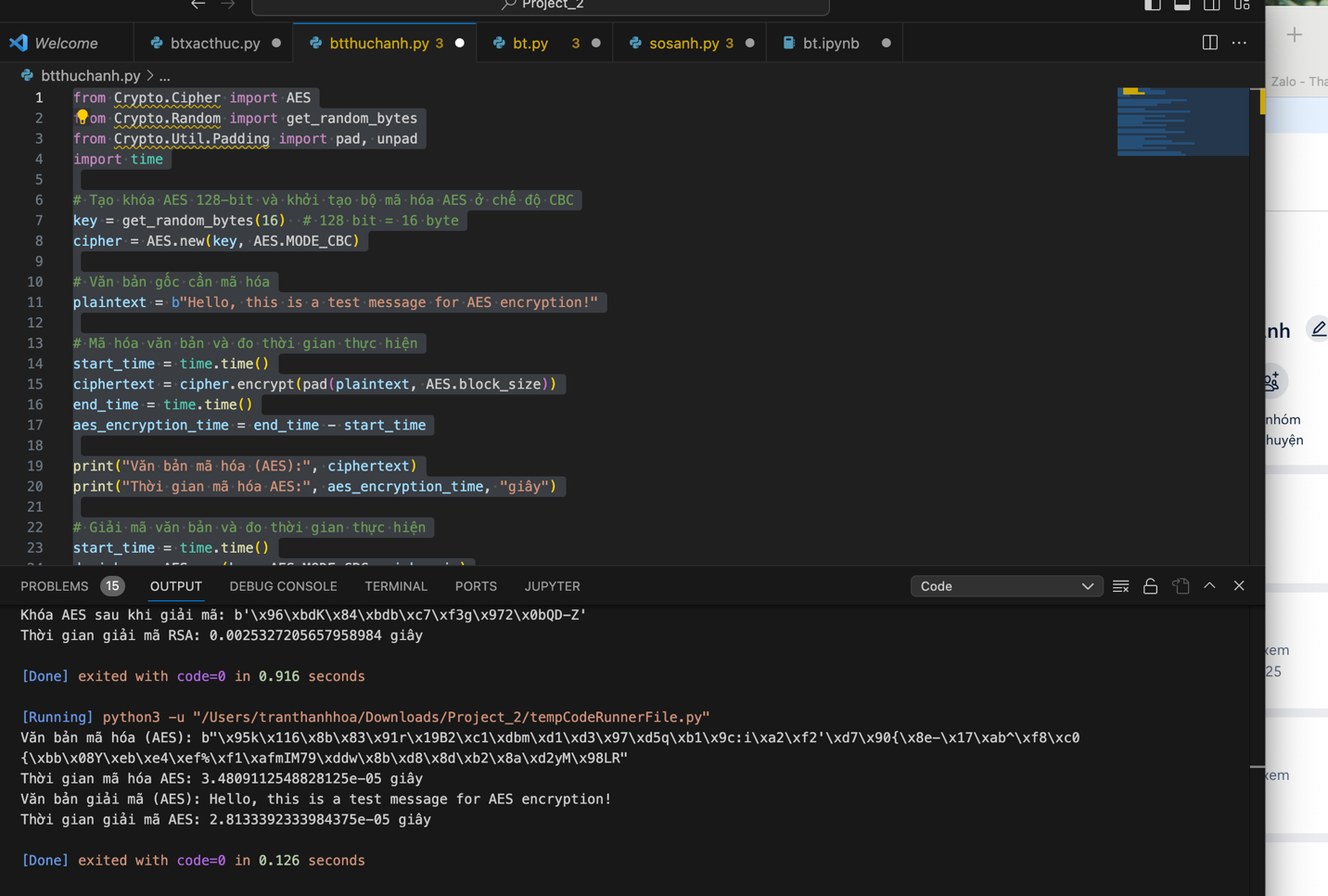
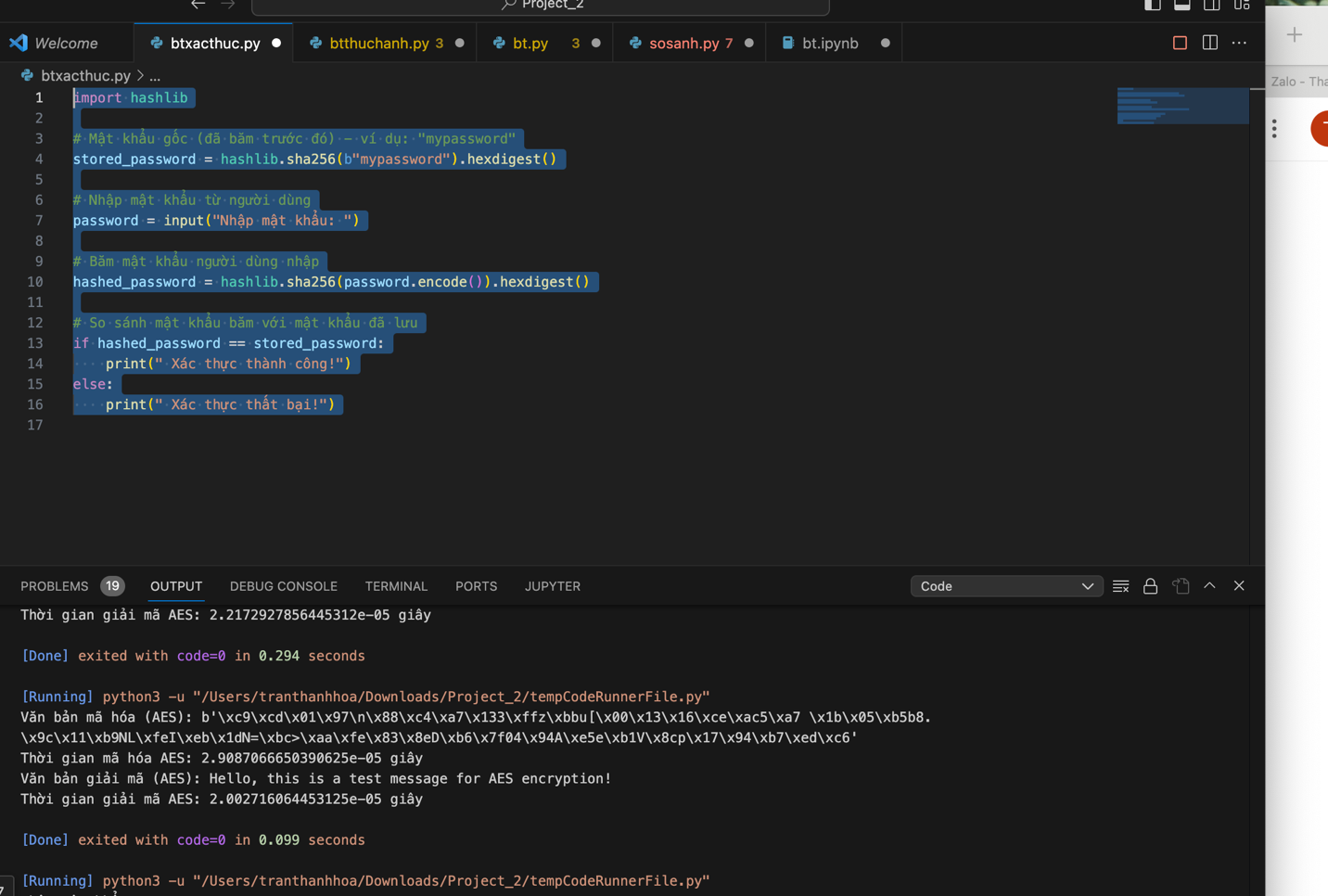
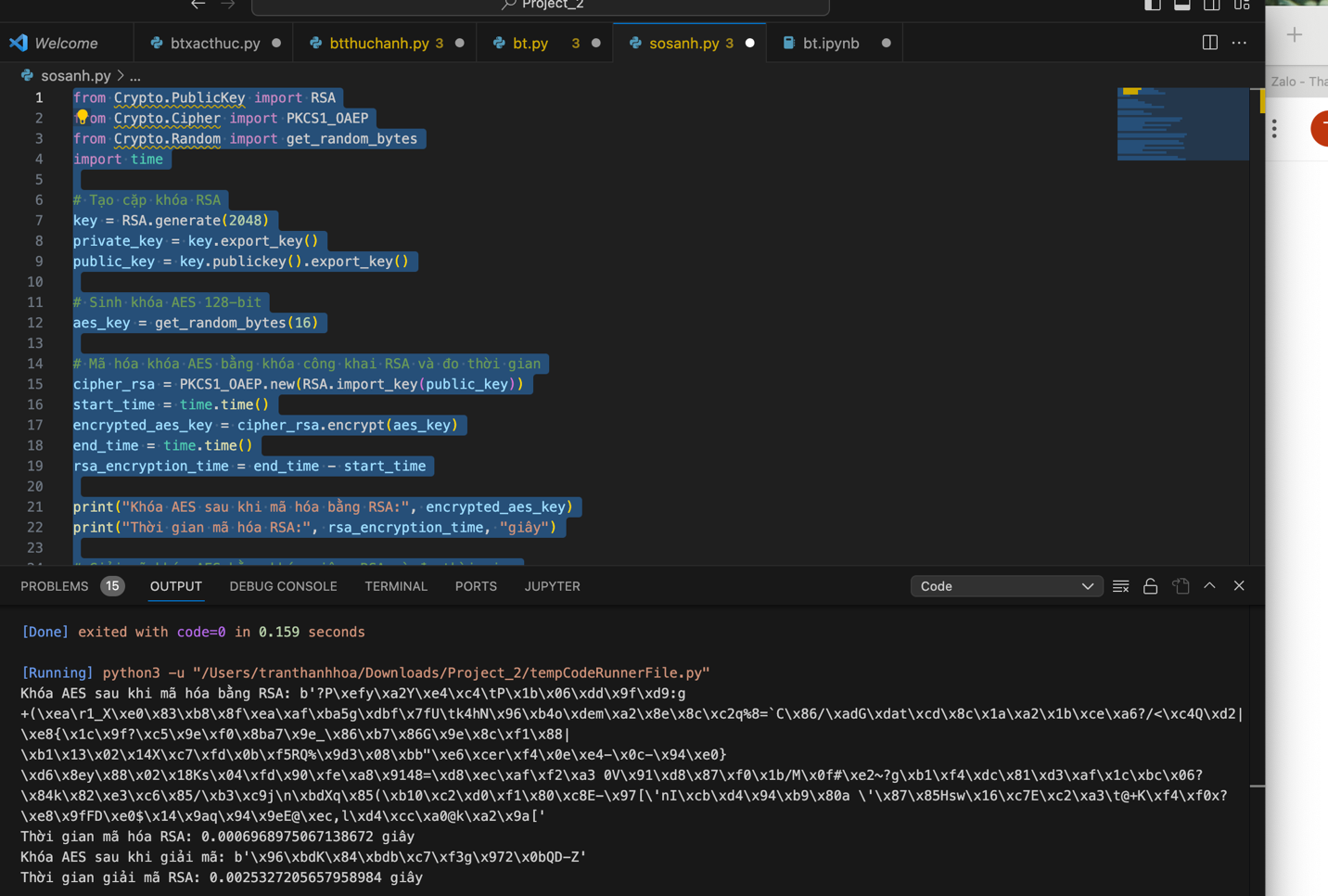
Câu 1:



Câu 2:



Câu 3:



1. Tại sao mã hóa AES có tốc độ nhanh hơn đáng kể so với RSA?

Lý do chính nằm ở bản chất thuật toán và cách xử lý dữ liệu:

|  |  |  |
| --- | --- | --- |
| Đặc điểm | AES (Mã hóa đối xứng) | RSA (Mã hóa bất đối xứng) |
| Loại thuật toán | Đối xứng (sử dụng 1 khóa) | Bất đối xứng (2 khóa: công khai & riêng) |
| Toán học | Dựa trên các phép toán đơn giản (XOR, vòng lặp, thay thế, hoán vị) | Dựa vào số học lớn (luỹ thừa mô, số nguyên tố lớn) |
| Tốc độ xử lý | Nhanh vì thao tác nhẹ, được tối ưu hóa | Chậm do phải tính toán phức tạp, dùng số nguyên lớn |
| Thiết kế | Thiết kế cho mã hóa khối lượng lớn | Thiết kế cho mã hóa ngắn (ví dụ: khóa) |

 Vì vậy, AES có thể xử lý dữ liệu nhanh gấp nhiều lần RSA khi nói đến mã hóa văn bản, hình ảnh, file, v.v.

2. Trong thực tế, tại sao người ta thường kết hợp cả AES và RSA trong một hệ thống bảo mật?

Lý do: kết hợp ưu điểm của cả hai loại mã hóa.

Đây là mô hình gọi là Hybrid Cryptosystem (Hệ mật mã lai):

|  |  |
| --- | --- |
| Thành phần | Vai trò |
| AES | Dùng để mã hóa dữ liệu (văn bản, file, ảnh) vì tốc độ cao |
| RSA | Dùng để mã hóa khóa AES (không mã hóa dữ liệu lớn) vì đảm bảo an toàn khi truyền tải khóa |

Quy trình thực tế:

1. Tạo khóa AES ngẫu nhiên.
2. Mã hóa dữ liệu bằng AES (rất nhanh).
3. Mã hóa khóa AES bằng RSA (bảo mật).
4. Gửi cả dữ liệu đã mã hóa + khóa AES đã mã hóa cho người nhận.

Người nhận dùng khóa riêng RSA để giải mã khóa AES, rồi dùng nó để giải mã dữ liệu.

 Kết hợp này đảm bảo vừa bảo mật vừa hiệu quả.

3. Dựa trên kết quả đo thời gian, loại mã hóa nào phù hợp hơn cho việc mã hóa dữ liệu dung lượng lớn?

 AES là loại mã hóa phù hợp hơn cho dữ liệu dung lượng lớn.

 Lý do:

* AES có thời gian mã hóa và giải mã cực nhanh, không phụ thuộc nhiều vào kích thước khóa.
* AES được thiết kế để mã hóa từng khối dữ liệu (ví dụ 128-bit, 256-bit) và có thể xử lý hàng MB dữ liệu chỉ trong vài mili-giây.
* RSA chỉ nên dùng để mã hóa các đoạn dữ liệu nhỏ như khóa, chứ không nên dùng để mã hóa cả file.