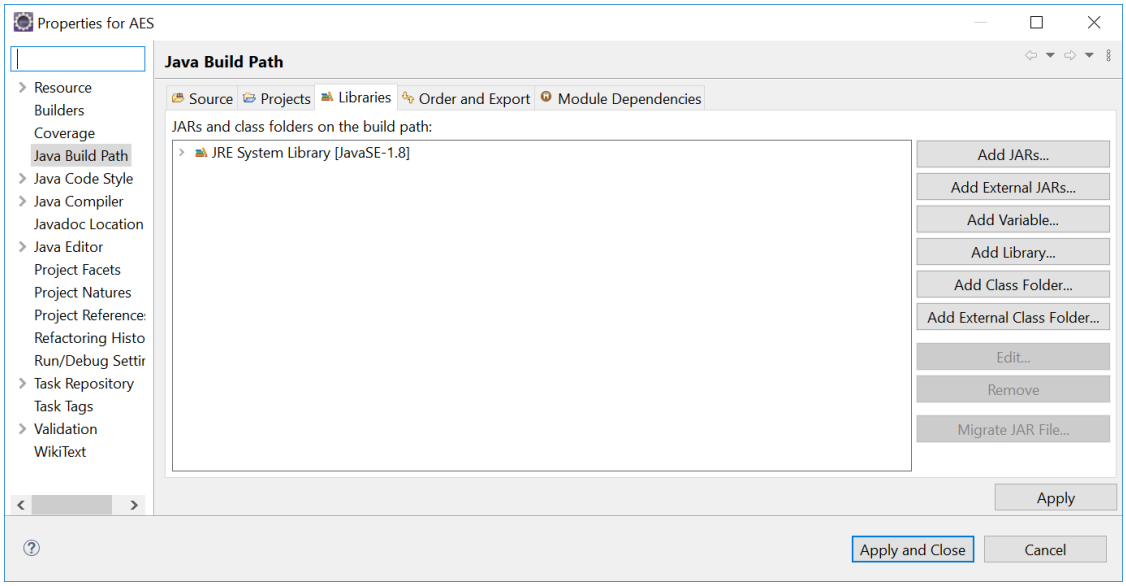
README

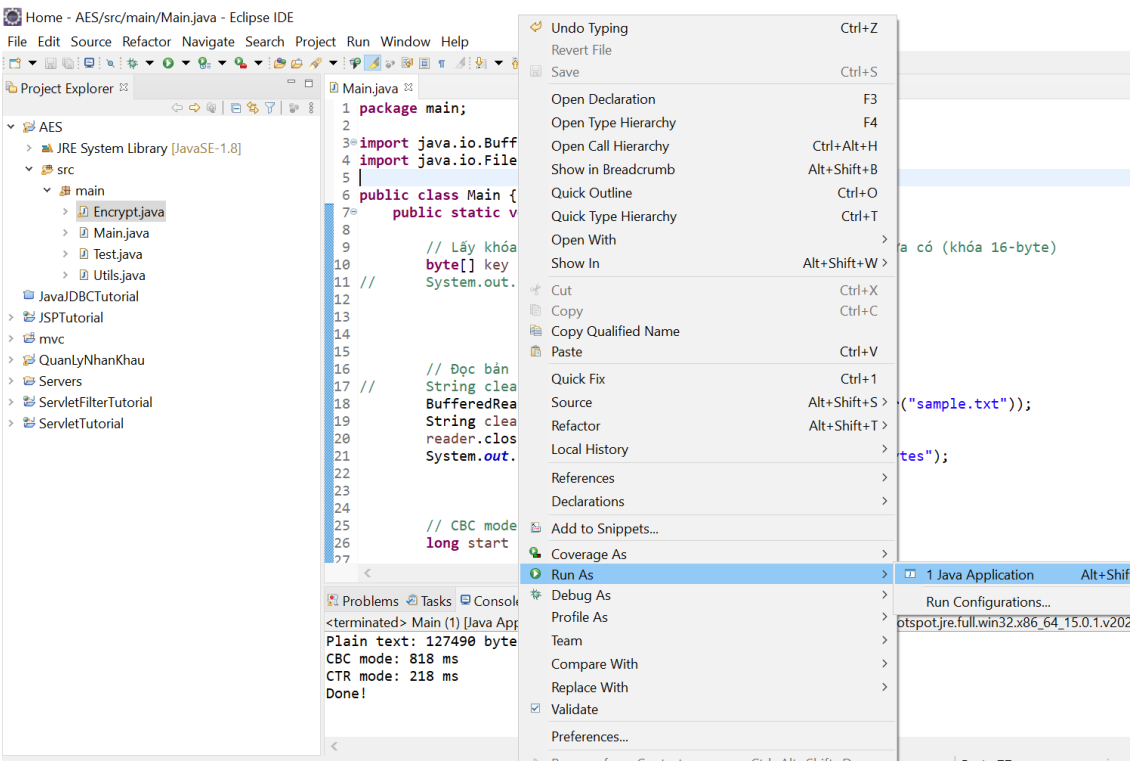
1. Thông tin chung

- Project được tạo trong Eclipse IDE

- Về môi trường: JavaSE-1.8 (Java 8). Nếu khi mới mở project gặp lỗi thì có thể xem lại xem đã cấu hình Java Build Path chưa.



- Chạy chương trình: Chạy file Main.java



2. Mô tả chương trình

- Project có sử dụng hàm mã hóa AES của thư viện *javax.crypto*.
- Khóa 16-byte được sinh và lưu trong file *key.txt*.
- Bản rõ được lưu trong file *sample.txt*.
- Bản mã sau khi mã hóa AES với CBC mode lưu trong file *output_cbc_mode.txt*.
- Bản mã sau khi mã hóa AES với CBC mode lưu trong file *output_ctr_mode.txt*.

Về cấu trúc project:

- Lớp Utils chứa các phương thức tiện ích, như chuyển mảng byte thành String kiểu hexa, PKCS#7 padding, sinh IV ngẫu nhiên…
- Lớp Encypt chứa hàm mã hóa AES ECB mode(thư viện javax.crypto), hàm mã hóa AES với CBC mode PKCS#7 padding (tự viết), CTR mode (tự viết).
- Lớp Test chứa hàm mã hóa AES với CBC mode, CTR mode của thư viện javax.crypto, có thể dùng để đối chiếu kết quả mã hóa với phần code tự viết.

- Lớp Main chứa chương trình chạy.

Kết quả sau khi chạy chương trình:

```
Plain text: 127490 bytes
CBC mode: 597 ms
CTR mode: 165 ms
Done!
```