**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN 1**

****

**Môn: THỰC TẬP CƠ SỞ**

**BÁO CÁO BÀI THỰC HÀNH SỐ 16**

**Họ và tên sinh viên:**

**Đỗ Tiến Sĩ**

**Mã số sinh viên:**

**B20DCAT153**

**Bài 16: Lập trình thuật toán mật mã học cơ sở.**

**Họ và tên giảng viên:**

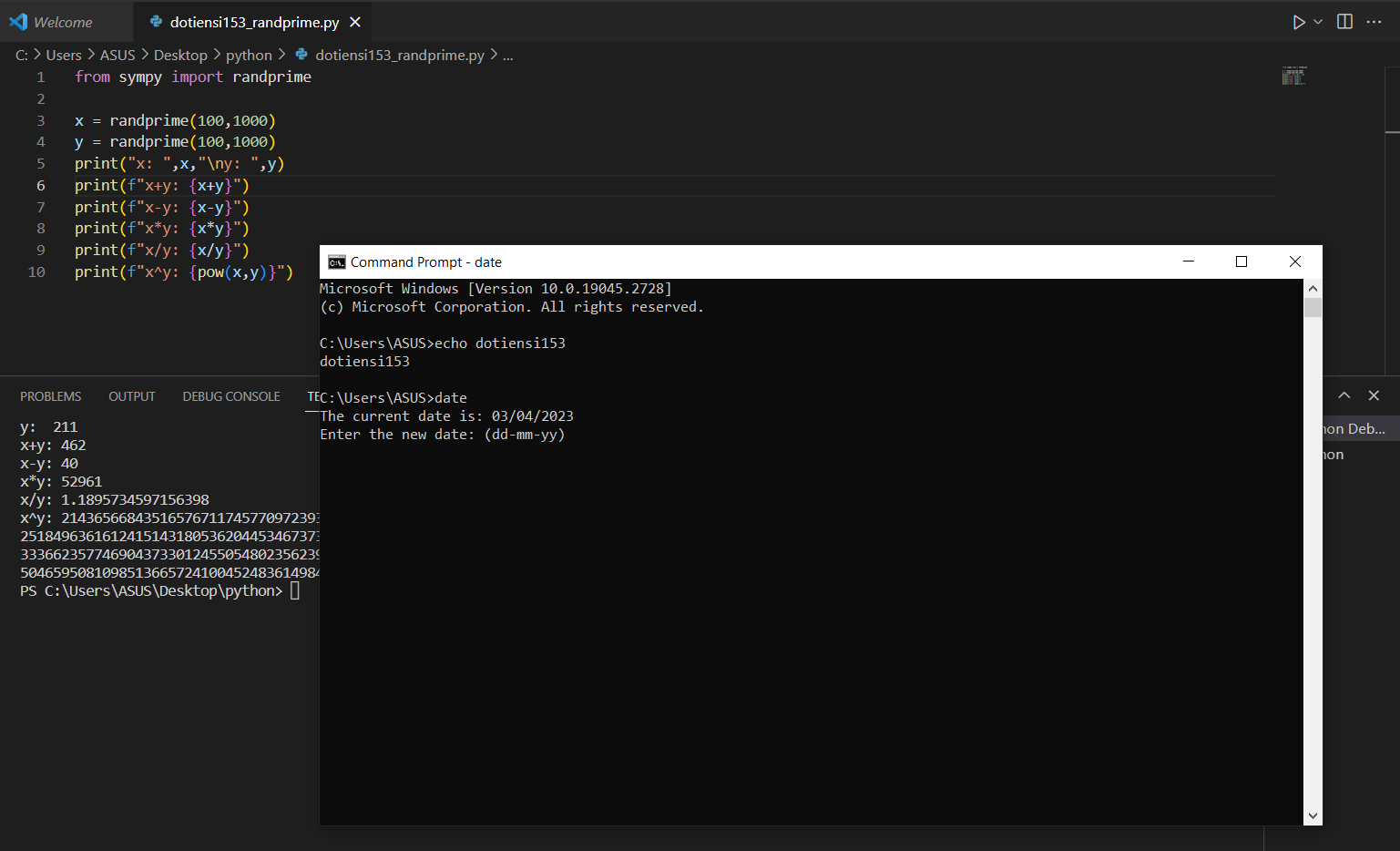
**Thầy: Đỗ Xuân Chợ**

**Hà Nội 3/2023 (tháng/năm)**

Để lập trình thư viện RSA ta dùng các hàm có sẵn trên python

- Thư viện sympy hỗ trợ random số nguyên tố: randprime

Chứng minh hàm randprime hoạt động ổn với các phép toán thông trường.



1. Lập trình thư viện số lớn với các phép toán cơ bản để sử dụng trong

giải thuật mã hóa/giải mã RSA

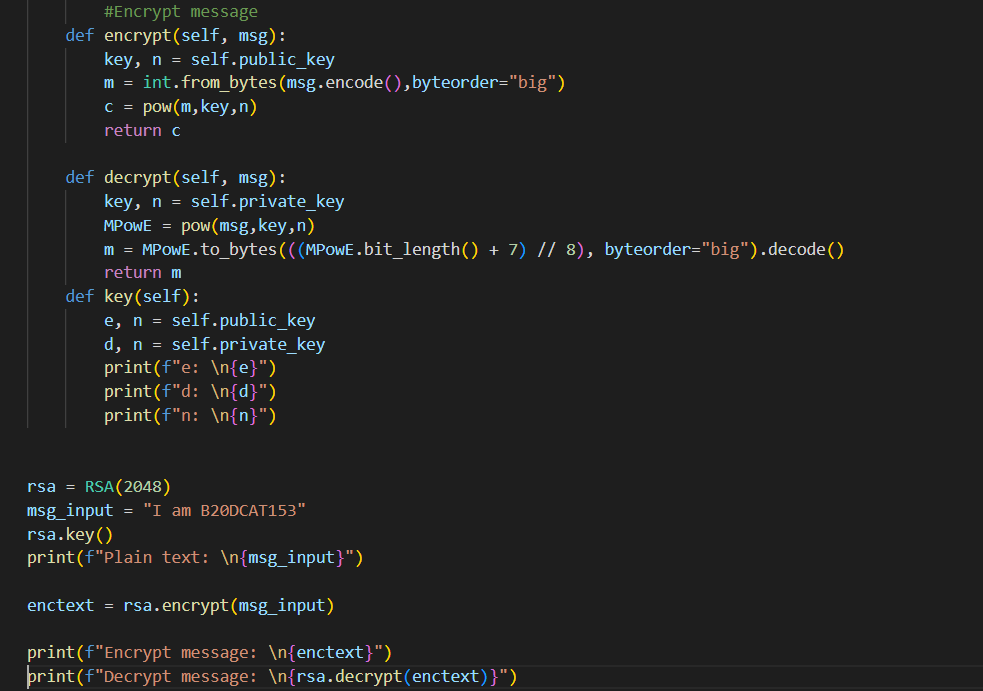
Tạo class và hàm sinh khóa:

Random số nguyên tố 1024 bit để tăng tính bảo mật cho RSA

Graphical user interface, text

Description automatically generated

Hàm mã hóa, hàm giải mã và hàm main:



Thử nghiệm mã hóa và giải mã chuỗi ký tự: “I am <ma\_sv>”

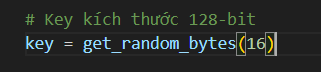
Text

Description automatically generated

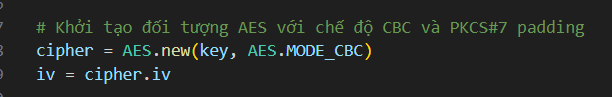
Thuật Toán AES:

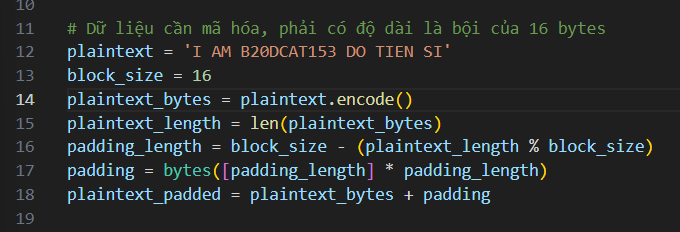
Ta sử dụng thư viện pycryptodome để thực hiện chế độ mà sử dụng là CBC và PKCS#7 padding.

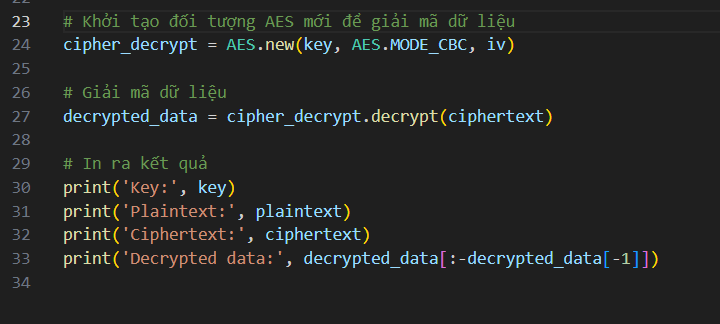
Bước 1: ta tạo khóa key kích thước 128 bit sử dụng:



Bước 2: khởi tạo đối tượng với:



Bước 3: ta tạo 1 dữ liệu để nhập vào làm sao cho ứng dụng đúng độ dài của thuật toán:  


Bước 4: cuối cùng là mã hóa và ghi dữ liệu ra màn hình  


KẾT QUẢ:  
