BÀI THỰC HÀNH SỐ 3

Môn: MẬT MÃ & AN NINH MẠNG

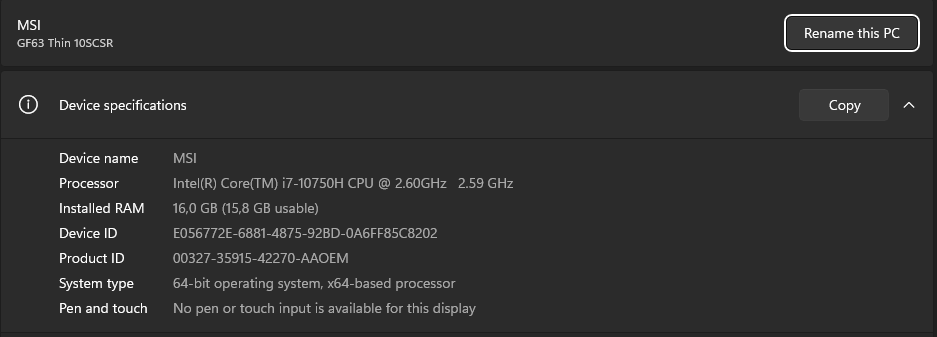
-o0o-

**Họ tên: Chế Quang Huy**

**MSSV: 1812340**

**Câu 1:**

a. Source code đã nộp đính kèm theo báo cáo.

b.

*Hình 1: Cấu hình máy tính được sử dụng*

* Mã hóa và giải mã file 10MB:
* Chế độ: DES/ECB/PKCS5Padding.
* Thời gian mã hóa: 2937 ms.
* Text

  Description automatically generatedThời gian giải mã: 2950 ms.

*Hình 2: Thực hiện mã hóa và giải mã file 10MB (DES/ECB/PKCS5Padding)*

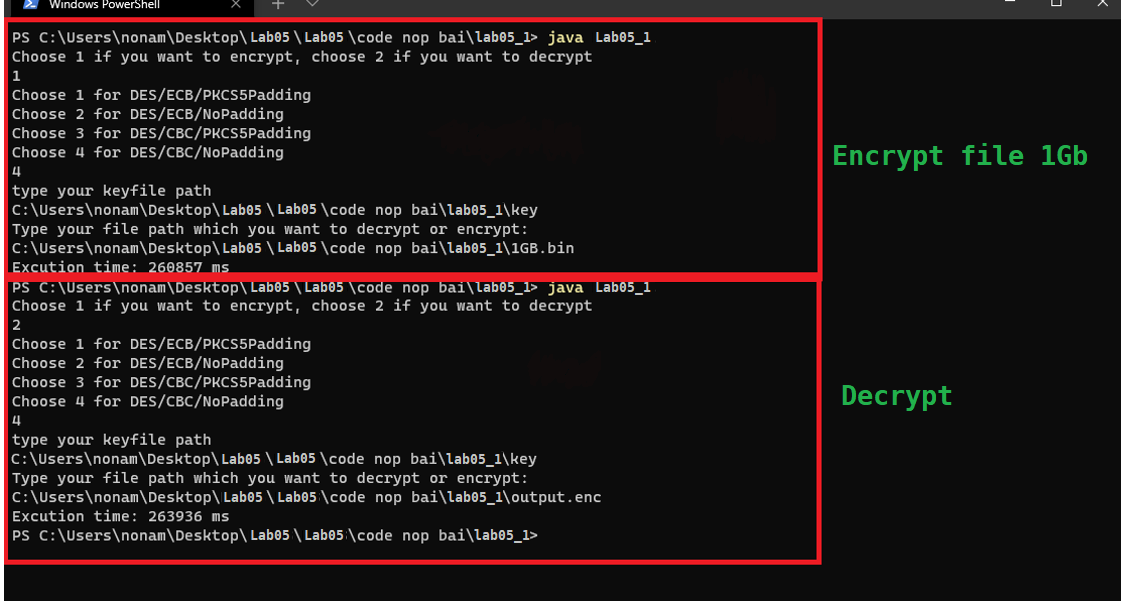
* Mã hóa và giải mã file 100MB:
* Chế độ: DES/ECB/NoPadding.
* Thời gian mã hóa: 26678 ms.
* Thời gian giải mã: 26554 ms.

Text

Description automatically generated

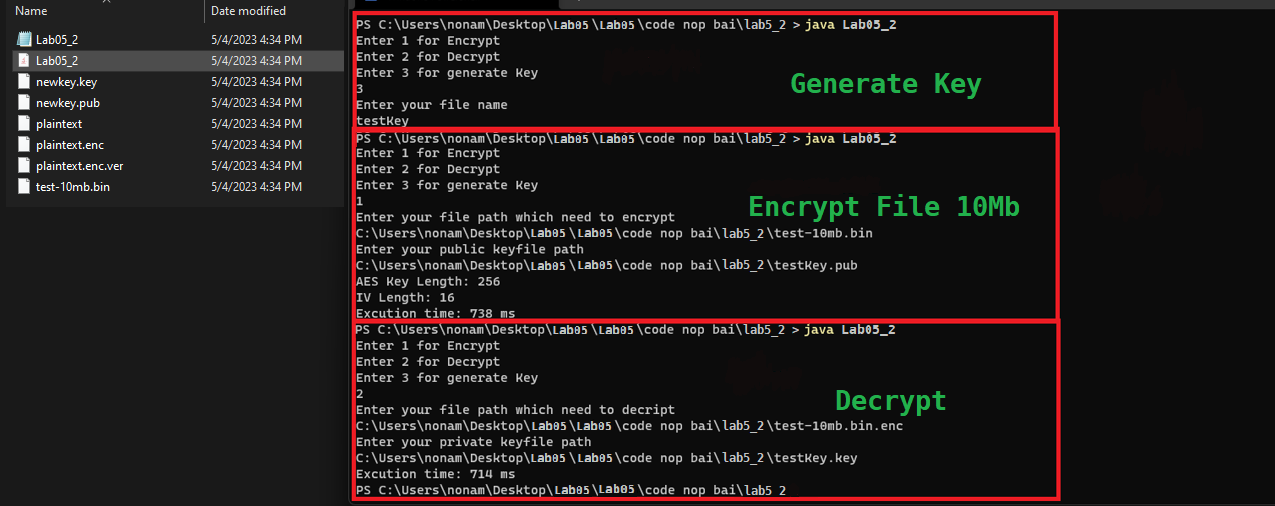
*Hình 3: Thực hiện mã hóa và giải mã file 100MB (DES/ECB/NoPadding)*

* Mã hóa và giải mã file 1GB:
* Chế độ: DES/CBC/NoPadding.
* Thời gian mã htóa: 260857 ms.
* Thời gian giải mã: 263936 ms.



*Hình 4: Thực hiện mã hóa và giải mã file 1GB (DES/CBC/NoPadding)*

**Câu 2:**

****

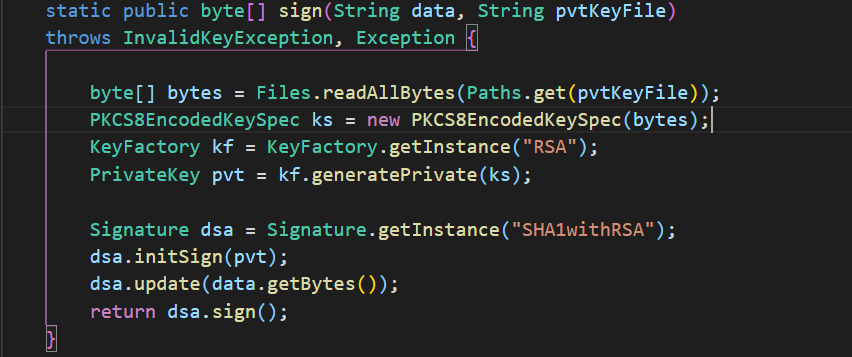
*Hình 5: Tạo khóa, mã hóa file 10Mb, giải mã*

* Với file 10MB:
* Thời gian mã hoá: 738ms.
* Thời gian giải mã: 714ms.

Thời gian mã hoá và giải mã nhanh gấp khoảng 4 lần so với giải thuật DES ở **Câu 1**.

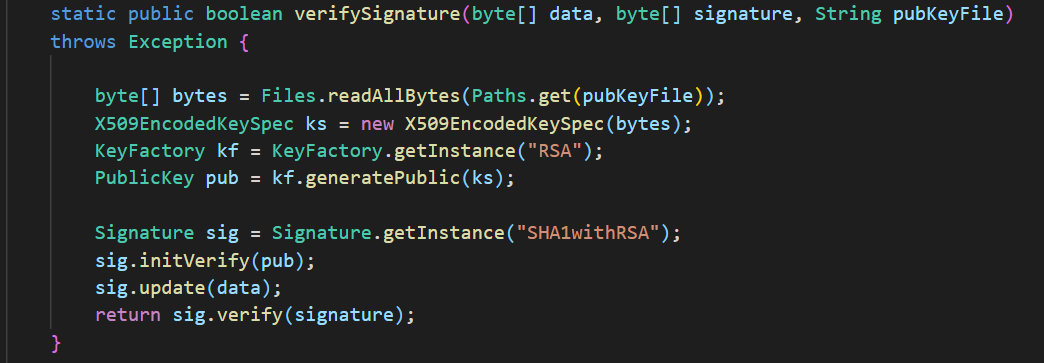
**Câu 3:**

a)Phương thức để ký trên một thông điệp: *sign()*



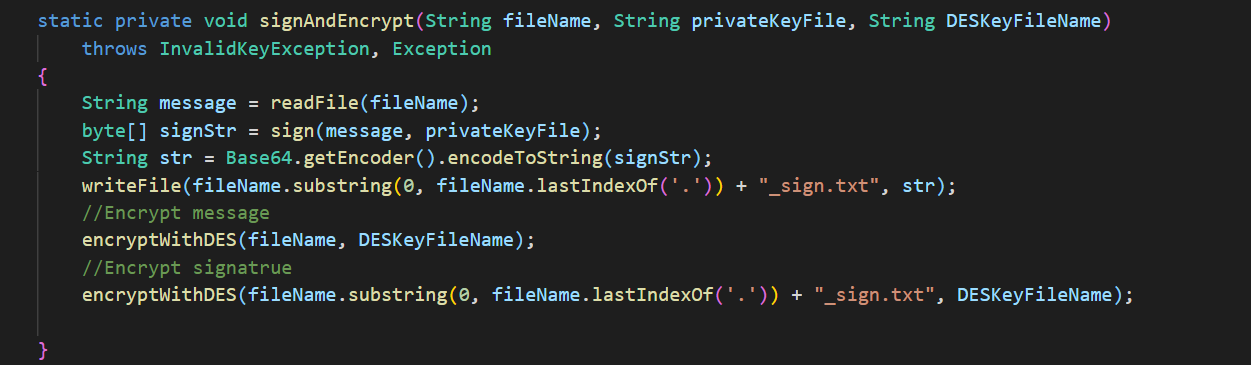
*Hình 6: Phương thức sign()*

b) Phương thức để xác minh chữ ký trên một thông điệp: *verifySignature()*



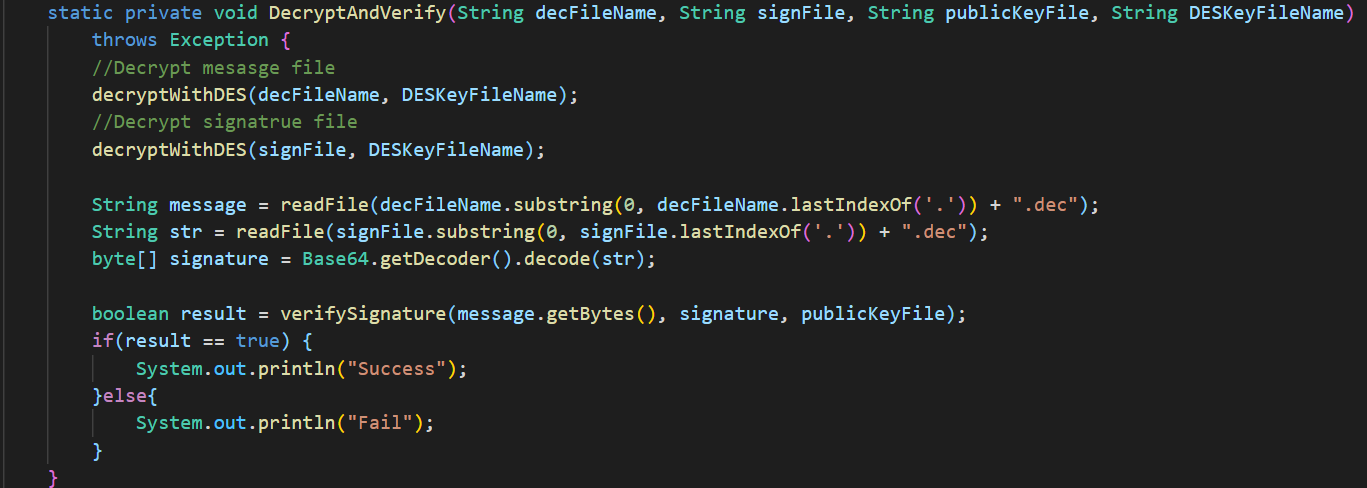
*Hình 7: Phương thức verifySignature()*

c) Phương thức để k. trên một thông điệp và sau đó mã hoá toàn bộ (dùng giải thuật DES với giả sử khoá đối xứng đã được chia sẻ giữa bên gởi và bên nhận): *signAndEncrypt()*



*Hình 8: Phương thức signAndEncrypt()*

d) Phương thức để giải mã toàn bộ (dùng giải thuật DES với giả sử khoá đối xứng đã được chia sẻ giữa bên gởi và bên nhận) và xác minh chữ ký số: *DecryptAndVerify()*



*Hình 9: Phương thức DecryptAndVerify()*