TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**

****

**BÁO CÁO BÀI TẬP LỚN**

**MÔN BẢO MẬT THÔNG TIN**

**TÌM HIỂU CÁC HÀM BĂM VÀ CÁCH SỬ DỤNG THƯ VIỆN CRYPTO**

*Người hướng dẫn*: PhD.**Huỳnh Ngọc Tú**

*Người thực hiện*: **Trần Công Đạt – 51800183**

**Nghiệm Minh Tiến – 51800247**

**Nguyễn Trần Khôi Nguyên - 51800909**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2020**

TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**

****

**BÁO CÁO BÀI TẬP LỚN**

**MÔN BẢO MẬT THÔNG TIN**

**TÌM HIỂU CÁC HÀM BĂM VÀ CÁCH SỬ DỤNG THƯ VIỆN CRYPTO**

*Người hướng dẫn*: PhD.**Huỳnh Ngọc Tú**

*Người thực hiện*: **Trần Công Đạt – 51800183**

**Nghiệm Minh Tiến – 51800247**

**Nguyễn Trần Khôi Nguyên - 51800909**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2020**

# LỜI CẢM ƠN

Chúng em xin chân thành cảm ơn Cô **Huỳnh Ngọc Tú** đã hướng dẫn và tạo dựng những điều kiện cần thiết để chúng em hoàn thành bài tập lớn. Chúng em rất mong nhận được những ý kiến đóng góp quý báu của Cô và các bạn cùng lớp để kiến thức của chúng em trong lĩnh vực này được hoàn thiện hơn. Nhóm xin chân thành cảm ơn.

Sau cùng, chúng tôi xin kính chúc quý Thầy Cô trong Khoa Công Nghệ Thông  
Tin thật dồi dào sức khỏe, niềm tin để tiếp tục thực hiện sứ mệnh cao đẹp của mình  
là truyền đạt kiến thức cho thế hệ mai sau.

**ĐỒ ÁN ĐƯỢC HOÀN THÀNH**

**TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

Chúng tôi xin cam đoan đây là sản phẩm đồ án của riêng chúng tôi và được sự hướng dẫn của Cô **Huỳnh Ngọc Tú**. Các nội dung nghiên cứu, kết quả trong đề tài này là trung thực và chưa công bố dưới bất kỳ hình thức nào trước đây. Những số liệu trong các bảng biểu phục vụ cho việc phân tích, nhận xét, đánh giá được chính tác giả thu thập từ các nguồn khác nhau có ghi rõ trong phần tài liệu tham khảo.

Ngoài ra, trong đồ án còn sử dụng một số nhận xét, đánh giá cũng như số liệu của các tác giả khác, cơ quan tổ chức khác đều có trích dẫn và chú thích nguồn gốc.

**Nếu phát hiện có bất kỳ sự gian lận nào tôi xin hoàn toàn chịu trách nhiệm về nội dung đồ án của mình.** Trường đại học Tôn Đức Thắng không liên quan đến những vi phạm tác quyền, bản quyền do tôi gây ra trong quá trình thực hiện (nếu có).

*TP. Hồ Chí Minh, ngày tháng năm*

*Trưởng nhóm*

*(ký tên và ghi rõ họ tên)*

*Trần Công Đạt*

# PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN

**Phần xác nhận của GV hướng dẫn**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tp. Hồ Chí Minh, ngày tháng năm

(ký và ghi họ tên)

**Phần đánh giá của GV chấm bài**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tp. Hồ Chí Minh, ngày tháng năm

(ký và ghi họ tên)

# DANH MỤC KÍ HIỆU VÀ CHỮ VIẾT TẮT

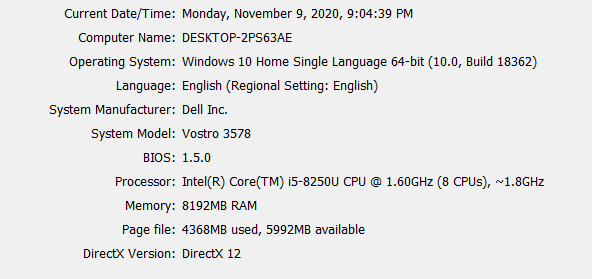
DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ

## DANH MỤC HÌNH

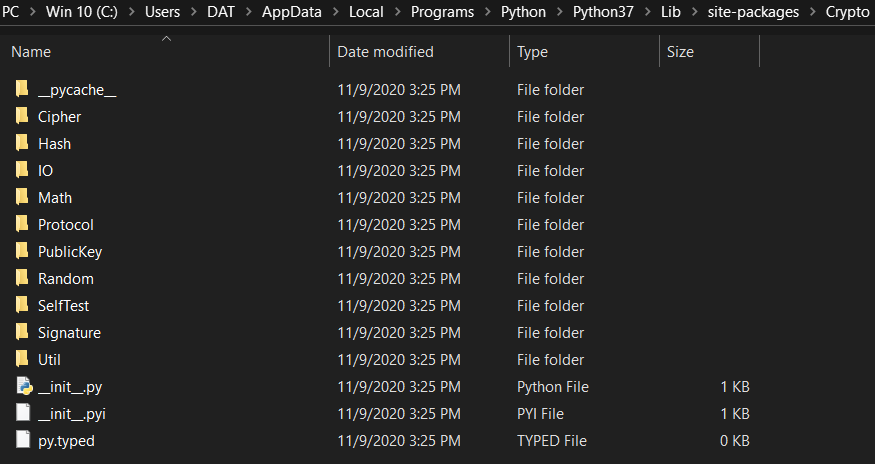
CHƯƠNG I: THÔNG TIN PHẦN CỨNG

Một số thông tin phần cứng của máy :

* RAM : 8GB
* CPU : core i5 – 8250U 1.6 GHz
* Hệ điều hành : Windows 10 Home
* Ổ cứng : SSD INTEL 128GB 545S SSDSC2KW128G8X1
* Vì sử dụng Python để code nên Lib: PyCrypto, PyCrytodome tương đương.



Hình . Thông tin phần cứng



Hình . Thư mục chứa Lib

CHƯƠNG II: THE COMPILER VERSION, HASH FUNCTION, BLOCK CIPHERS, PUBLIC KEY SIGNATURE SCHEMES

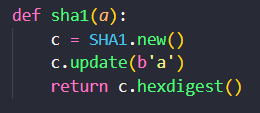
*1.Hash function:*

- SHA (Secure Hash Algorithm hay thuật giải băm an toàn) là năm thuật giải được chấp nhận bởi FIPS dùng để chuyển một đoạn dữ liệu nhất định thành một đoạn dữ liệu có chiều dài không đổi với xác suất khác biệt cao.

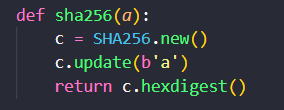
- Hàm **new()** dùng để tạo một hash object mới.

- Hàm **update()** dùng để tiếp tục băm một tin nhắn bằng cách sử dụng phần dữ liệu tiếp theo.

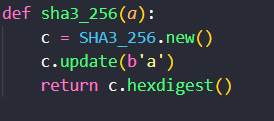
- Hàm **digest()** dùng để trả về thông điệp có thể in ra từ hàm băm.



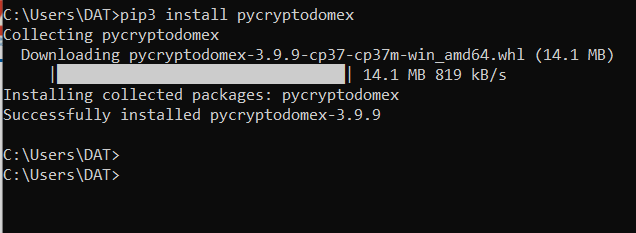
Hình . Hàm SHA1



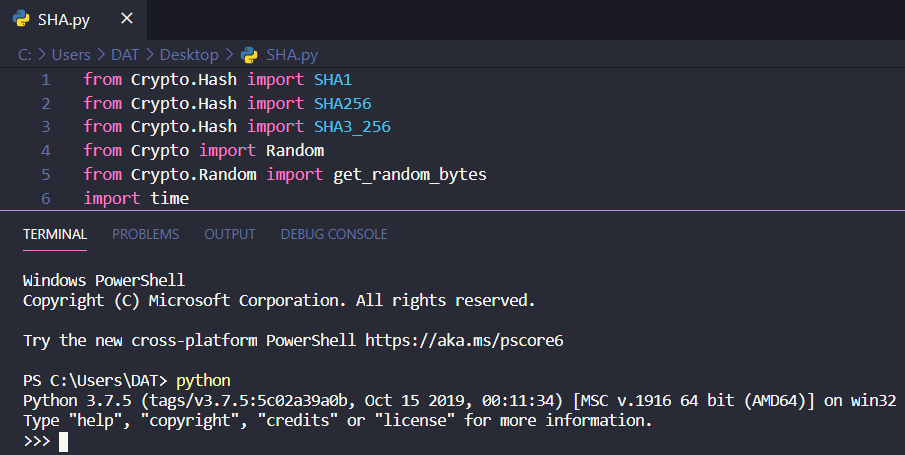
Hình . Hàm SHA256



Hình . Hàm SHA356



Hình . Installing Lib



Hình . The compiler version and lib

*2.* *Block Ciphers:*

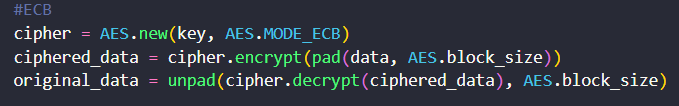
- **data=get\_random\_bytes(32)** : sử dụng hàm get\_random\_bytes trong Cryto lấy 32 byte ngẫu nhiên

- **key = get\_random\_bytes(16)** : tạo ra khóa ngẫu nhiêu dài 16 bytes = 128 bít

- Hàm **encrypt(pad(data, AES.block\_size))** : dùng để mã hóa dữ liện trong data, sử dụng pad để đệm dữ liệu để vừa với block\_size của mã hóa AES.

- Hàm **unpad(cipher.decrypt(ciphered\_data), AES.block\_size)**: dùng để giải mã và tháo thành phần dữ liệu đệm.

- Hàm **AES.new(key, AES.MODE\_CBC,iv)** : tạo ra mã hóa bằng hàm AES với mode CBC và iv.



Hình . ECB mode

*3.Public Key Signature Schemes:*

- Hàm **generate()** trả về một DSA key object mới.

- Hàm **export\_key()** trả về encoded key với kiểu trả về là byte string.

- Hàm **import\_key()** trả về một a DSA key object với kiểu trả về Dsakey



Hình . Hàm DSA

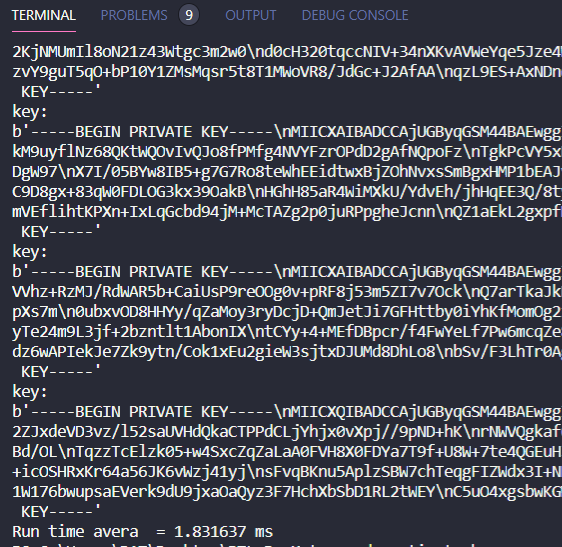
CHƯƠNG III: TEST FUNCTION



Hình . Test of SHA



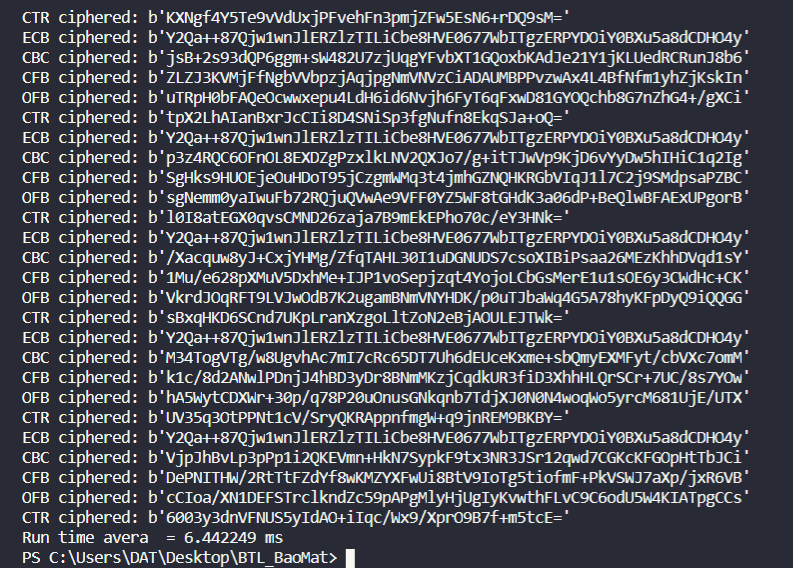
Hình .Test of DSA (10 lần)



Hình . Test of DSA (1000 lần)



Hình . Test of ECC



Hình .Test of Ciphers

# TÀI LIỆU THAM KHẢO

1. [SHA]: <https://vi.wikipedia.org/wiki/SHA#SHA-1>
2. [pryptodome]: https://pycryptodome.readthedocs.io/en/latest/src/hash/sha1.html
3. Link Github : https://github.com/CongDatt/AssignmentOfInformationSecurity