**Cách sinh ra private key và public key dạng pem file cho JWT:**

*openssl genrsa -out private\_key.pem 2048*

* Openssl là lệnh để gọi công cụ OpenSSL, một thư viện mã hóa mạnh mẽ được sử dụng để thực hiện các tác vụ liên quan đến bảo mật.
* genrsa là tham số chỉ định rằng bạn muốn tạo một khóa RSA (Rivest-Shamir-Adleman), một trong những thuật toán mã hóa phổ biến nhất.
* -out private\_key.pem: Tùy chọn cho phép chỉ định tên file đầu ra.
* private\_key.pem: Tên file mà khóa riêng sẽ được lưu vào. Đuôi .pem thường được sử dụng để chỉ định định dạng PEM, một định dạng mã hóa dữ liệu nhị phân thành ASCII.
* 2048 là kích thước của khóa RSA tính bằng bit. Kích thước 2048 bit là kích thước tiêu chuẩn hiện nay cho khóa RSA. Kích thước lớn hơn (như 4096 bit) có thể được sử dụng cho độ bảo mật cao hơn, nhưng cũng sẽ làm giảm hiệu suất.
* Lệnh này tạo ra một private key RSA với kích thước 2048 bit và được lưu vào file private\_key.pem

*openssl rsa -in private\_key.pem -pubout -out public\_key.pem*

* rsa là tham số chỉ định rằng bạn muốn làm việc với khóa RSA. Lệnh này cho phép bạn thực hiện các thao tác như tạo khóa, chuyển đổi giữa các định dạng và xuất khóa công.
* -in private\_key.pem: Tùy chọn chỉ định file đầu vào với private\_key.pem là tên file chứa khóa riêng
* -pubout: Tùy chọn này chỉ định rằng bạn muốn xuất khóa công khai
* -out public\_key.pem: Tùy chọn này chỉ định tên file đầu ra với tên file là public\_key.pem
* Lệnh này đọc khóa riêng từ file private\_key.pem, tạo khóa công khai tương ứng và lưu nó vào file public\_key.pem. Khóa công khai thường được chia sẻ công khai, trong khi khóa riêng cần được giữ bí mật.