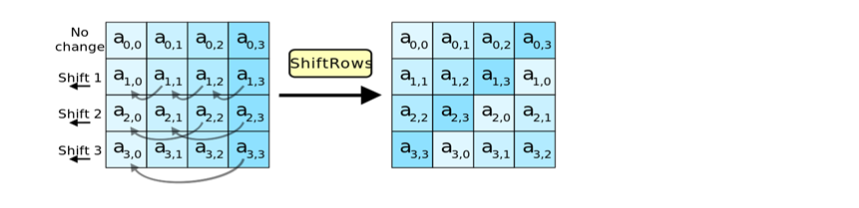
* Trong biến đổi ShiftRows(), các byte trong ba hàng cuối cùng của trạng thái được dịch vòng đi các số byte khác nhau (độ lệch). Cụ thể :



* Trong đó giá trị dịch shift (r, Nb) phụ thuộc vào số hàng r như sau:



* Hàng đầu tiên không bị dịch, ba hàng còn lại bị dịch tương ứng:
  + Hàng thứ 1 giữ nguyên.
  + Hàng thứ 2 dịch vòng trái 1 lần.
  + Hàng thứ 3 dịch vòng trái 2 lần.
  + Hàng thứ 4 dịch vòng trái 3 lần.



### e. Hàm MixColumns.

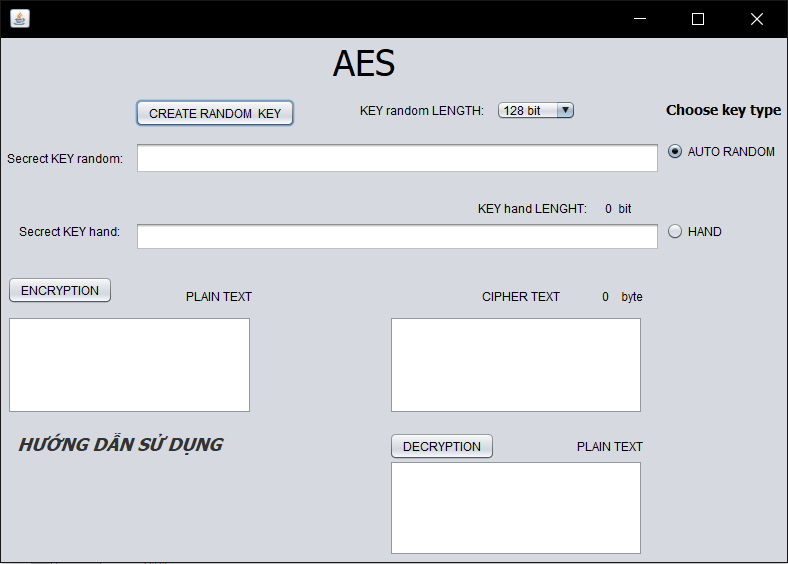
* Biến đổi MixColumns() tính toán trên từng cột của state. Các cột được coi như là đa thức trong trường GF(28) và nhân với một đa thức a(x) với:



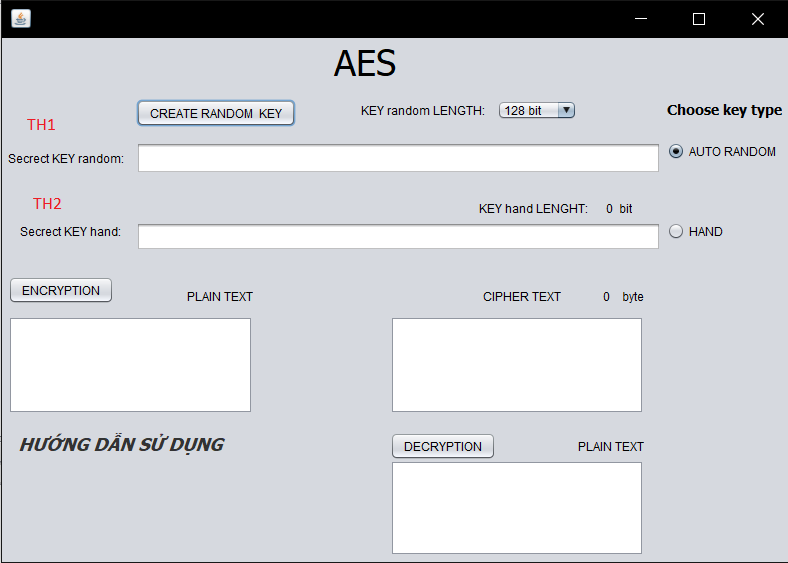
* Biến đổi này có thể được trình bày như phép nhân một ma trận, mà mỗi byte được hiểu như là một phần tử trong trường GF(28): s’(x) = a(x) ⊗ s(x):
* Mô tả bằng ma trận như sau :



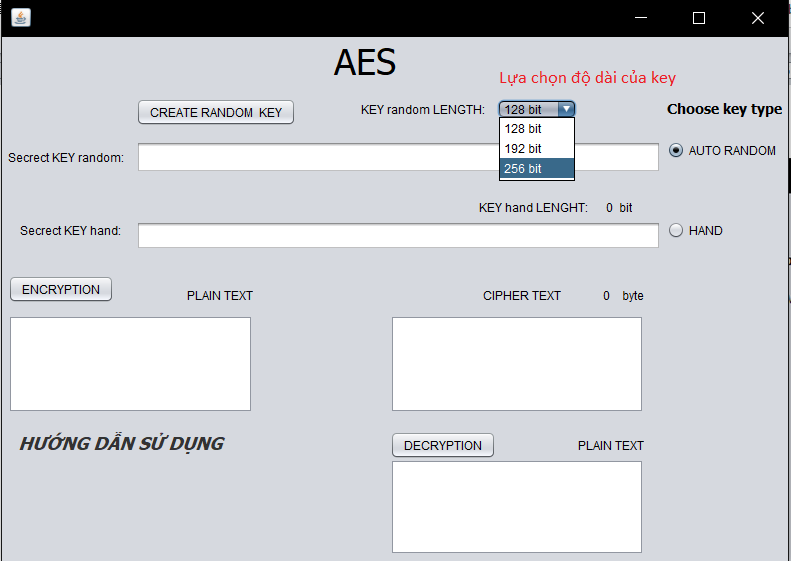
Demo mã hóa thuật toán AES



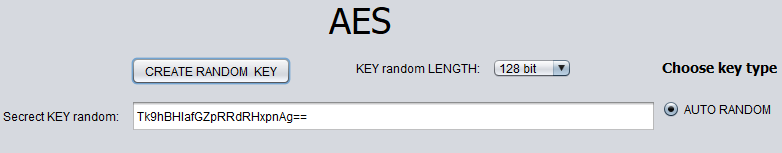
Đầu tiên chúng ta có 2 loại key là key random và key hand thì chúng ta sẽ chia làm 2 trường hợp TH1 là key random và trường hợp TH2 là key hand

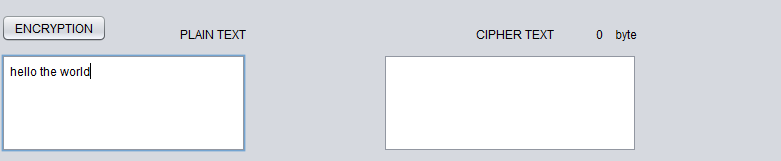


Nào cùng bắt đầu với TH1 nhé:

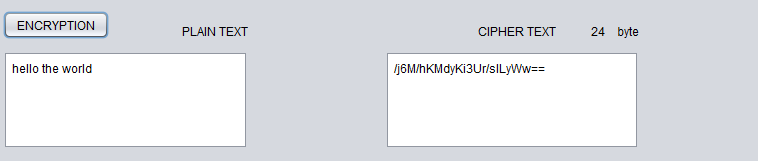
Bước 1: Chúng ta sẽ tạo một đoạn key random tùy theo số bit chung ta lựa chọn như hình 

và bấm nút **CREATE RANDOM KEY**

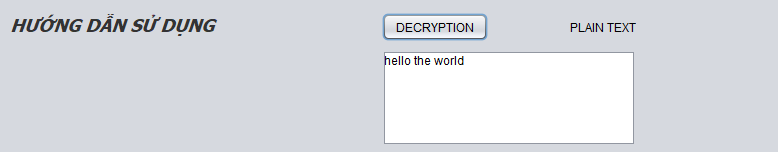


Bước 2 : Chúng ta nhập đoạn mã chúng ta muốn mã hóa vào ô PLAIN TEXT

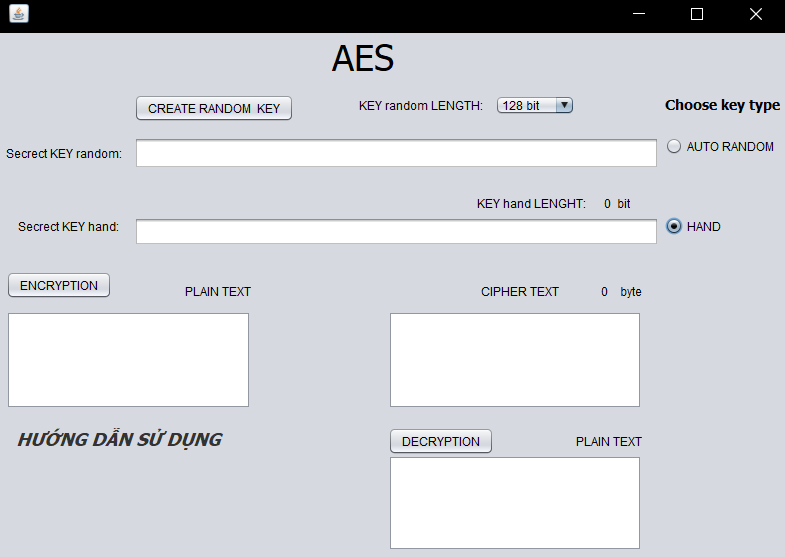
Sau đó nhận nút ENCRYPTION để mã hóa



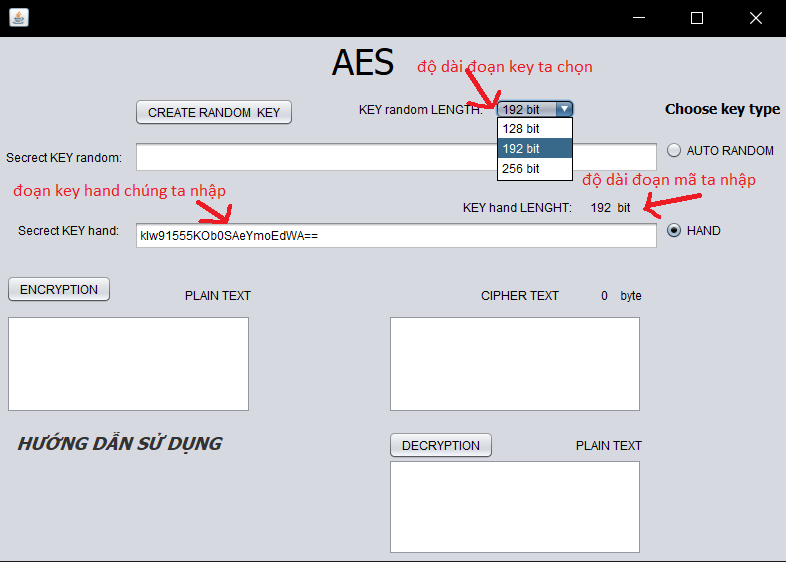
Bước 3: Nếu bạn muốn từ Cipher text quay trở lại plain text thì bấm nút DECRYPTION nó sẽ giải mã đoạn cho bạn



Đến với trường hợp thứ 2 : Chúng ta sẽ chọn kiểu key là key hand như hình

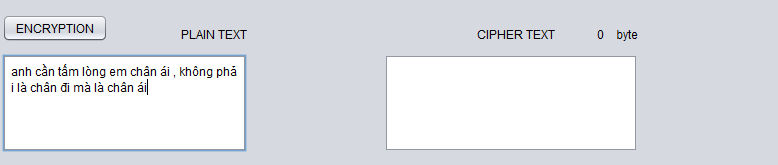


Và lúc này key hand chung ta nhập vào phải có độ dài là 128bit ,192bit ,256bit như hình

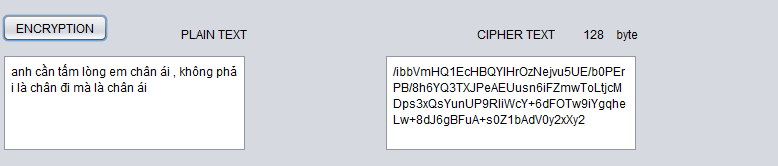


Bước 1: chúng ta nhập đoạn mã có độ dài như ta đã chọn như hình trên

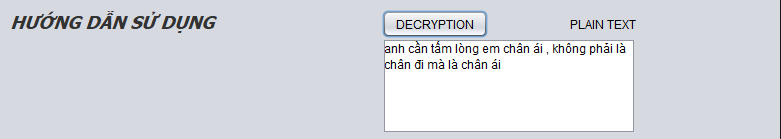
Bước 2: Chúng ta sẽ nhập đoạn mã muốn mã hóa vào ô PLAINT TEXT



Và nhấn nút ENCRYPTION để mã hóa đoạn text đó.

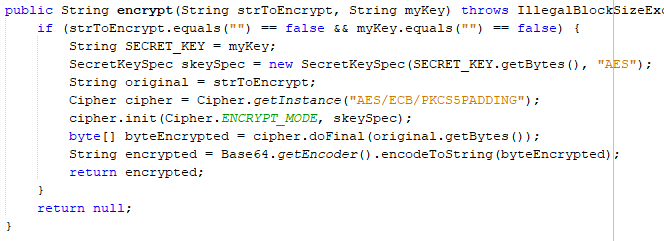


Bước 3: Nếu chúng ta muốn từ cipher text quay lại plaint text thì chúng ta nhấn nút DECRYTION

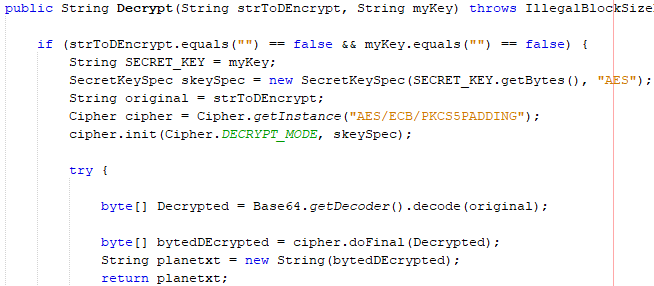


**CODE:**

Code mã hóa AES.

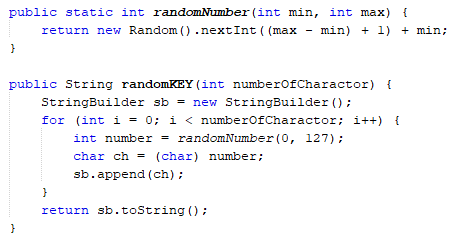


Code giải mã AES.



Code sinh KEY random

Sinh random



Tạo key sau khi sinh random

Sau đó hiển thị Key ra dạng mã hóa của Base64

