**Bài Tập 1**

Sử dụng python và thư viện pycrypto để viết những command sau:

**1.** Mã hóa dữ liệu với thuật toán AES

Cú pháp: encrypt.py –m <mode> –i <IV> <tên file input> <tên file output>

**2.** Giải mã dữ liệu với thuật toán AES

Cú pháp: decrypt.py –m <mode> <tên file input> <tên file output>

**3.** Tính checksum của file với các thuật toán hex và kiểm tra có khớp với checksum cho trước không

Cú pháp: checksum.py –h <hash> -c <checksum> <tên file input>

Với

* -h <hash> là thuật toán hash để tạo checksum như md5, sha1, sha256
* -c <checksum>: checksum đua vào kiểm tra có khớp với checksum được tính từ file hay không, nếu có trường này thì sẽ kiểm tra checksum, nếu không có sẽ tính checksum của file và xuất ra output chuẩn

**4.** Tạo chữ ký

Cú pháp: sign.py –h <hash> <tên file input> <tên file sẽ ghi chữ ký vào>

**5.** Kiểm tra chữ ký

Cú pháp: very\_sign.py –h <hash> <tên file input> <tên file chứa chữ ký >

### 6. Tìm hiểu cơ chế trao đổi khóa của openssh version 1 và openssh version 2. Phân tích cơ chế [Perfect Forward Secrecy](https://www.perfectforwardsecrecy.com/) của hai version trên.