ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH

Mật mã và An ninh mạng (TN) - CO3070

Báo cáo

BÀI THỰC HÀNH SỐ 4

Giảng viên hướng dẫn: ThS. Nguyễn Cao Đạt

Sinh viên thực hiện: 2014486 - Đậu Xuân Thành

TP. Hồ Chí Minh, 05/2024

Mục lục

Danh mục hình ảnh

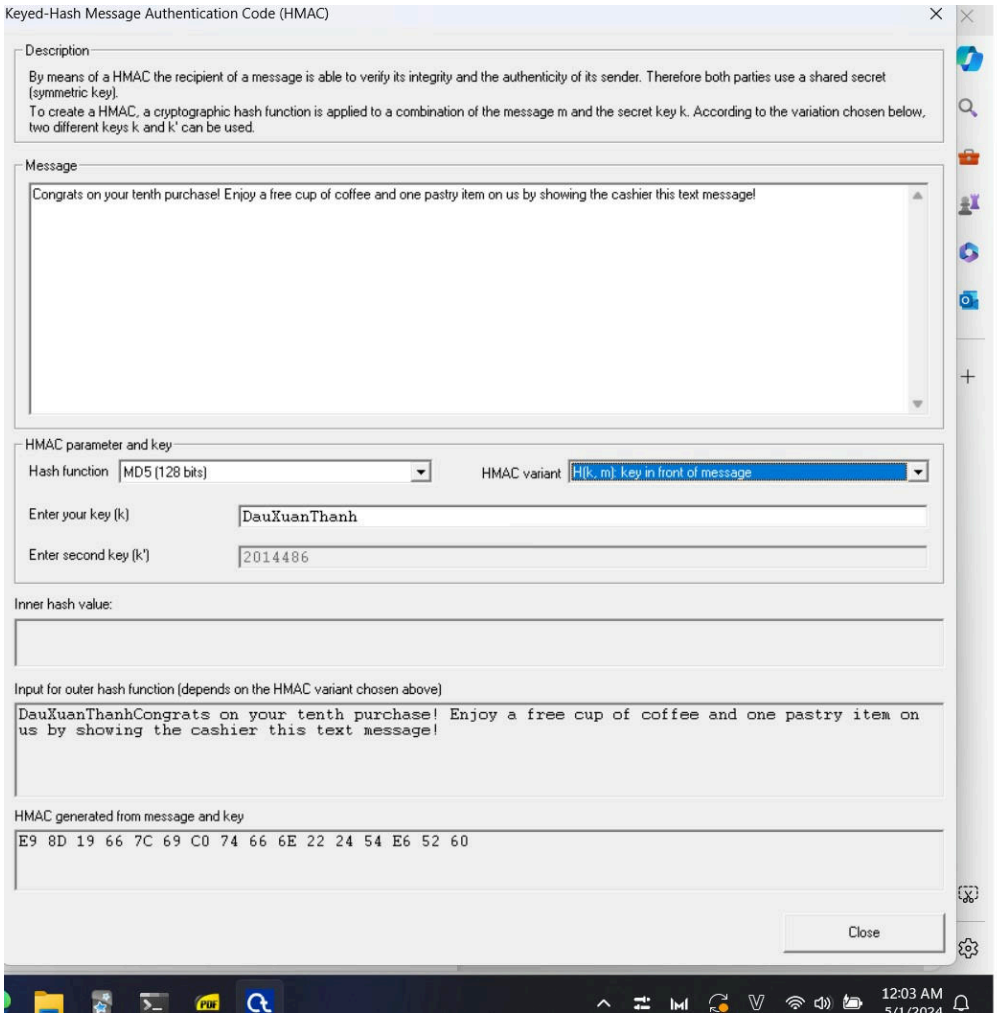
1. Mã xác thực thông điệp MAC

1.1. Câu 1: Sử dụng công cụ Cryptool để tính toán HMAC cho một thông điệp theo các

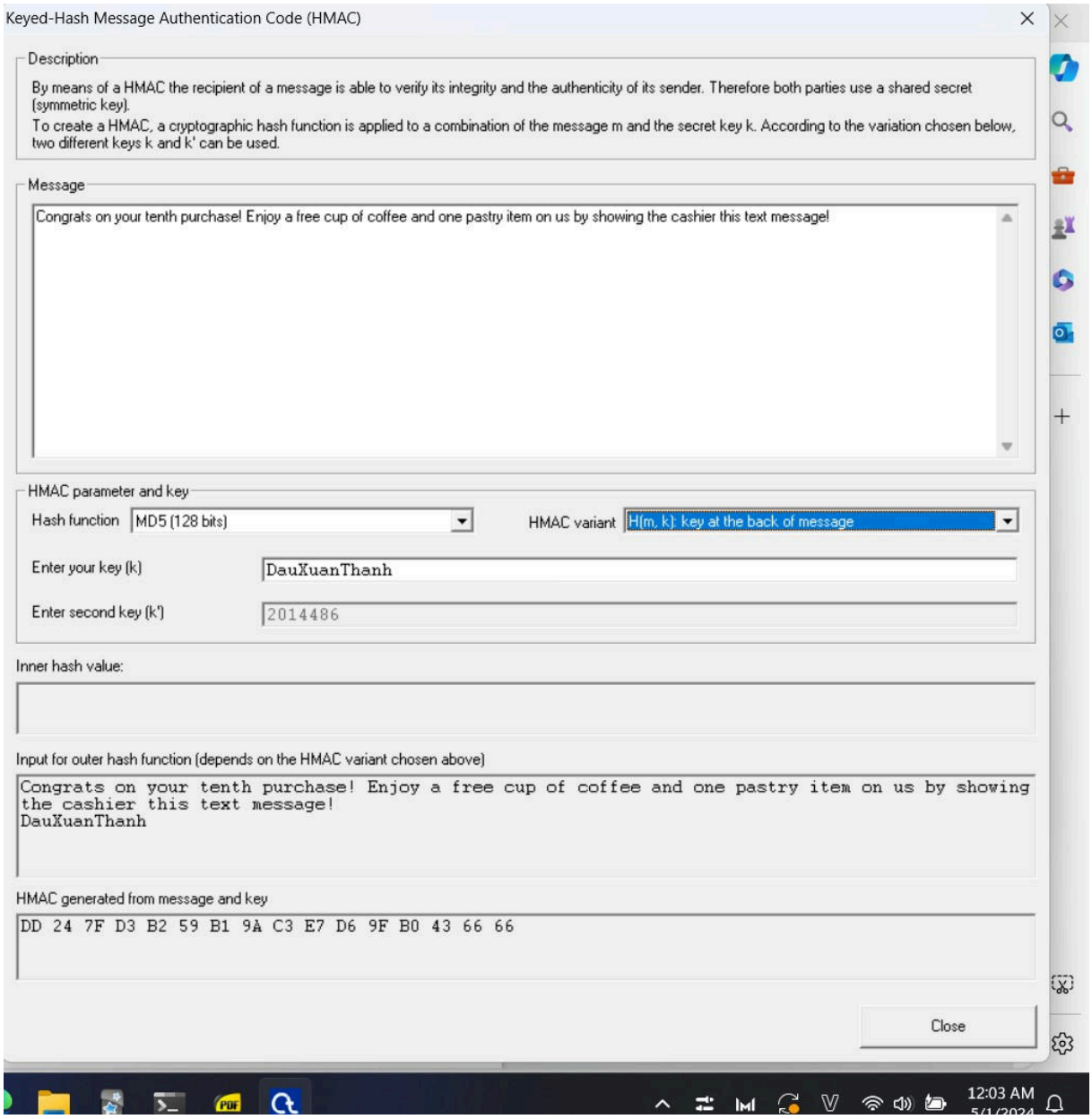
bước như bên dưới

1.1.1. Tính Hmac cho hàm MD5

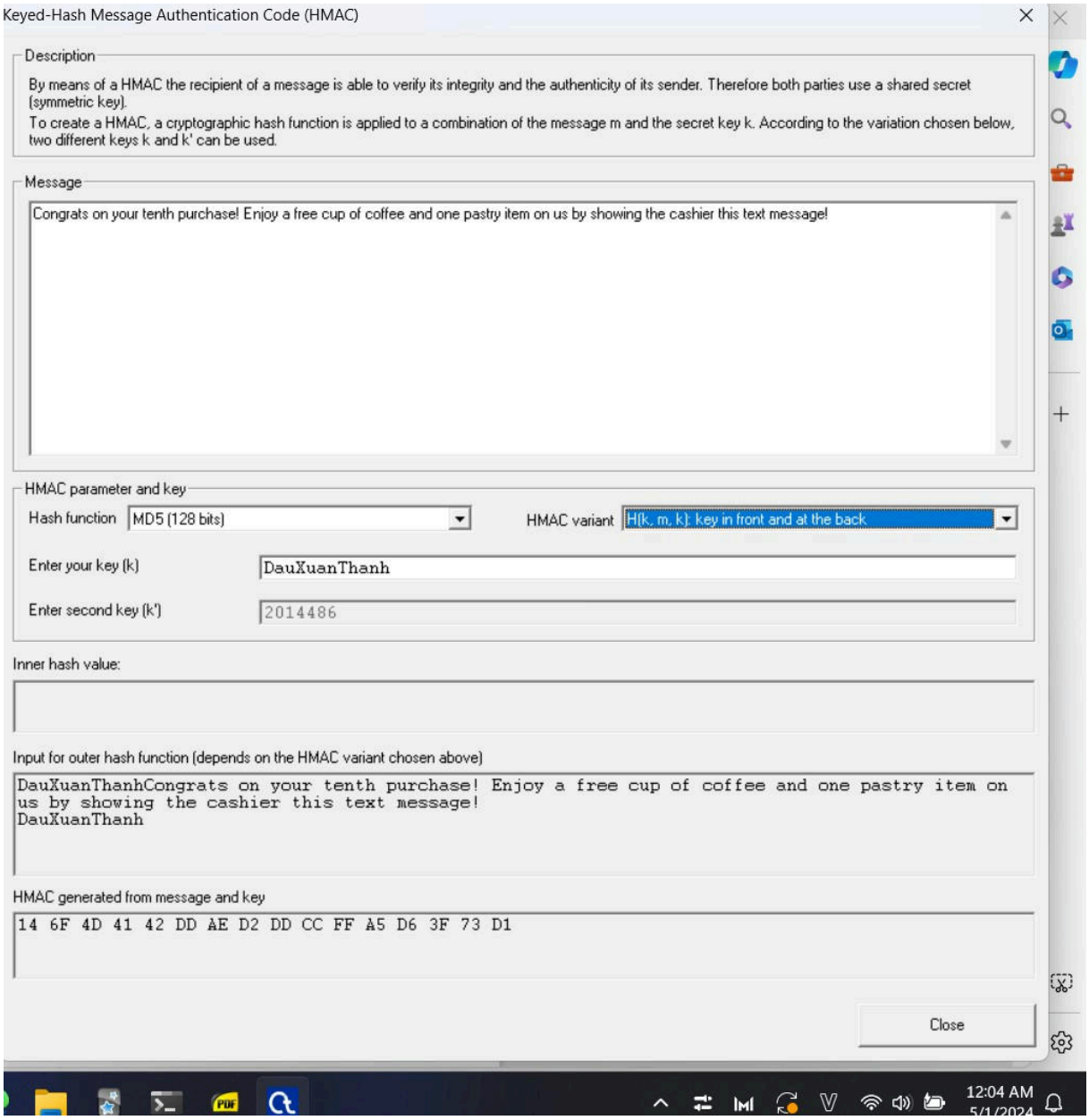
- H(k,m): key in front of message



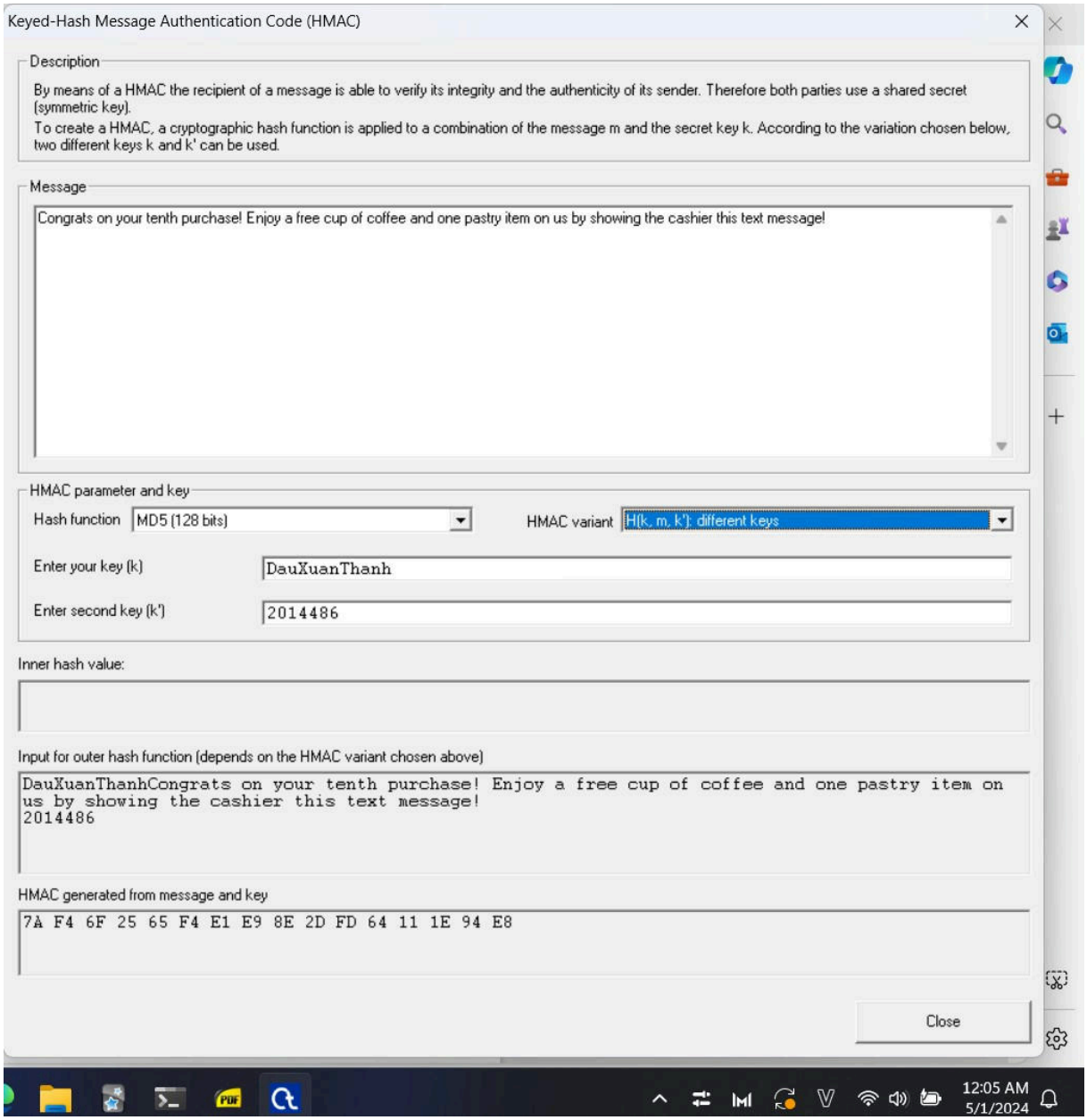
- H(m,k): key in back of message



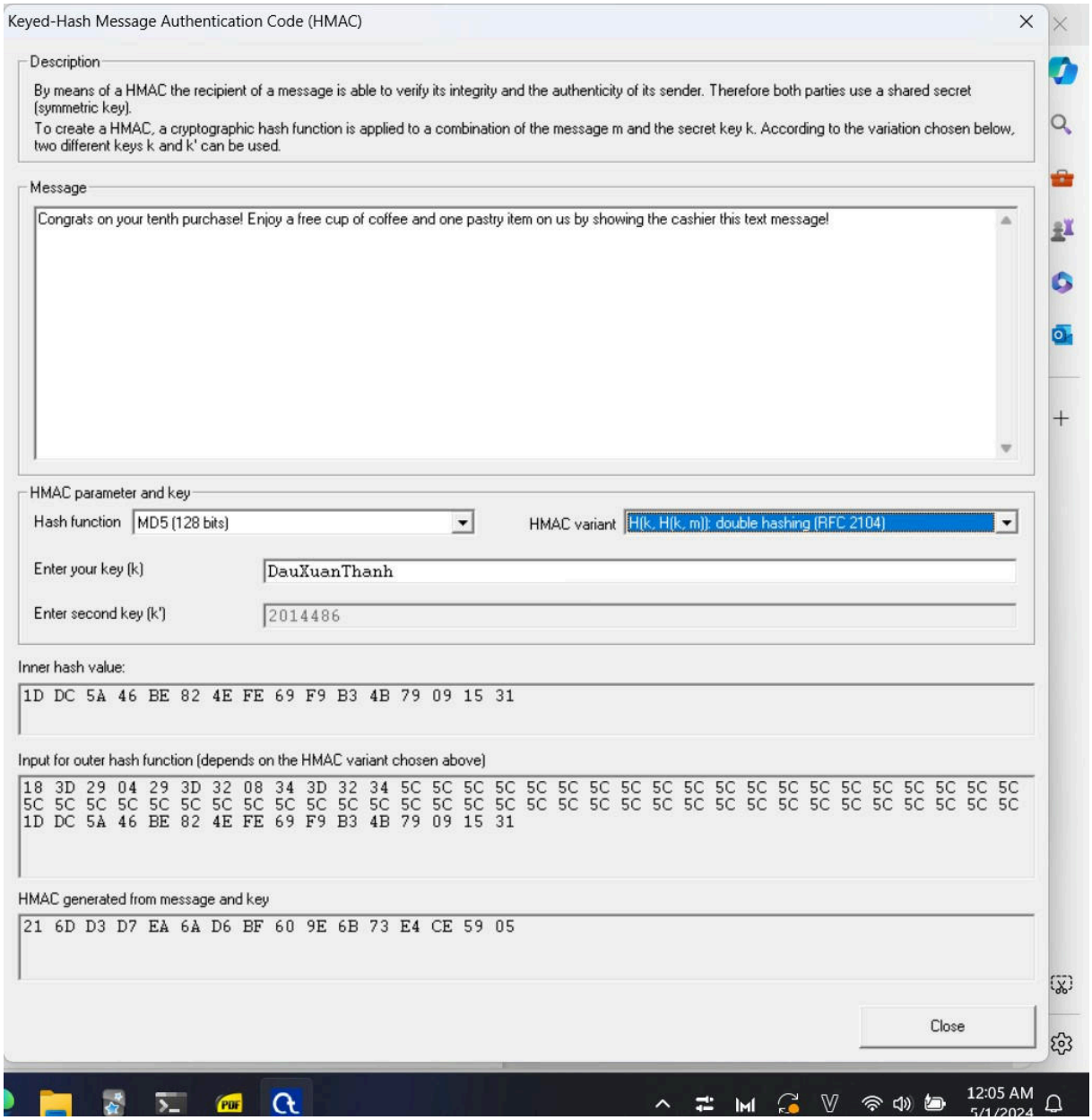
- H(k,m,k): key in front and at the back of message



- H(k,m,k'): different keys

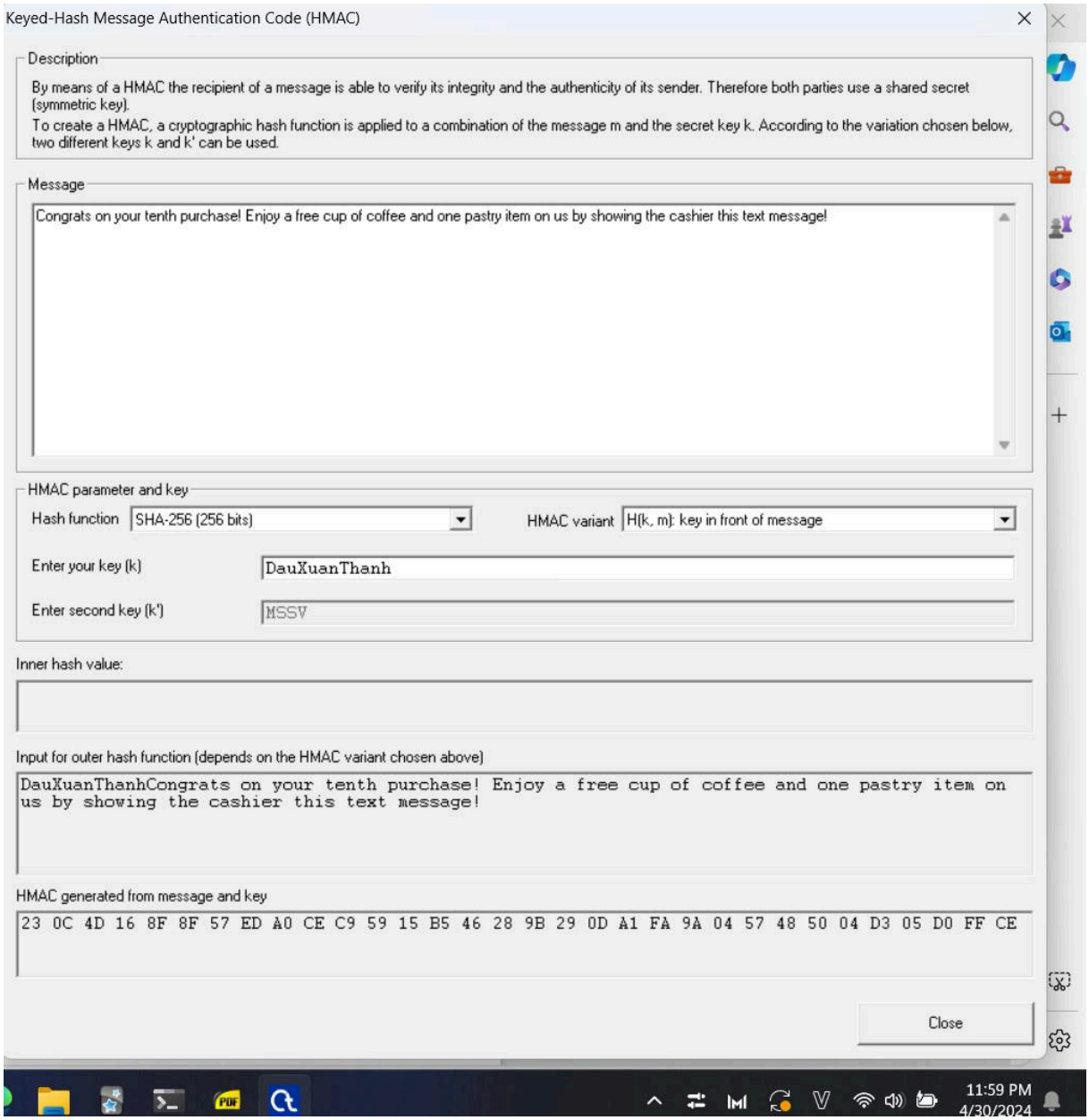


- H(k,H(k,m)): double hashing (RFC 2104)

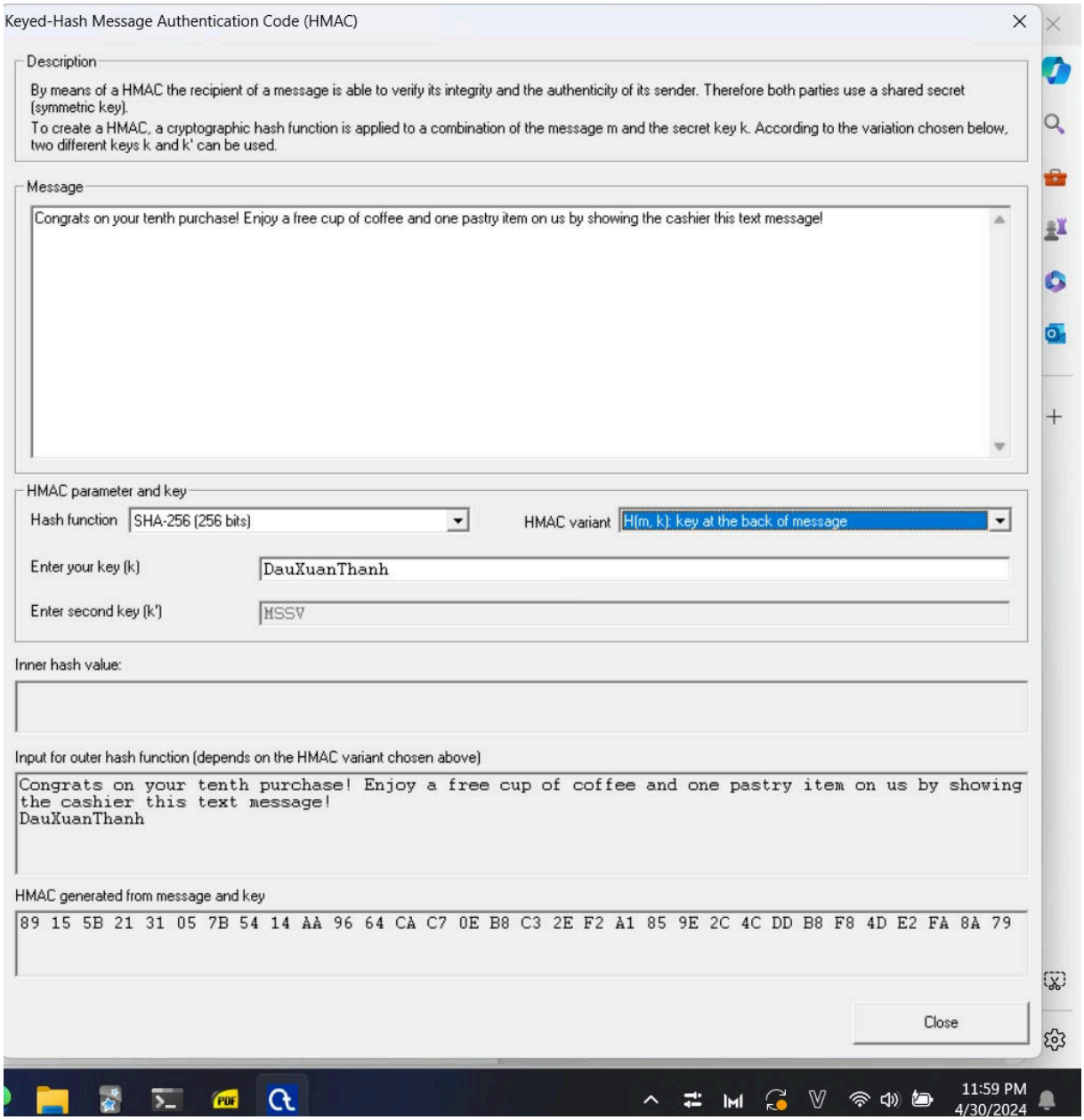


1.1.2. Tính Hmac cho hàm SHA-256

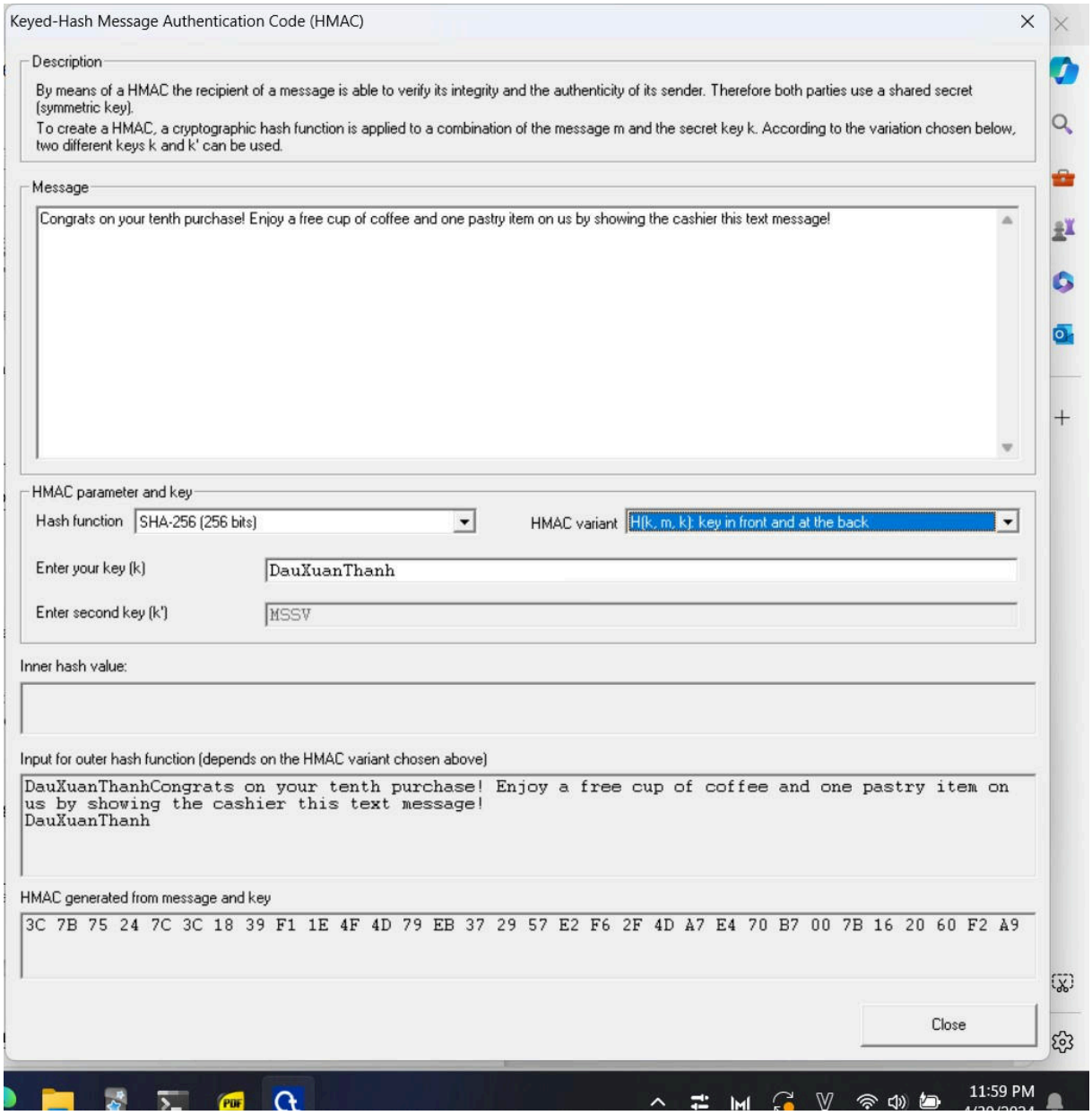
- H(k,m): key in front of message



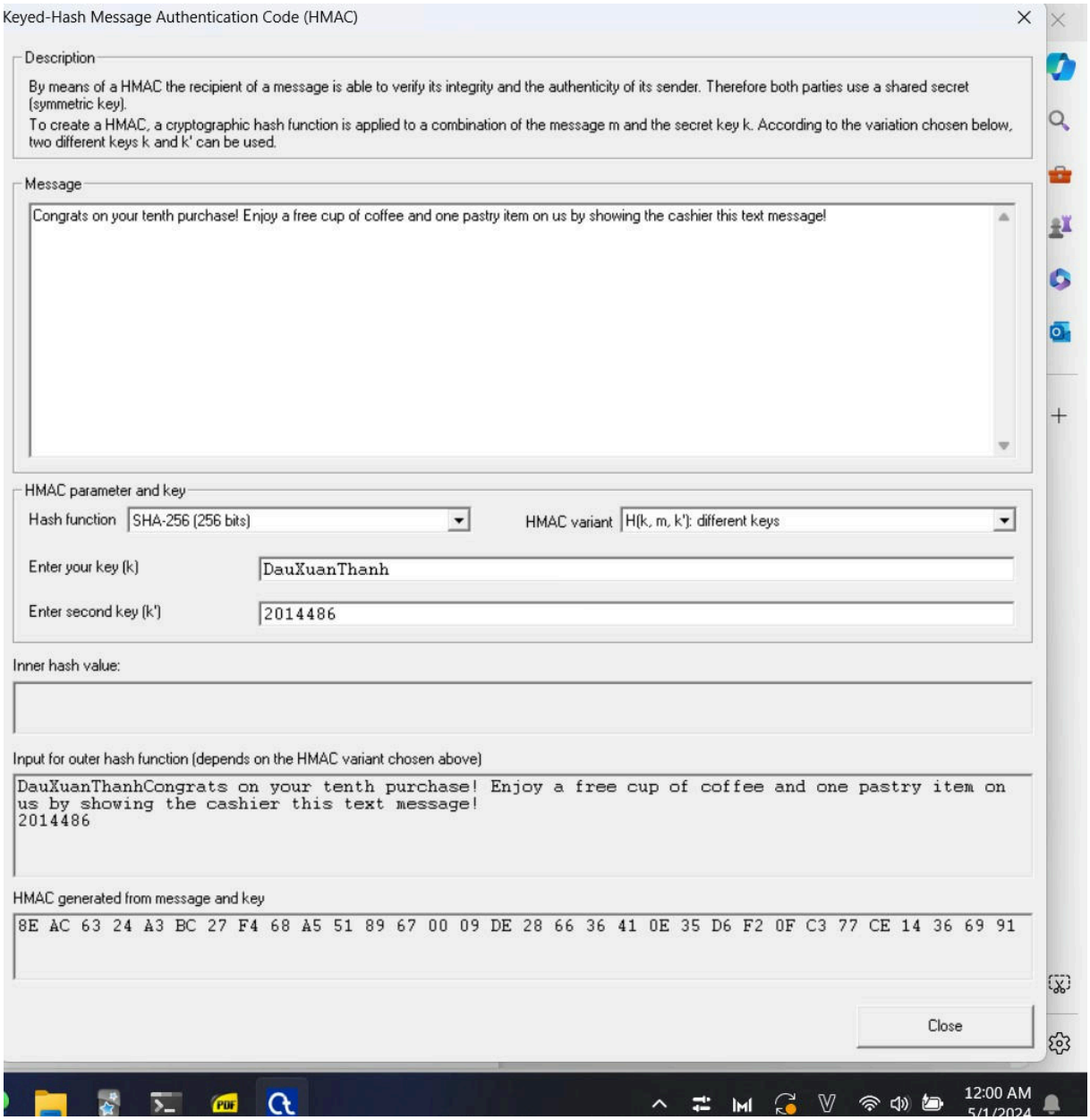
- H(m,k): key in back of message



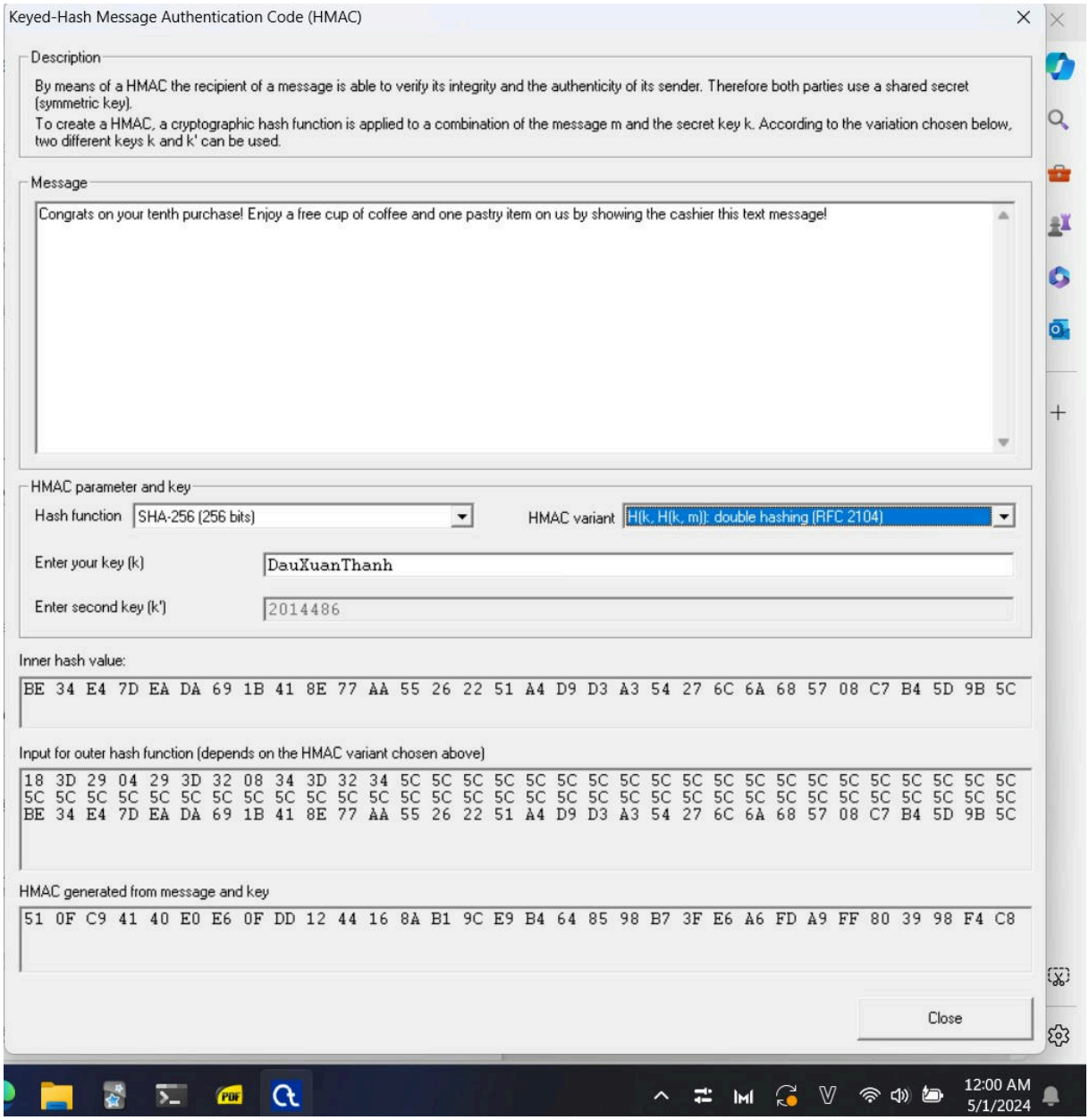
- H(k,m,k): key in front and at the back of message



- H(k,m,k'): different keys



- H(k,H(k,m)): double hashing (RFC 2104)



1.2. Câu 2: Hãy liệt kê những hình thức tấn công dựa trên xác thực thông điệp?

- Tấn công ngày sinh nhật
- Tấn công Meet in the middle
- Tấn công brute force

1.3. Câu 3: Trình bày sự khác nhau giữa mã xác thực thông điệp (MAC) và hàm băm (Hash)

	MAC	**Hashing**
Tính chất	Xác thực, toàn vẹn	Toàn vẹn

	MAC	**Hashing**
Giải thuật	Cô đọng một thông điệp M có chiều dài thay đổi dùng một khóa bí mật K thành một mã xác thực có chiều dài cố định.	Cô đọng một thông điệp M có chiều dài thay đổi thành một mã xác thực có chiều dài cố định.
Yêu cầu	• Phân bố đồng đều • Phụ thuộc như nhau trên tất cả các bit • Biết thông điệp và mã xác thực thông điệp của nó thì không khả thi để tìm ra một thông điệp khác có cùng mã xác thực thông điệp	• Cho h thì không khả thi để tìm x mà H(x)=h • Cho x thì không khả thi để tìm y mà H(y)=H(x) • Không khả thi để tìm x,y mà H(y)=H(x)

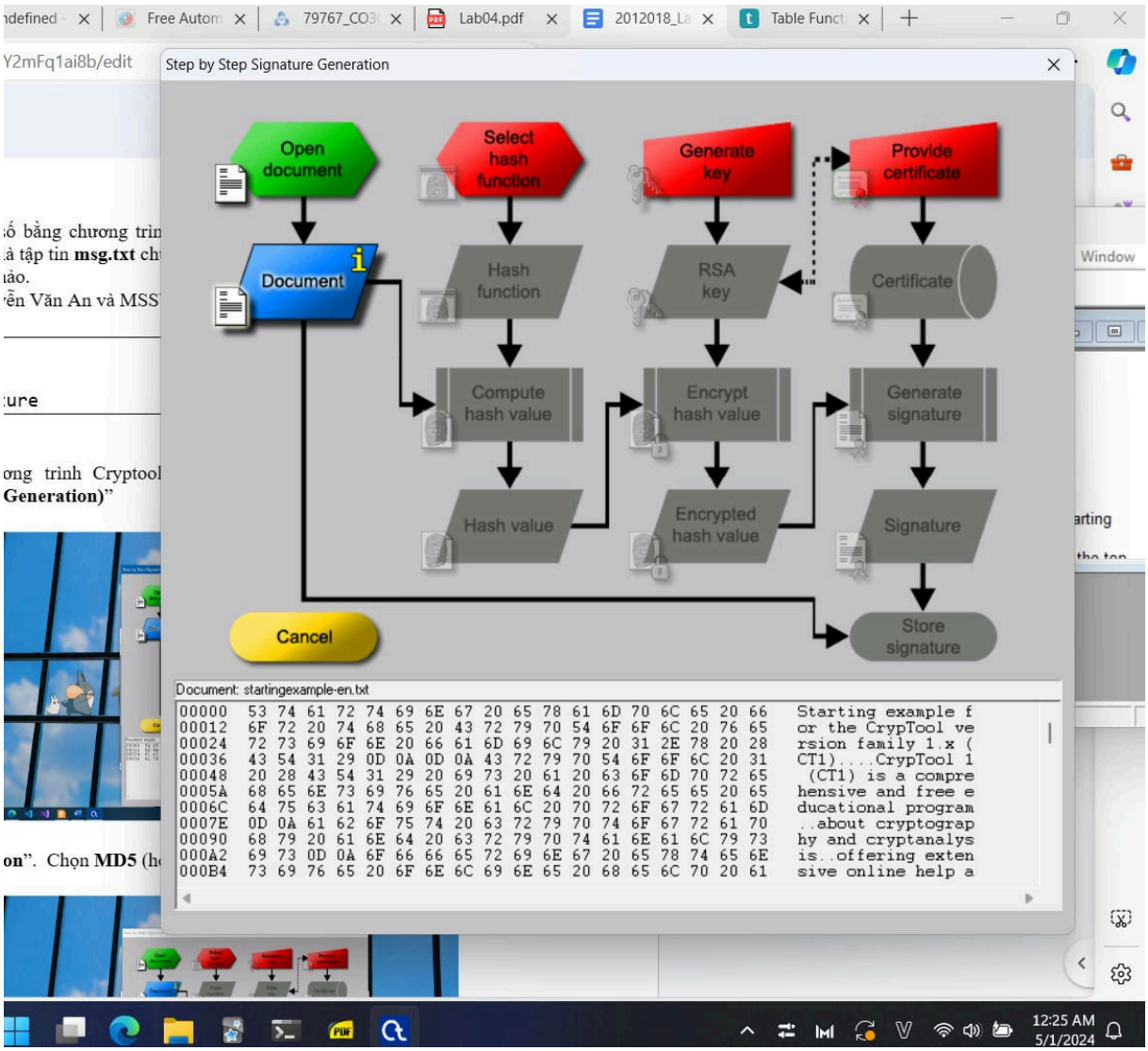
2. Chữ ký số

2.1. Câu 1: Mô phỏng chữ ký số bằng chương trình Cryptool, thực hiện theo các bước như hướng dẫn tham khảo bên dưới, với đầu vào là tập tin msg.txt chứa thông tên đầy đủ và mã số sinh viên. Chụp ảnh màn hình từng bước như phần tham khảo.

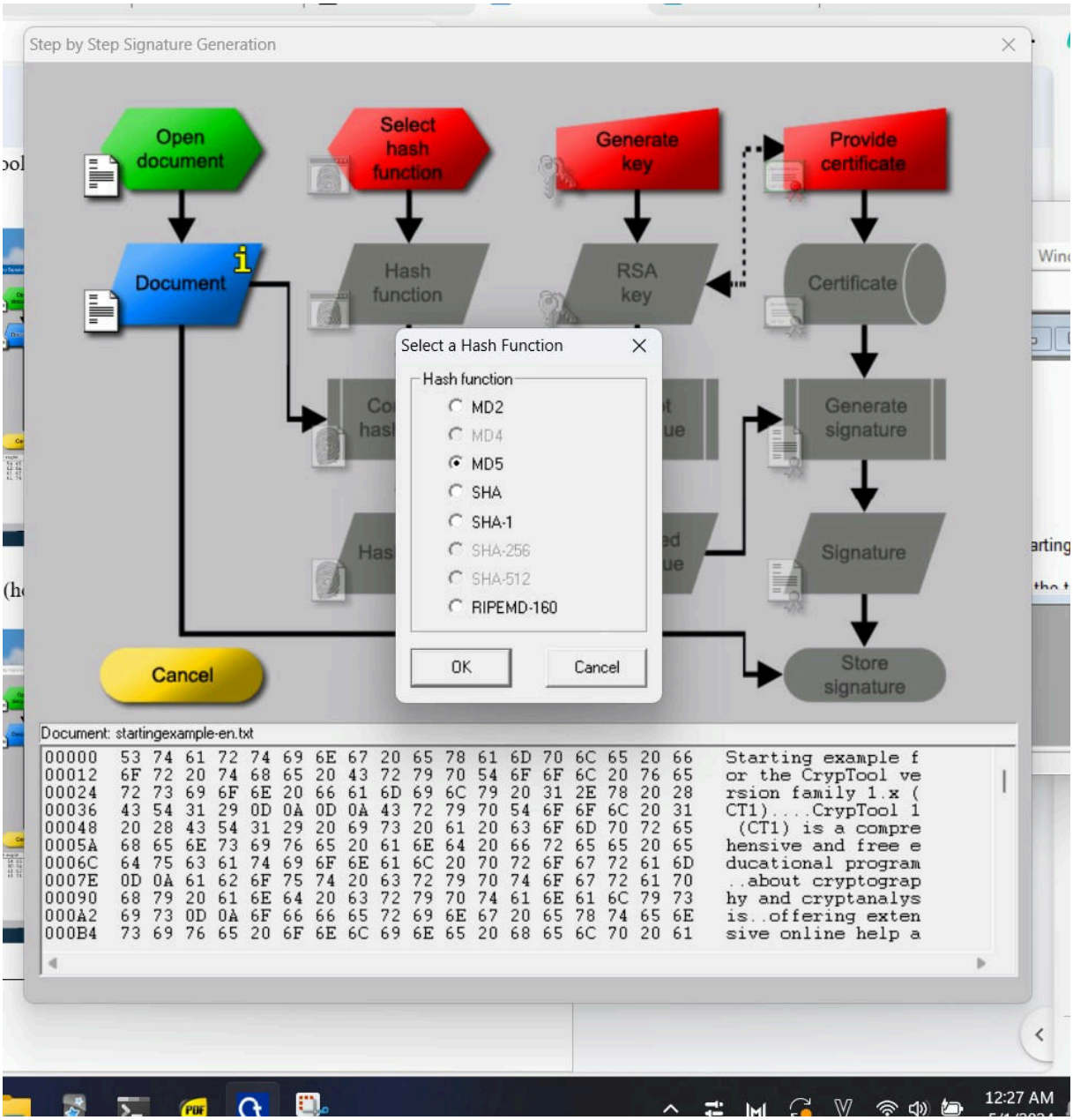
Ví dụ: sinh viên có tên Nguyễn Văn An và MSSV là 123456789, tập tin msg.txt có nội dung như sau:

```
Ten: Nguyen Van An
MSSV: 123456789
Lab 04 Digital Signature
```

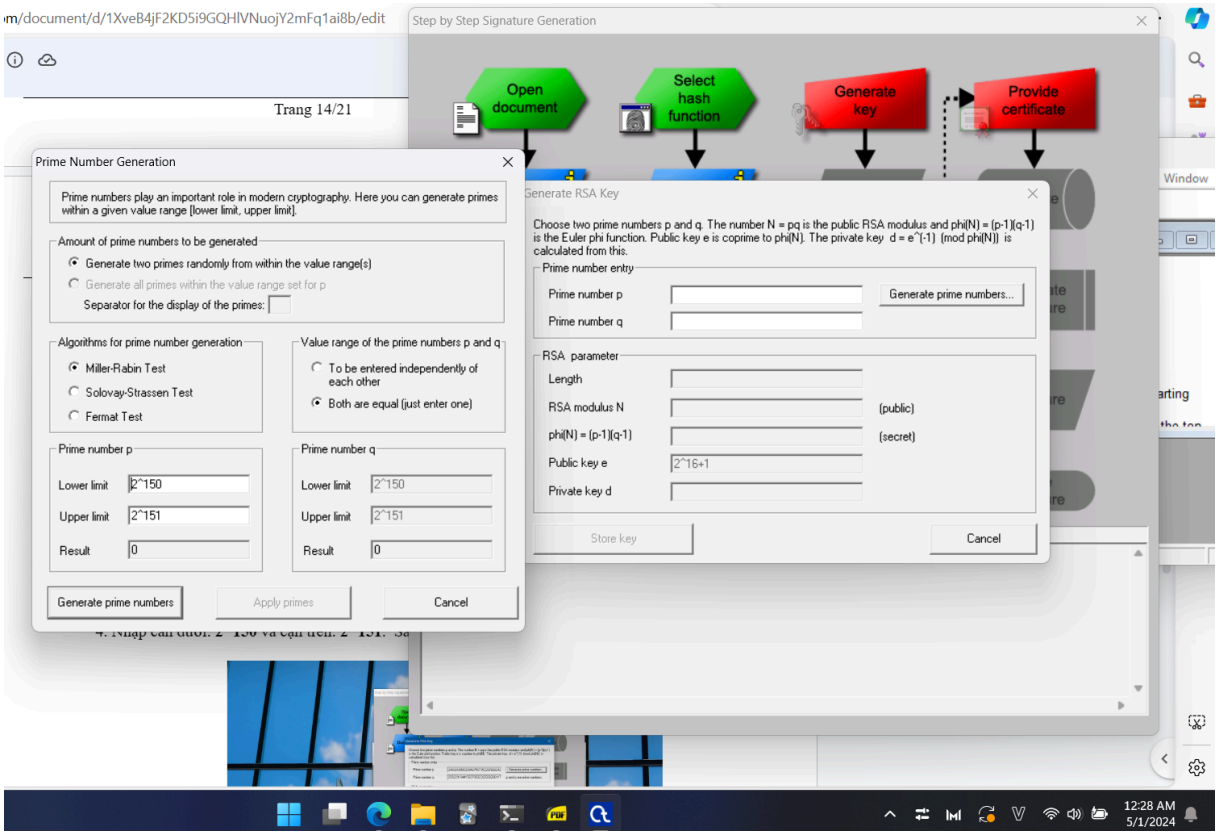
- Bước 1: Từ giao diện của chương trình Cryptool, chọn menu “Digital Signatures/PKI” → “Signature Demonstration (Signature Generation)”



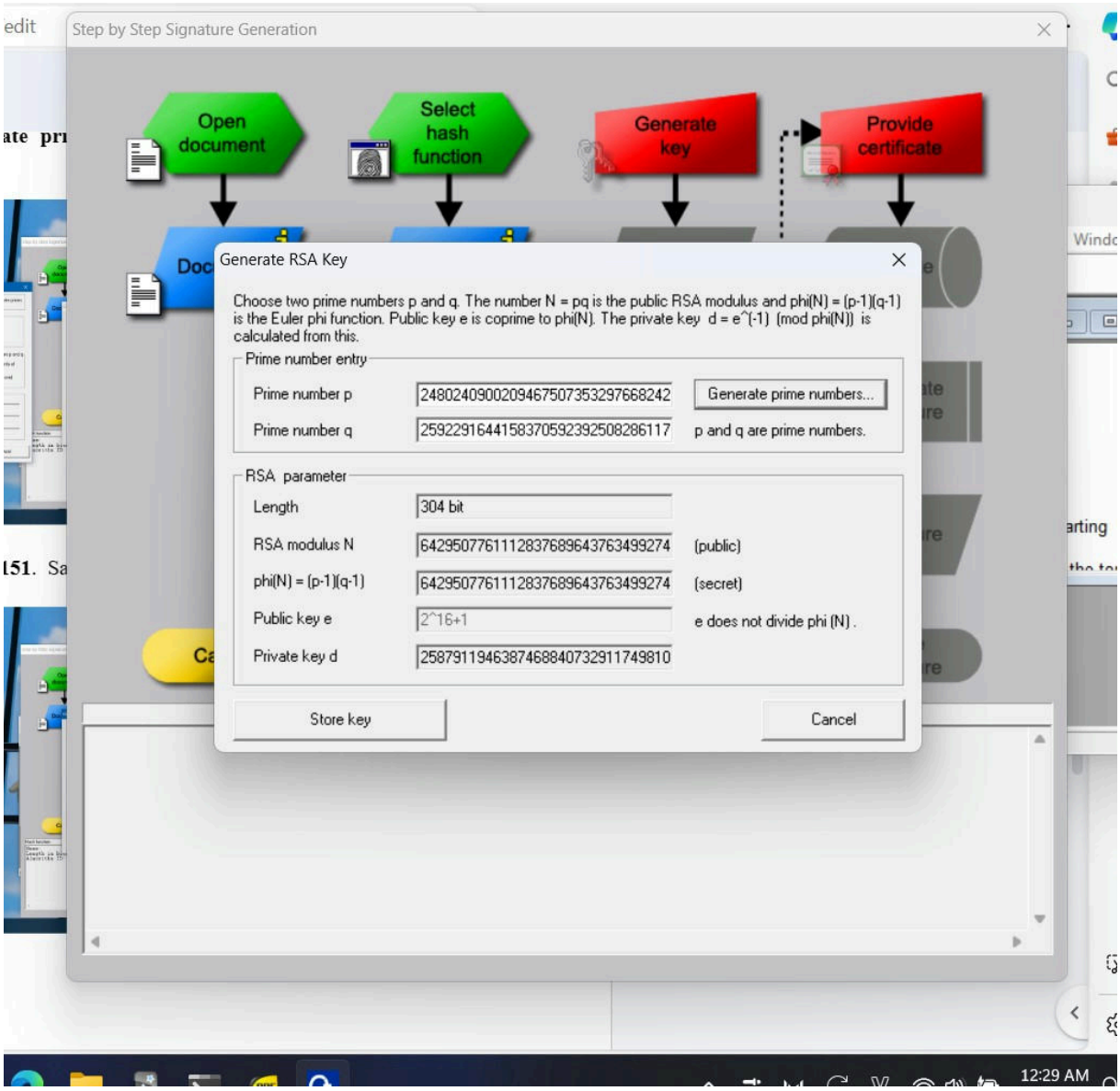
- Bước 2: Chọn “Select hash function”. Chọn MD5 (hoặc một giải thuật hash khác) và nhấn OK.



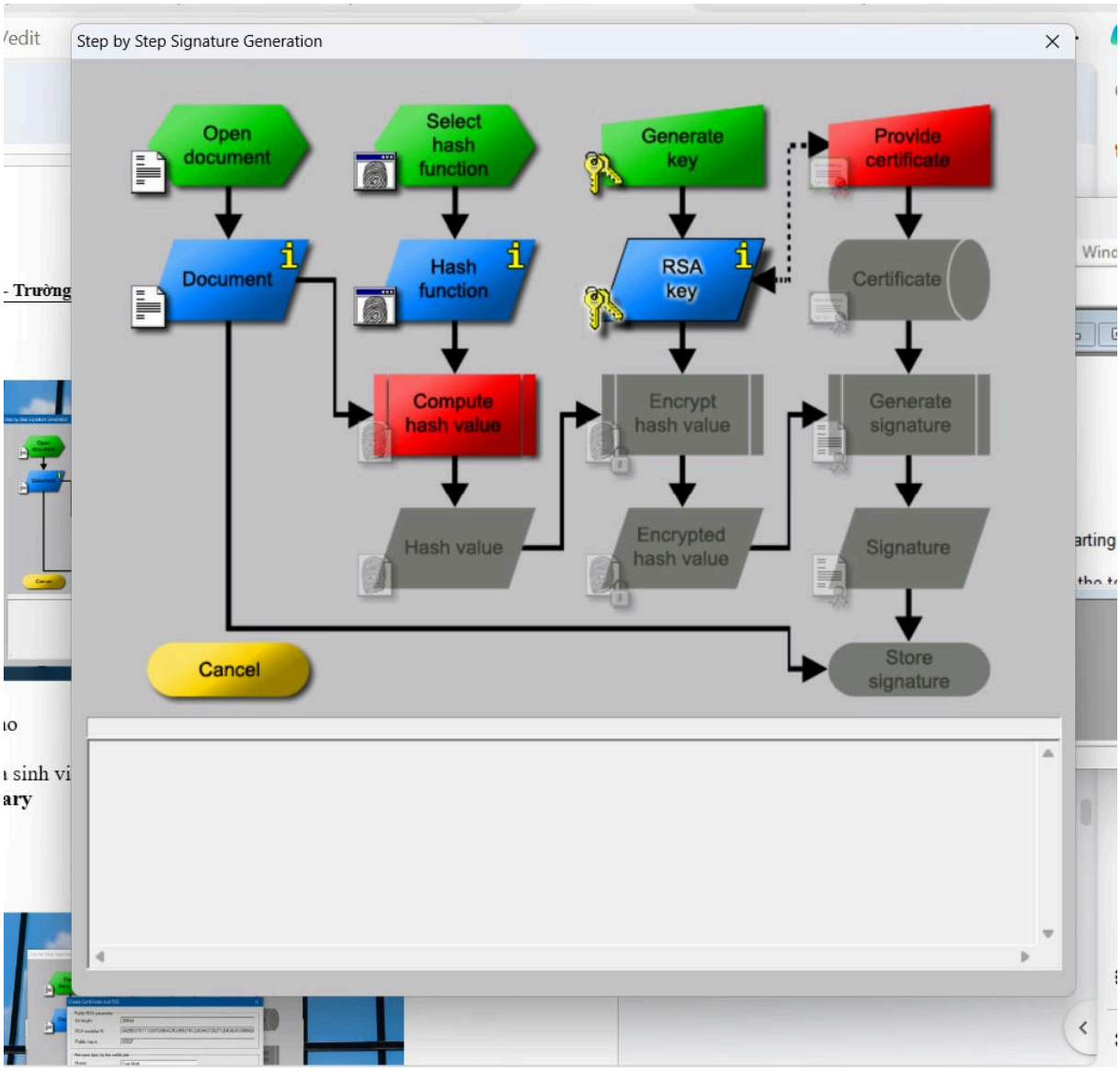
- Chọn “Generate Key” và “Generate prime numbers” trong hộp thoại step by step Signature Generation



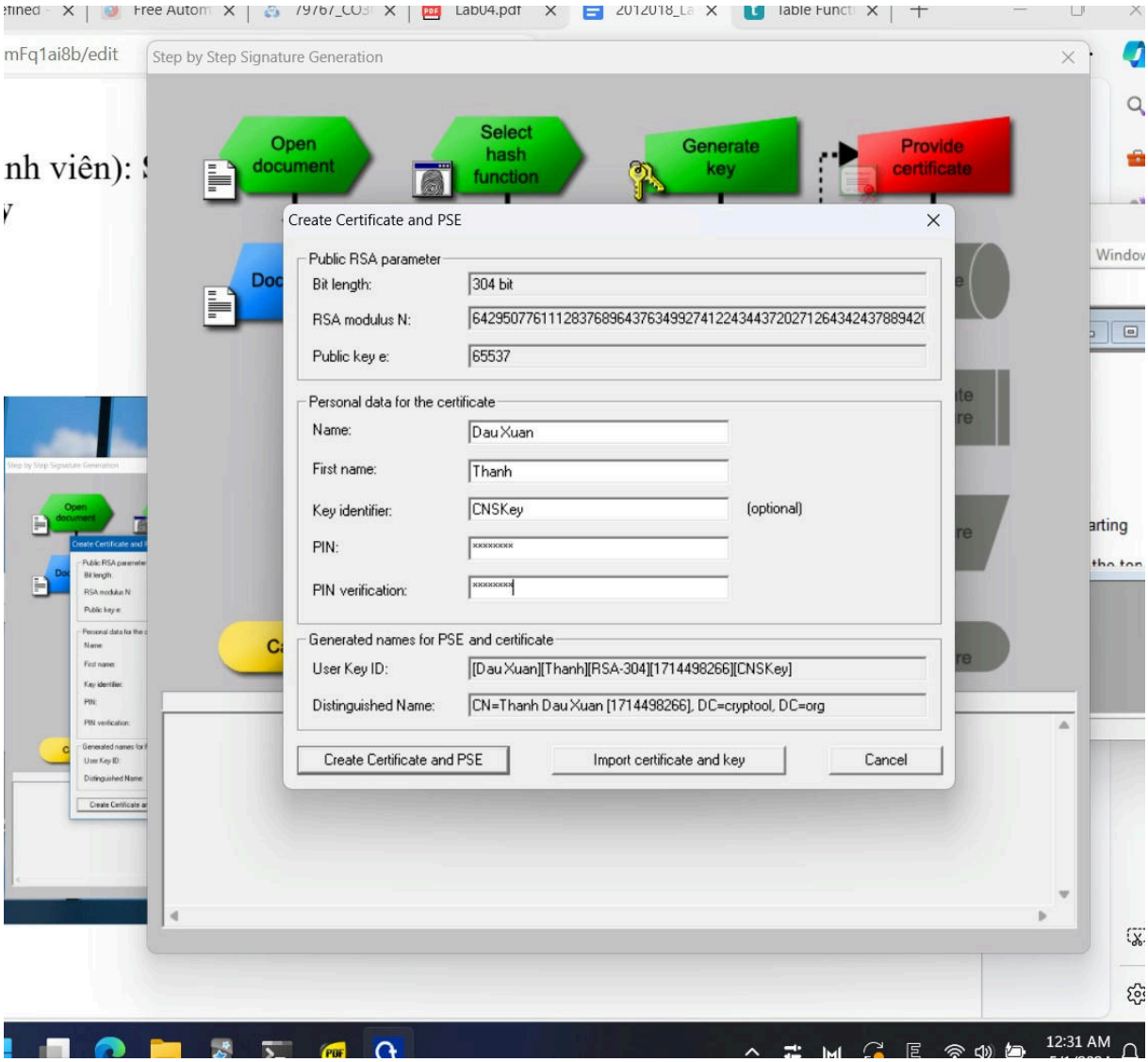
- Nhập cân dưới: 2^150 và cận trên: 2^151. Sau đó nhấn nút Generate prime numbers và apply primes.



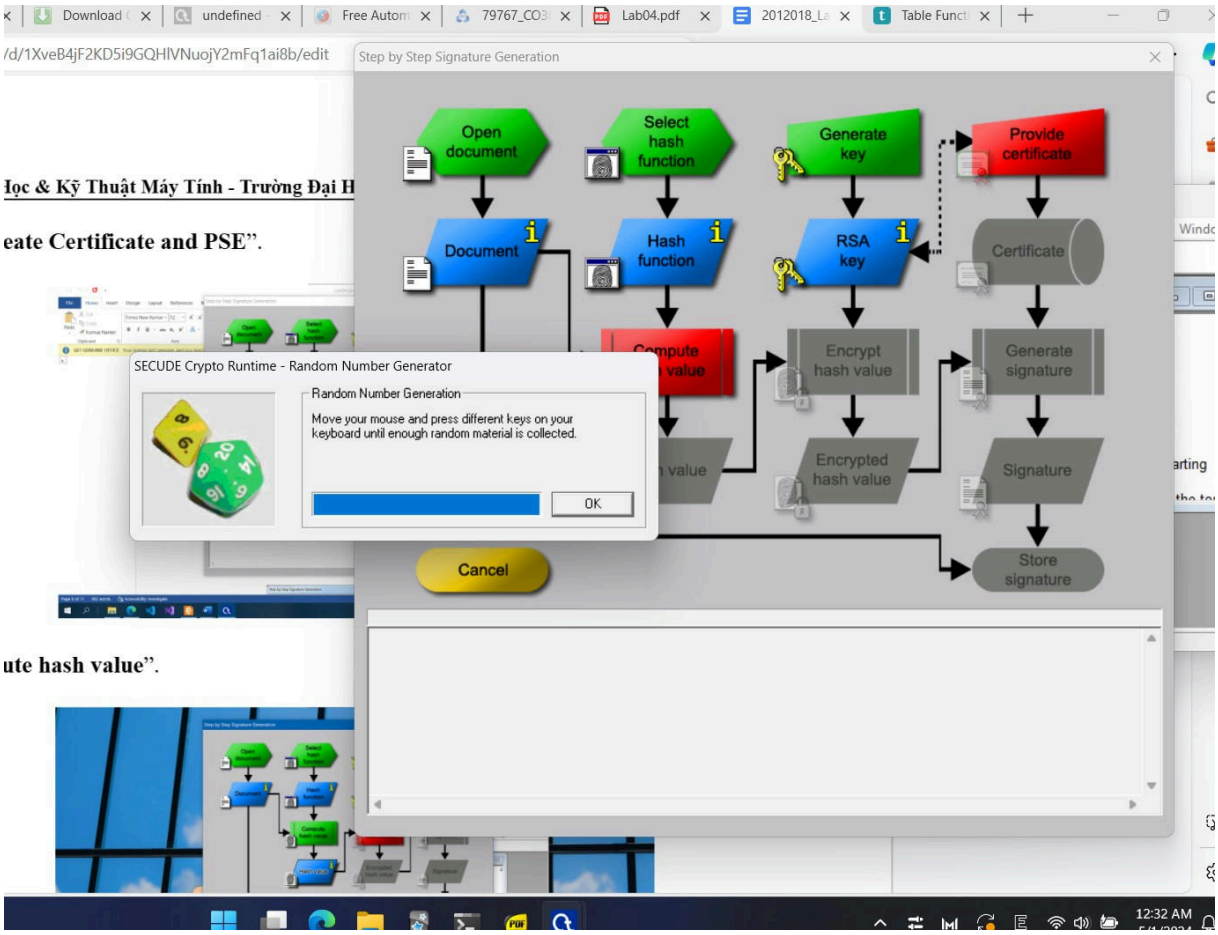
- Nhấn nút Store key



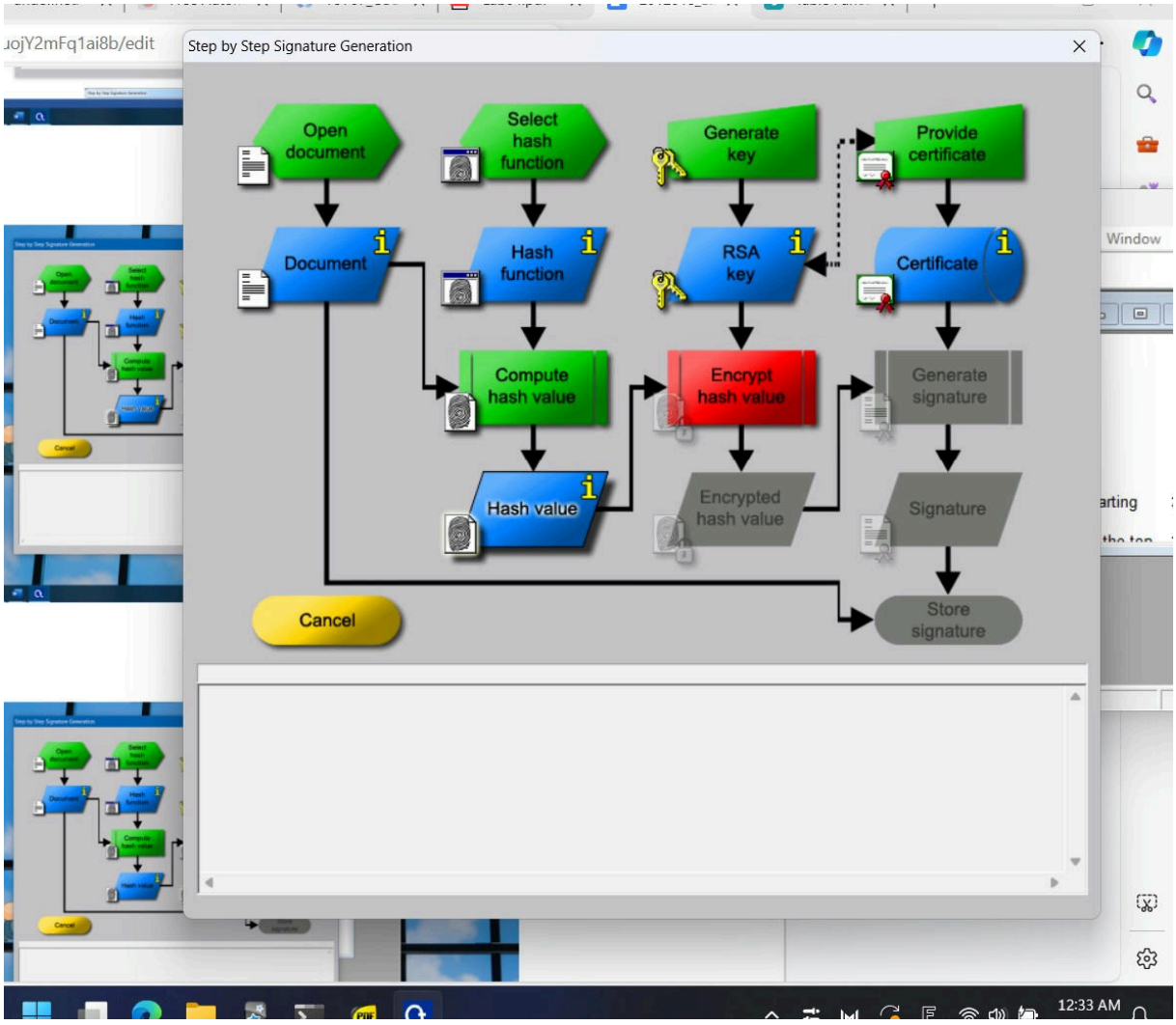
- Nhấn nút Provide certificate, nhập vào
  - Name (nhập thông tin họ và chữ lót của sinh viên): Smith
  - First name (nhập tên của sinh viên): Mary
  - Key identifier (key): Mary key
  - PIN: cryptool
  - PIN verification: cryptool



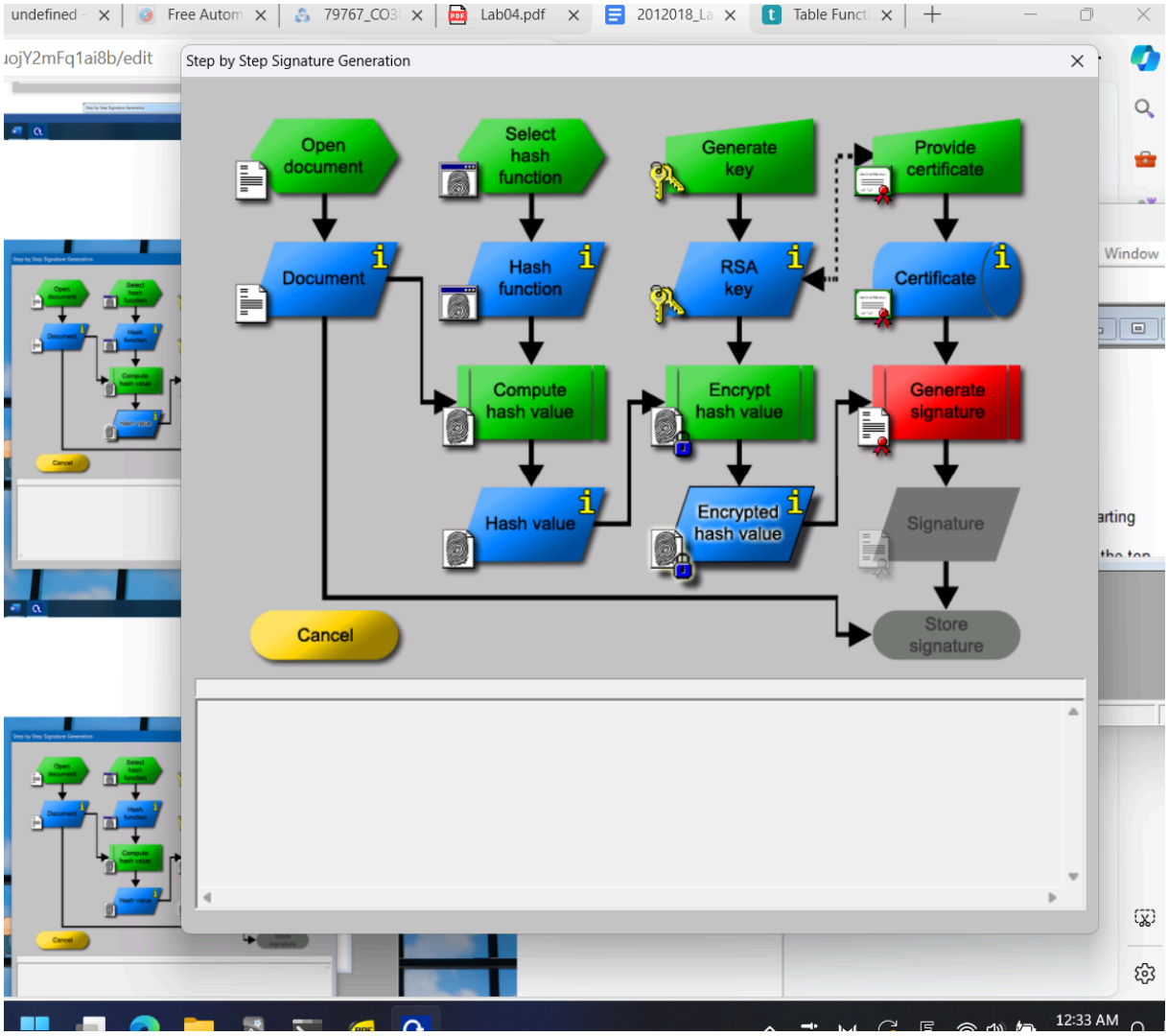
- Nhấn nút “Create Certificate and PSE”.



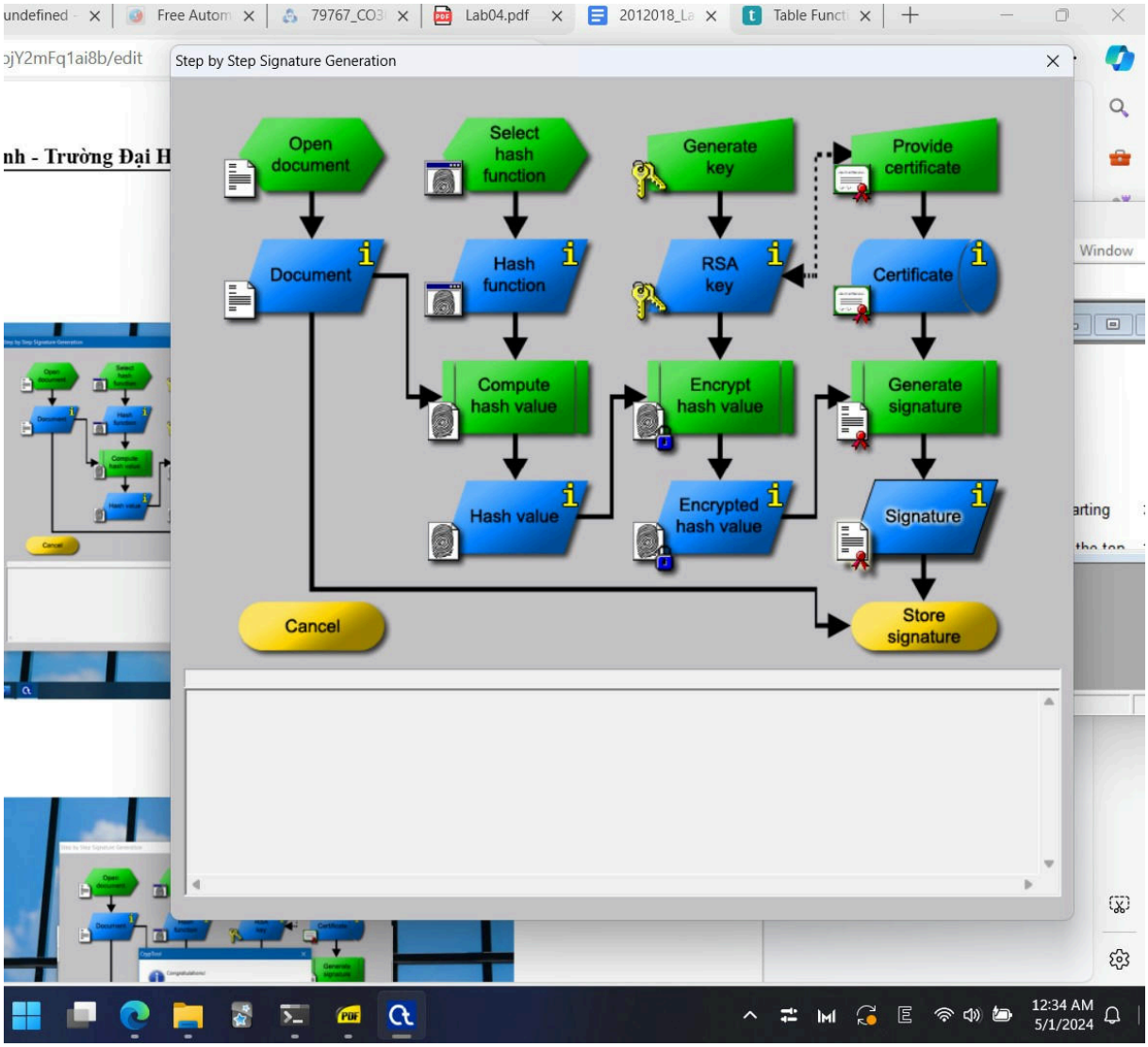
- Chọn “Compute hash value”.



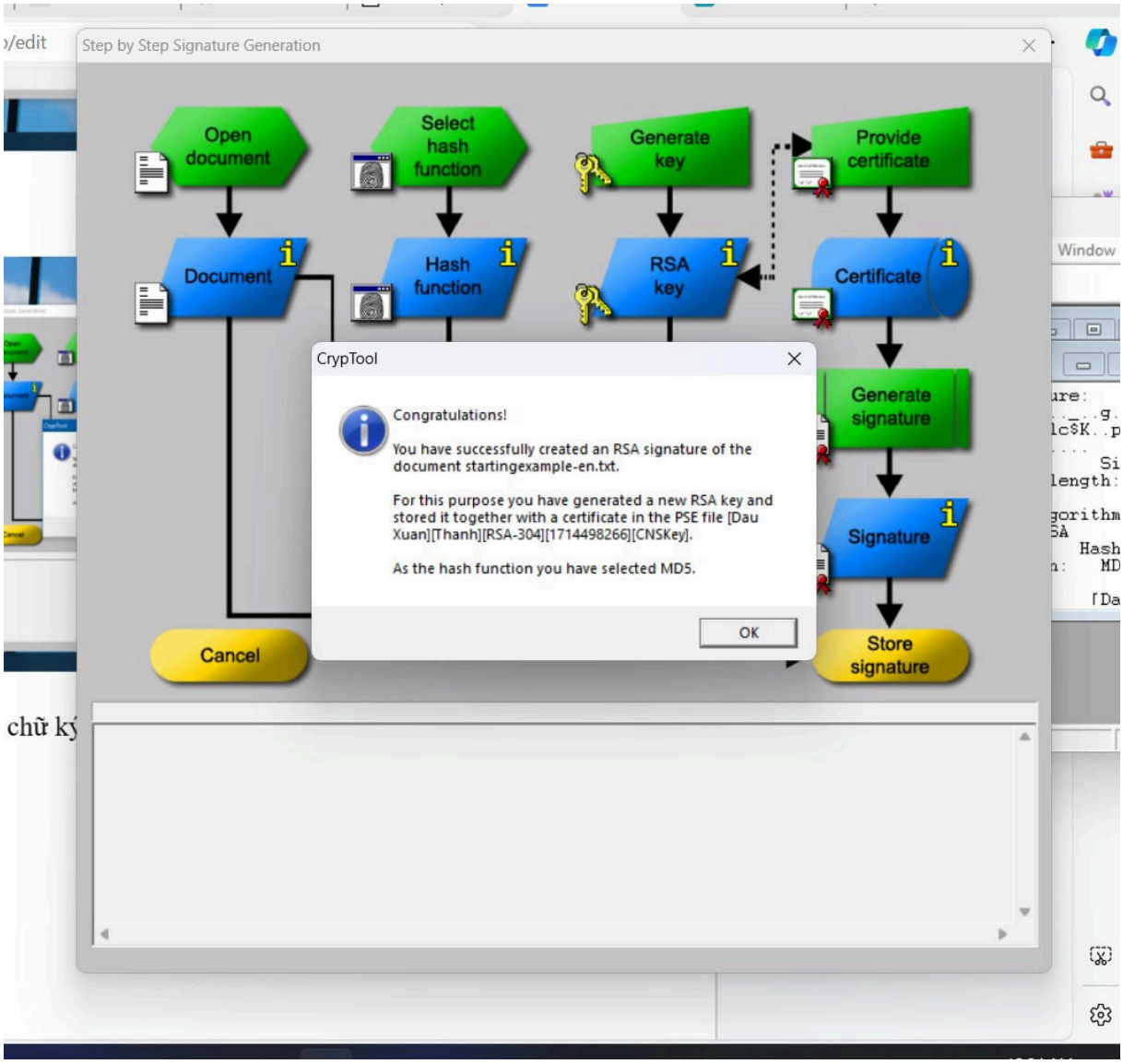
- Chọn “Encrypt hash value”.



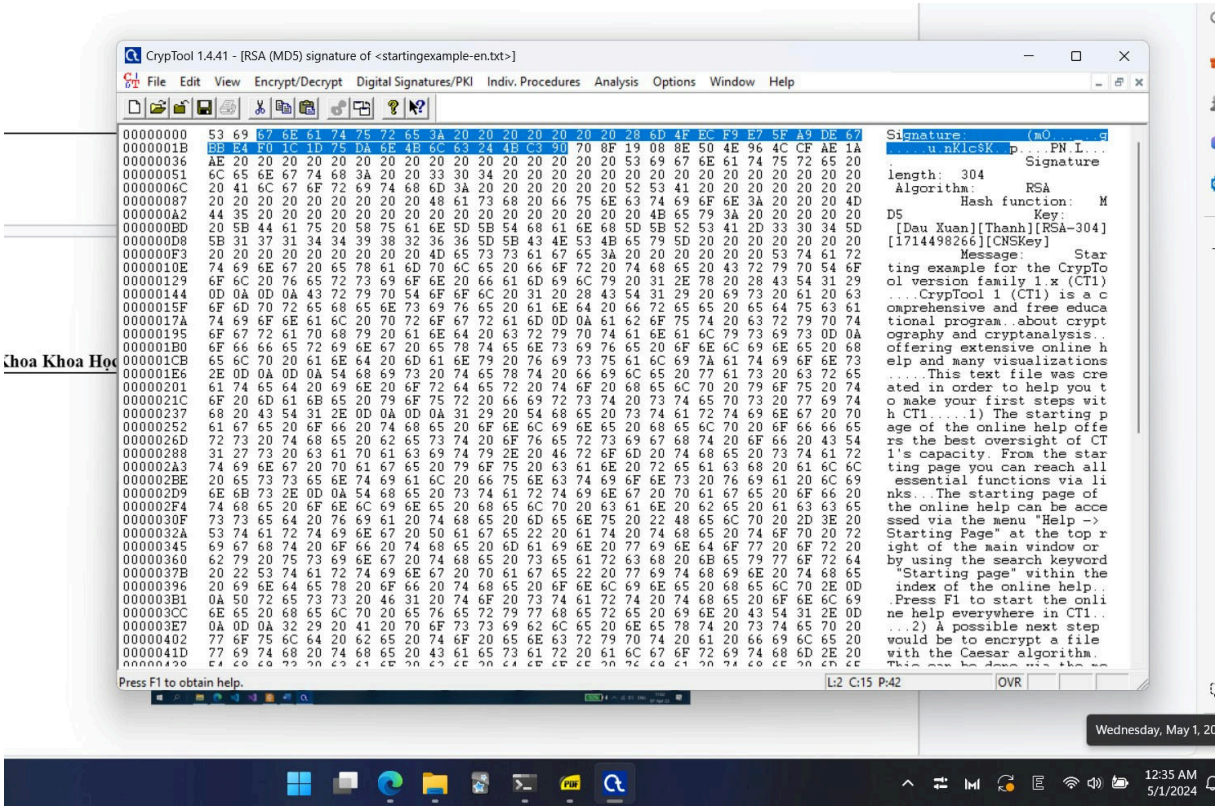
- Chọn “Generate signature”



- Chọn “Store signature”



- Nhấn nút OK, chúng ta được thông điệp và chữ ký số như hình bên dưới.



2.2. Câu 2: Hãy cho biết các yêu cầu của chữ ký số?

- Phải phụ thuộc trên thông điệp được ký.
- Phải sử dụng thông tin duy nhất từ người gửi để tránh giả mạo và từ chối.
- Phải tương đối dễ dàng để tạo.
- Phải tương đối dễ dàng để nhận biết và xác minh.
- Không khả thi trong tính toán để giả mạo
- Một thông điệp mới với chữ ký số đang tồn tại.
- Chữ ký số cho một thông điệp đã cho.
- Lưu trữ chữ ký số trong thực tế

Tài liệu tham khảo