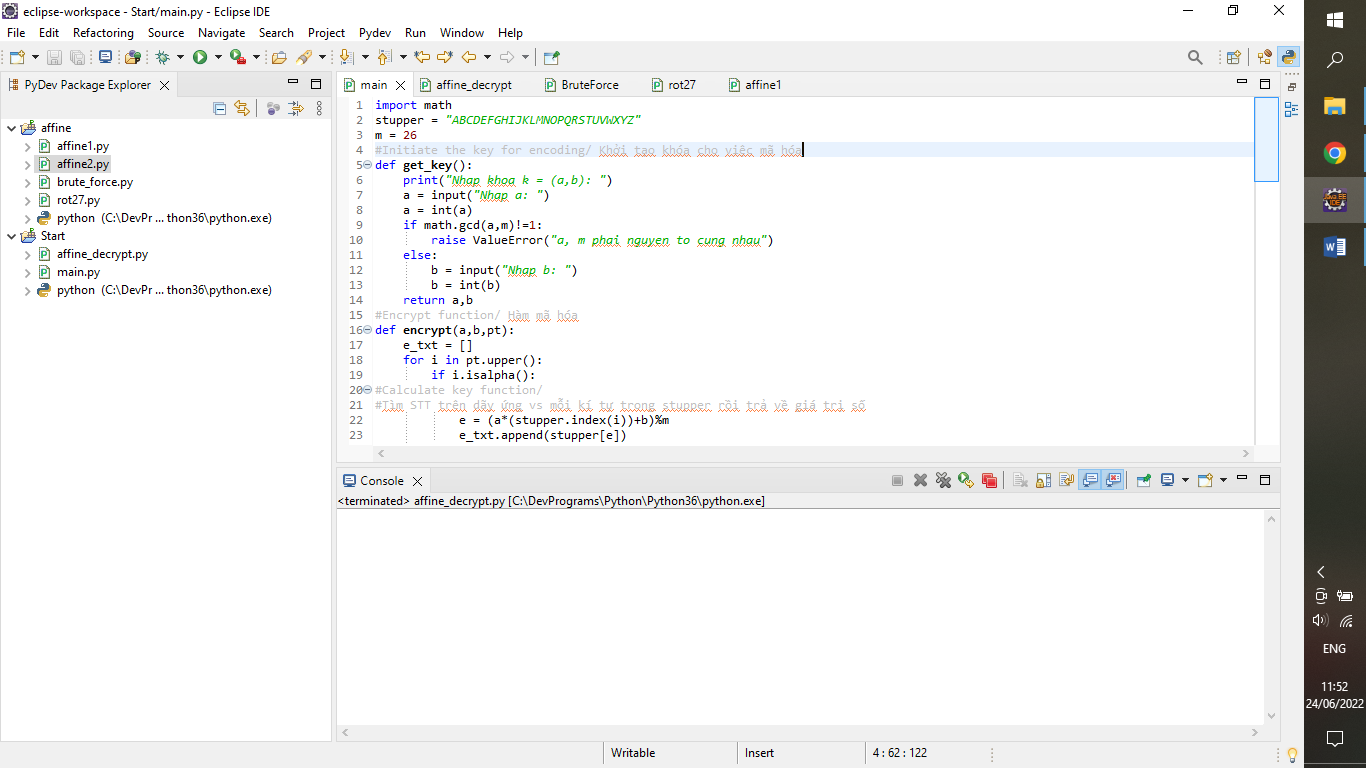
1. Mã hóa:

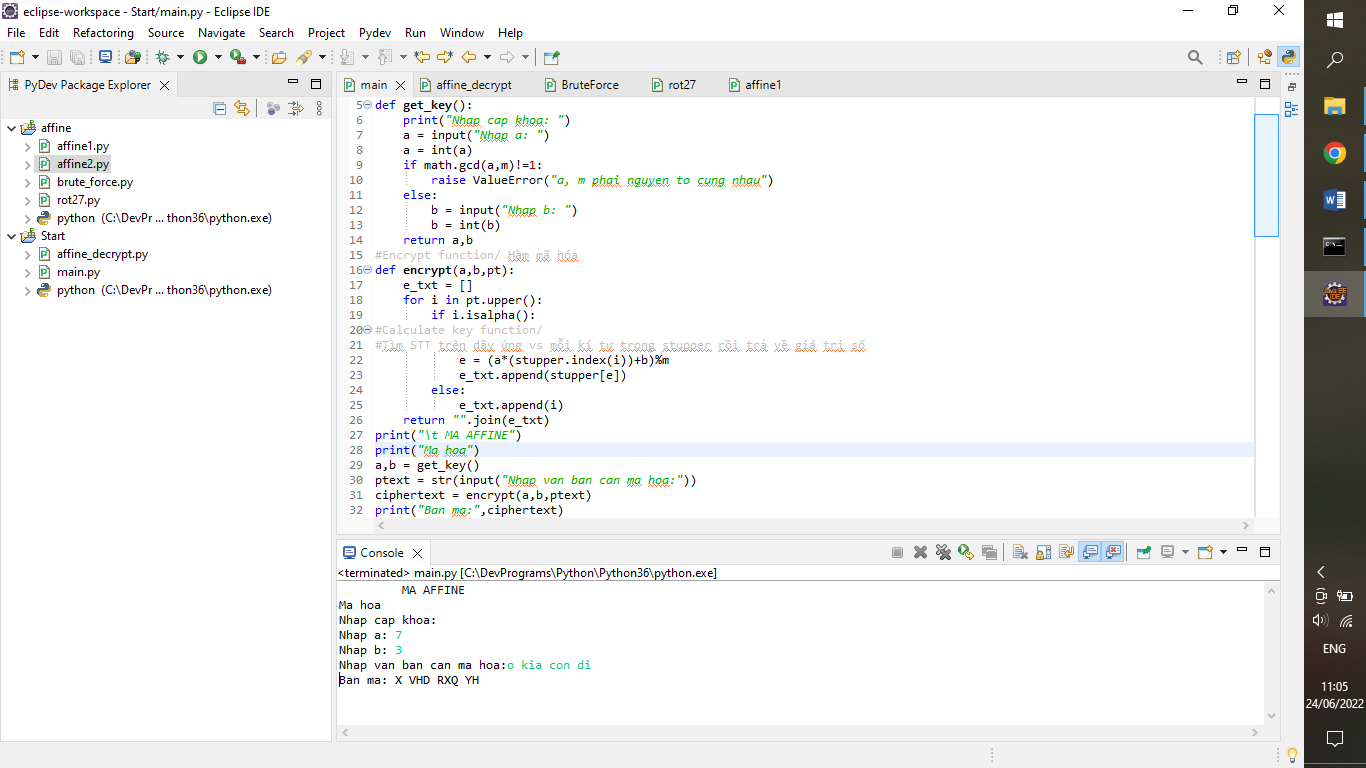
Đầu tiên ta khai báo biến chuỗi gồm 26 ký tự trong bảng chữ cái Latinh từ A – Z để đối chiếu.

Khởi tạo cặp khóa với a phải là số nguyên tố cùng nhau với 26; a và b thuộc Z26

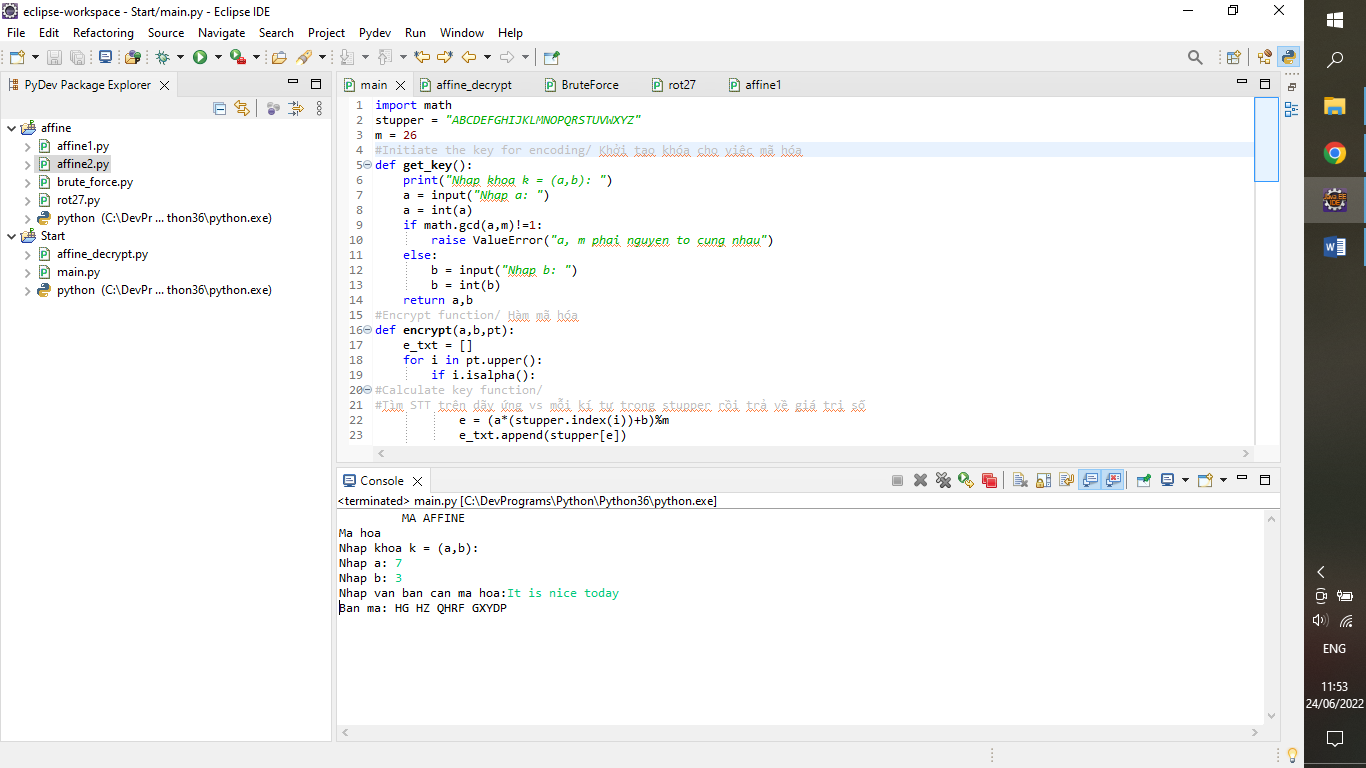


Ở vòng lặp for, biến i chạy hết chiều dài bản rõ dưới dạng chữ hoa nhập từ bàn phím thì dừng lại.

Nếu ký tự bản rõ là chữ cái thì sẽ thực hiện phép toán: [a\*(x + b)] mod 26 với x là số thứ tự trên bảng chữ cái của kí tự thứ i trong bản rõ dưới dạng [biến chuỗi bảng chữ cái].index(i)



Kết quả:



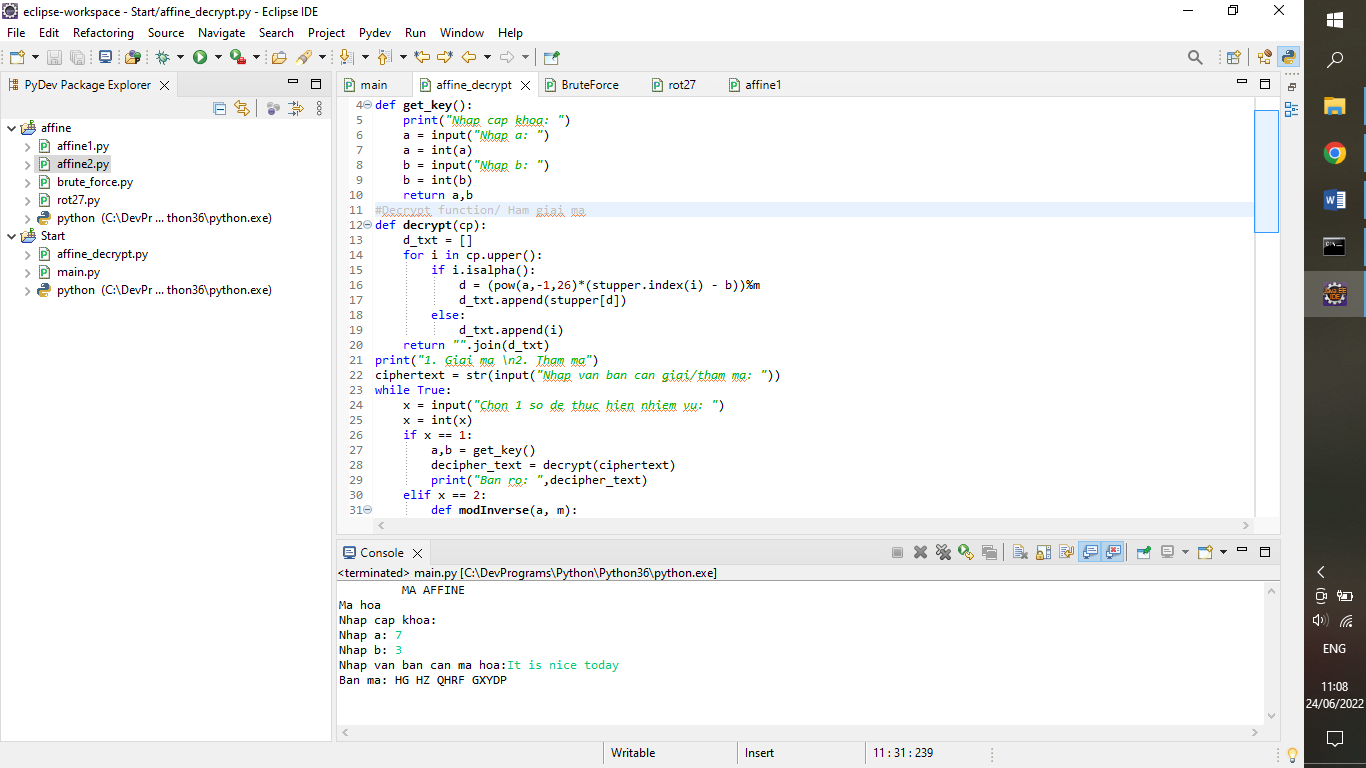
2. Giải mã:

Với khóa đã nhận từ người gửi, ta có thể dễ dàng giải bản mã

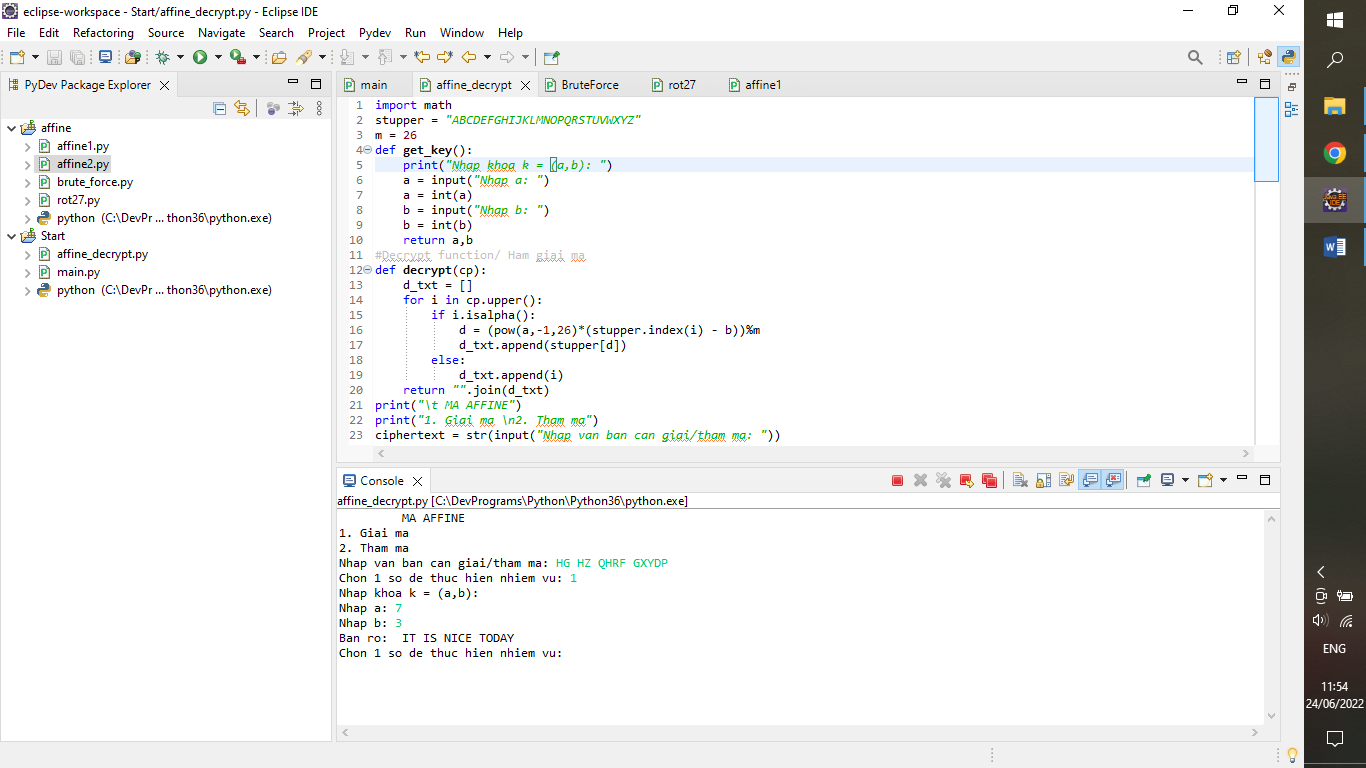
Ở vòng lặp for, biến i chạy hết chiều dài bản mã dưới dạng chữ hoa

Nếu ký tự bản mã là chữ cái, thực hiện phép toán [a-1\*(y – b)] mod 26 với y là số thứ tự trên bảng chữ cái của kí tự thứ i trong bản rõ dưới dạng [biến chuỗi bảng chữ cái].index(i)

a-1 là số nghịch đảo của a theo mod 26 /(a\*a-1 = 1 (mod 26))



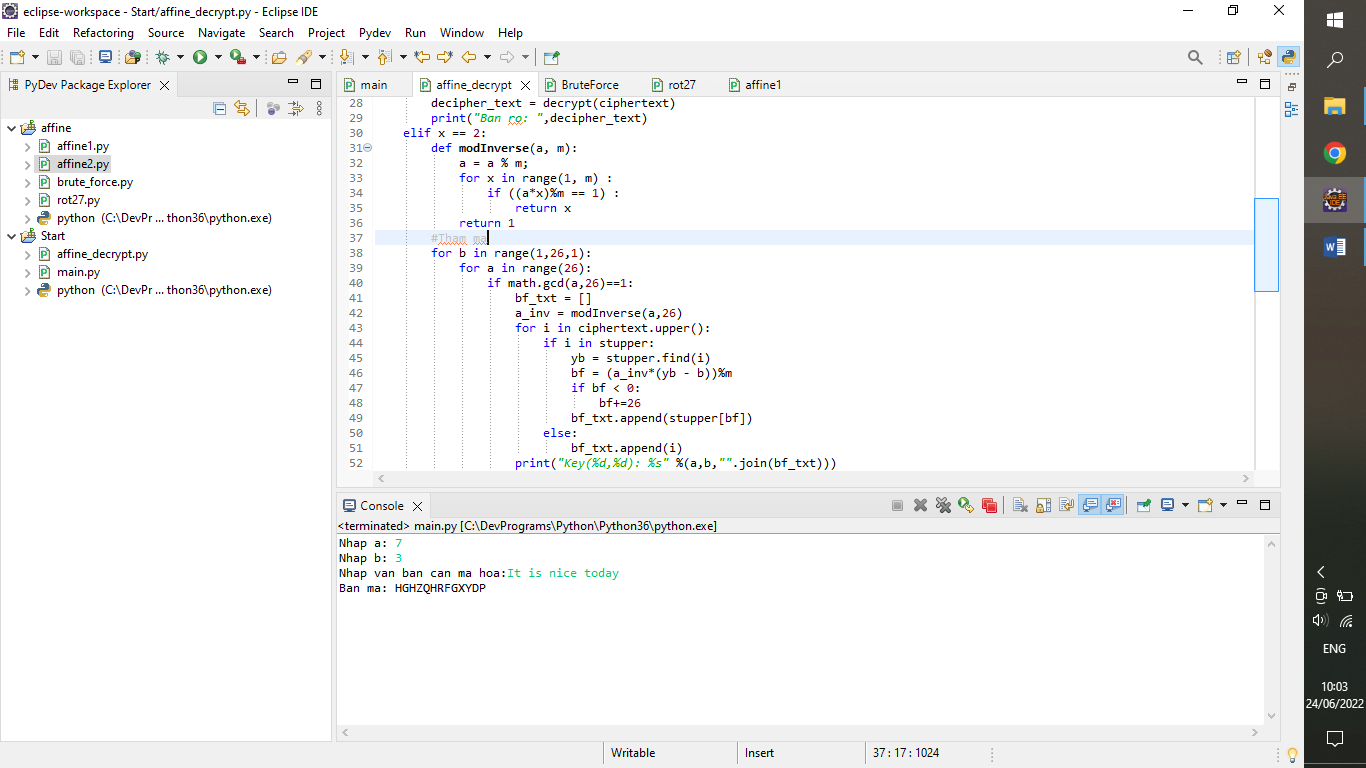
Kết quả:



3. Thám mã:

Đã biết mã Affine sử dụng cặp khóa nằm trong không gian Z26, ta có không gian khóa gồm 12\*26 = 312 phần tử (a phải nguyên tố cùng nhau với 26 => a nhận 12 giá trị).

Tương tự với công thức tính của hàm giải mã yd = [a-1\*(y – b)] mod 26, thám mã theo cách này sẽ liệt kê toàn bộ 312 khóa để xem cặp khóa nào cho ra bản rõ.



Kết quả:

