**TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI**

**THÀNH PHỐ HỒ CHÍ MINH**

-----🙚🙘🕮🙚🙘-----



**BÁO CÁO MÔN AN TOÀN THÔNG TIN**

**Hà Đức An MSSV: 22H1120001**

*Thành phố Hồ Chí Minh, tháng 04 năm 2025*

## **MỤC LỤC**

**[CHƯƠNG 1: GIỚI THIỆU 4](#_Toc3282)**

**[CHƯƠNG 2: CÁC KỸ THUẬT MÃ HÓA 5](#_Toc30453)**

**[2.1. Nghịch đảo modulo (Euclid mở rộng) 5](#_Toc27863)**

**[2.2. Mã hóa cổ điển Caesar 6](#_Toc27835)**

**[2.3. Mã hóa AES 128-bit 7](#_Toc3365)  
2.4. Mã hóa RSA............................................................................8**

**[2.5. Hàm băm SHA-256 9](#_Toc15770)**

**[CHƯƠNG 3. KẾT LUẬN 10](#_Toc24908)**

**[CHƯƠNG 4: TÀI LIỆU THAM KHẢO 10](#_Toc22643)**

### 

### 

### 

### 

### 

### 

### 

### 

### 

### 

### 

### 

### 

### 

### 

### 

### **LỜI CẢM ƠN**

Trong suốt quá trình thực hiện tiểu luận môn **An toàn thông tin**, em xin chân thành cảm ơn và gửi lời tri ân sâu sắc đến các thầy cô, bạn bè và những người đã đồng hành, hỗ trợ em hoàn thành bài báo cáo này.

Đầu tiên, em xin gửi lời cảm ơn đặc biệt đến **Thầy (Cô) Trưởng Bộ môn** và **Giảng viên** môn An toàn thông tin đã tận tình giảng dạy, chỉ bảo cho em những kiến thức quý báu về lĩnh vực bảo mật thông tin và các kỹ thuật mã hóa. Những kiến thức đó không chỉ giúp em hiểu rõ về an toàn thông tin mà còn giúp em hình dung được tầm quan trọng của việc bảo vệ dữ liệu trong môi trường số hiện nay.

Em cũng xin cảm ơn các bạn trong nhóm học tập và làm việc cùng em. Chúng ta đã có những giờ phút thảo luận sôi nổi, trao đổi kiến thức và kinh nghiệm, cùng nhau tìm hiểu và giải quyết các vấn đề khó khăn.

Cuối cùng, em xin gửi lời cảm ơn đến gia đình và người thân, những người đã luôn động viên, chia sẻ và tạo điều kiện cho em có thể hoàn thành bài tiểu luận này.

Em xin kính chúc các thầy cô, bạn bè và gia đình luôn khỏe mạnh, hạnh phúc và thành công trong cuộc sống.

# **CHƯƠNG 1: GIỚI THIỆU**

Trong kỷ nguyên số, thông tin trở thành tài sản quý giá nhất của mỗi tổ chức và cá nhân. “An toàn thông tin” không chỉ dừng lại ở việc bảo vệ máy chủ hay hệ thống mạng, mà còn bao hàm ba nguyên tắc cơ bản: tính bí mật, tính toàn vẹn và tính sẵn sàng của dữ liệu. Khi dữ liệu bị lộ lọt, thay đổi trái phép hoặc không thể truy cập kịp thời, hậu quả có thể rất nghiêm trọng: từ thất thoát tài chính đến mất uy tín và gián đoạn hoạt động.

Kỹ thuật mã hóa đóng vai trò nòng cốt trong chiến lược bảo vệ thông tin. Bằng cách biến đổi dữ liệu gốc thành bản mã chỉ có thể đọc được bởi người sở hữu khóa giải mã, mã hóa ngăn chặn truy cập trái phép và đảm bảo dữ liệu luôn giữ tính bí mật. Bên cạnh đó, một số kiểu mã hóa đồng thời hỗ trợ xác thực nguồn gốc và chống sửa đổi, góp phần đảm bảo tính toàn vẹn.

Báo cáo này giới thiệu năm kỹ thuật mã hóa tiêu biểu, tương ứng với năm bài tập thực hành:

1. Nghịch đảo modulo (Euclid mở rộng) – nền tảng tìm khóa bí mật trong RSA.
2. Mã hóa cổ điển Caesar – minh họa cơ chế dịch vòng đơn giản.
3. AES 128-bit – thuật toán đối xứng hiện đại, an toàn và nhanh.
4. RSA – mã hóa bất đối xứng dựa trên phân tích số nguyên lớn.
5. SHA-256 – hàm băm mật mã, bảo vệ toàn vẹn dữ liệu.

# **CHƯƠNG 2: CÁC KỸ THUẬT MÃ HÓA**

## **2.1. Nghịch đảo modulo (Euclid mở rộng)**

**Lý thuyết**

Để tính nghịch đảo d trong RSA, ta cần giải phương trình:

e \* d mod phi(n) = 1

Trong đó:

phi(n) = (p – 1) \* (q – 1)

Phương pháp Euclid mở rộng cho ta:

gcd(a, b) = d = a \* x + b \* y

Khi gcd(a, b) = 1 thì:

x ≡ a^(–1) mod b

Áp dụng vào RSA:

a = e

b = phi(n)

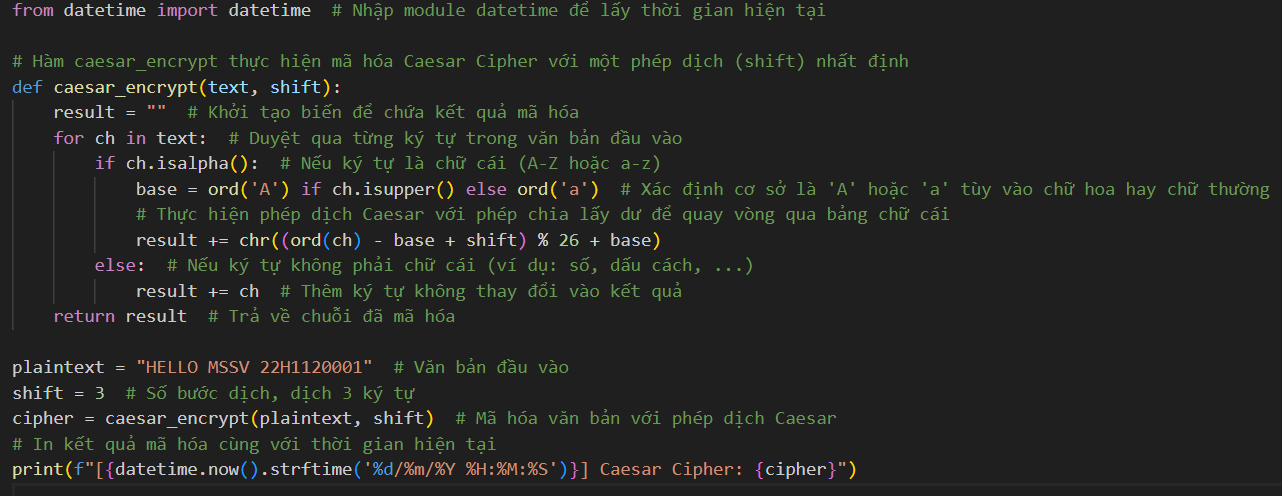
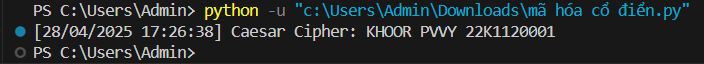
→ d = x mod phi(n)

.

## **Code Python Kết quả 2.2. Mã hóa cổ điển Caesar**

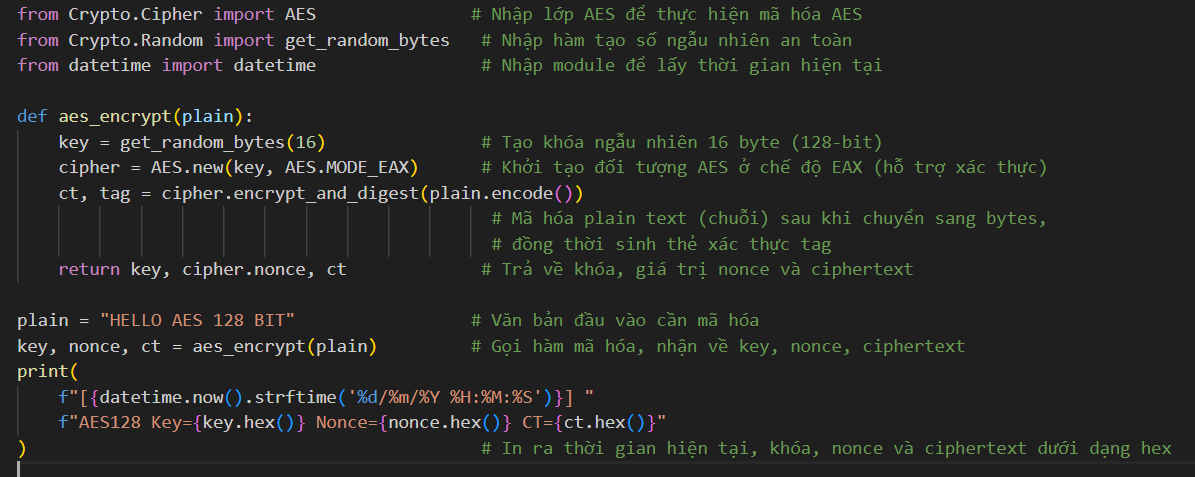
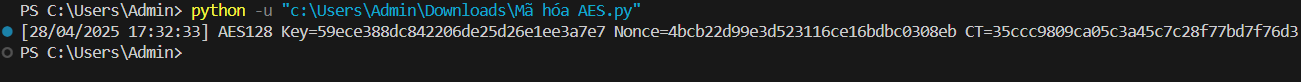
### **Lý thuyết**

**Caesar Cipher** dịch mỗi ký tự trong bản rõ một số vị trí cố định (shift) trên bảng chữ cái. Đây là ví dụ đơn giản về mã hóa đối xứng, không an toàn trong thực tế nhưng dễ hiểu.

**Code Python**  
**Kết quả**

## **2.3. Mã hóa AES 128-bit**

**Lý thuyết**

AES (Advanced Encryption Standard) là thuật toán đối xứng khối, độ dài khóa 128 bit được xem là an toàn và phổ biến. Dữ liệu được chia khối 16 byte, mỗi khối qua 10 vòng biến đổi phức tạp.  
**Code Python** **Kết quả**  
 **2.4. Mã hóa RSA**

**Lý thuyết**RSA dựa trên tính khó của phân tích số nguyên tố. Mỗi cặp khóa gồm:

Khóa công khai: (n, e)

Khóa riêng: (n, d)  
# Mã hóa

c = m\*e / n # tương đương c = pow(m, e, n)

# Giải mã  
m = c\*d / n # tương đương m = pow(c, d, n)

Trong đó:

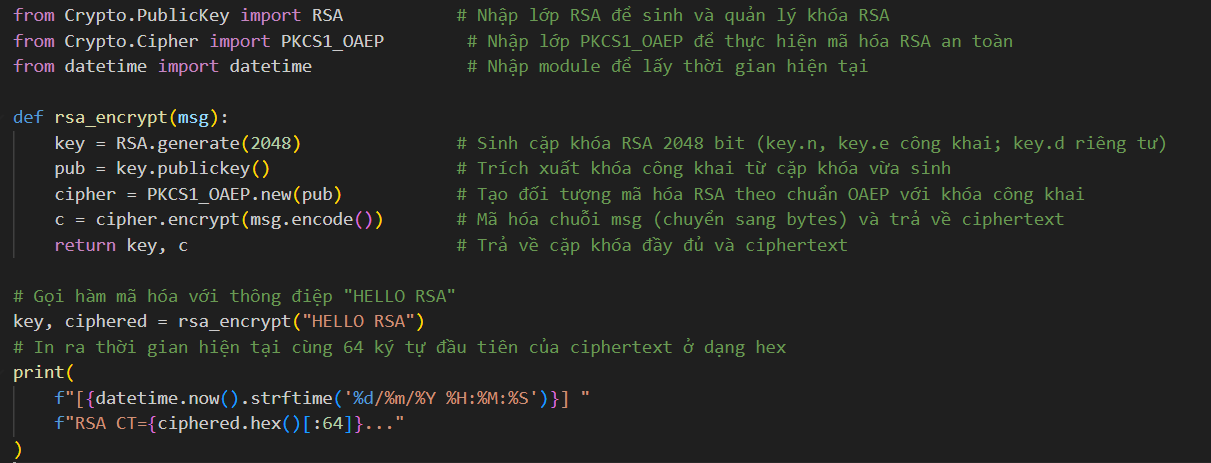
m = bản rõ (plaintext) dưới dạng số

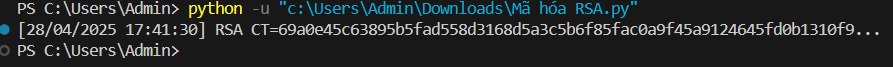
c = bản mã (ciphertext) dưới dạng số

e = số mũ công khai

d = số mũ bí mật (nghịch đảo của e mod phi(n))

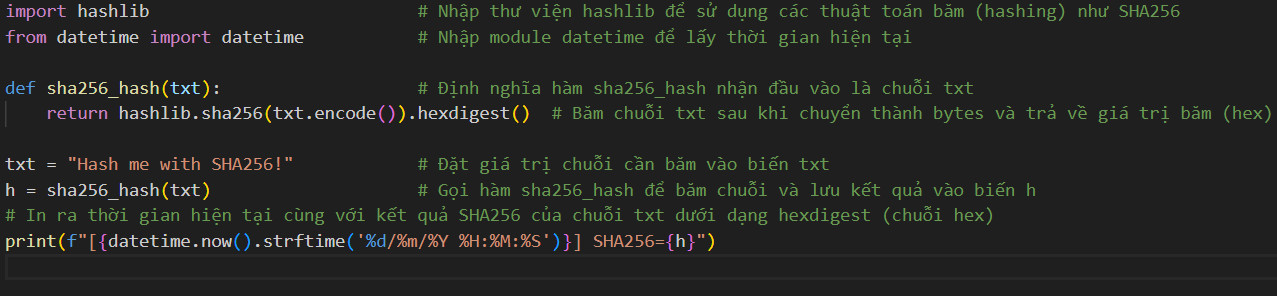
n = p \* q (tích hai số nguyên tố)

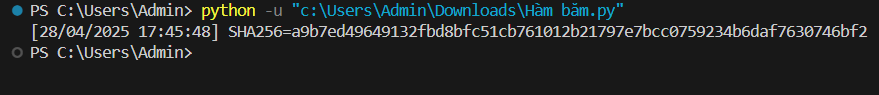
phi(n) = (p–1)\*(q–1)  
**Code Python** **Kết quả**



## **2.5. Hàm băm SHA-256**

**Lý thuyết**

SHA-256 là hàm băm mật mã họ SHA-2, đầu ra 256 bit. Không thể đảo ngược và rất mẫn cảm với thay đổi dữ liệu.  
**Code Python**

**Kết quả**

# **CHƯƠNG 3. KẾT LUẬN**

Qua năm bài tập mã hóa, chúng ta đã:

Hiểu cách tìm nghịch đảo modulo bằng Euclid mở rộng — nền tảng sinh khóa trong RSA.

Minh họa mã hóa cổ điển qua Caesar Cipher, tuy đơn giản nhưng giúp nắm rõ chuyển vị ký tự.

Áp dụng AES 128-bit, chứng minh mã hóa khối đối xứng hiện đại, an toàn và hiệu quả.

Triển khai RSA, thuật toán bất đối xứng dựa trên số nguyên tố lớn, đảm bảo an toàn trong truyền dữ liệu.

Sử dụng SHA-256 để băm dữ liệu, bảo vệ tính toàn vẹn trước mọi thay đổi.

Mỗi kỹ thuật có vai trò riêng trong hệ sinh thái an toàn thông tin: từ bảo vệ bí mật, xác thực đến toàn vẹn. Trong thực tế, một hệ thống an toàn thường kết hợp nhiều lớp mã hóa, hạ tầng khóa công khai (PKI) và cơ chế quản lý khóa chặt chẽ.

# **CHƯƠNG 4: TÀI LIỆU THAM KHẢO**

1. Stallings, W. (2020). Cryptography and Network Security: Principles and Practice.
2. Menezes, A., van Oorschot, P., & Vanstone, S. (1996). Handbook of Applied Cryptography.
3. Daemen, J., & Rijmen, V. (2002). The Design of Rijndael.
4. Ferguson, N., Schneier, B., & Kohno, T. (2010). Cryptography Engineering.
5. RFC 6234: US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF).

6. Documentation of PyCryptodome: <https://pycryptodome.readthedocs.io/>