

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

1. Mã xác thực thông điệp MAC	3
1.1. Câu 1: Sử dụng công cụ Cryptool để tính toán HMAC cho một thông điệp theo các	3
1.1.1. Tính Hmac cho hàm MD5	3
1.1.2. Tính Hmac cho hàm SHA-256	7
1.2. Câu 2: Hãy liệt kê những hình thức tấn công dựa trên xác thực thông điệp?	12
1.3. Câu 3: Trình bày sự khác nhau giữa mã xác thực thông điệp (MAC) và hàm băm (Hash)	12
2. Chữ ký số	14
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 tin đầy đủ và mã số sinh viên. Chụp ảnh màn hình từng bước như phần tham khảo.	14
2.2. Câu 2: Hãy cho biết các yêu cầu của chữ ký số?	25
Tài liệu tham khảo	26

Danh mục hình ảnh

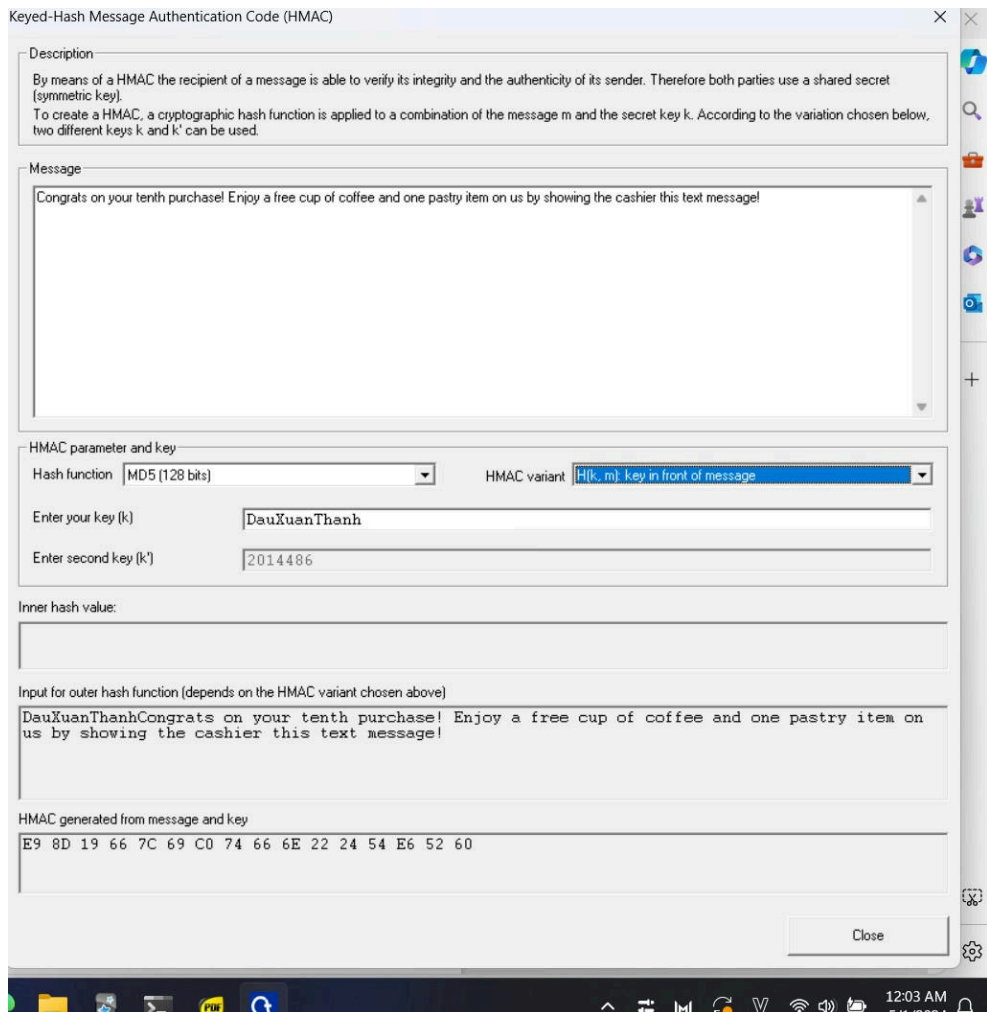
1. Mã xác thực thông điệp MAC

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

Keyed-Hash Message Authentication Code (HMAC)

Description

By means of a HMAC the recipient of a message is able to verify its integrity and the authenticity of its sender. Therefore both parties use a shared secret (symmetric key).
To create a HMAC, a cryptographic hash function is applied to a combination of the message m and the secret key k . According to the variation chosen below, two different keys k and k' can be used.

Message

Congrats on your tenth purchase! Enjoy a free cup of coffee and one pastry item on us by showing the cashier this text message!

HMAC parameter and key

Hash function: MD5 (128 bits) HMAC variant: $H(m, k)$: key at the back of message

Enter your key (k): DauXuanThanh

Enter second key (k'): 2014486

Inner hash value:

Input for outer hash function (depends on the HMAC variant chosen above)

Congrats on your tenth purchase! Enjoy a free cup of coffee and one pastry item on us by showing the cashier this text message!
DauXuanThanh

HMAC generated from message and key

DD 24 7F D3 B2 59 B1 9A C3 E7 D6 9F B0 43 66 66

Close

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

Keyed-Hash Message Authentication Code (HMAC)

Description
By means of a HMAC the recipient of a message is able to verify its integrity and the authenticity of its sender. Therefore both parties use a shared secret (symmetric key).
To create a HMAC, a cryptographic hash function is applied to a combination of the message m and the secret key k. According to the variation chosen below, two different keys k and k' can be used.

Message
Congrats on your tenth purchase! Enjoy a free cup of coffee and one pastry item on us by showing the cashier this text message!

HMAC parameter and key
Hash function: MD5 (128 bits) HMAC variant: $H(k, m, k)$: key in front and at the back
Enter your key (k): DauXuanThanh
Enter second key (k'): 2014486

Inner hash value:

Input for outer hash function (depends on the HMAC variant chosen above)
DauXuanThanhCongrats on your tenth purchase! Enjoy a free cup of coffee and one pastry item on us by showing the cashier this text message!
DauXuanThanh

HMAC generated from message and key
14 6F 4D 41 42 DD AE D2 DD CC FF A5 D6 3F 73 D1

Close

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

Keyed-Hash Message Authentication Code (HMAC)

Description

By means of a HMAC the recipient of a message is able to verify its integrity and the authenticity of its sender. Therefore both parties use a shared secret (symmetric key).
To create a HMAC, a cryptographic hash function is applied to a combination of the message m and the secret key k . According to the variation chosen below, two different keys k and k' can be used.

Message

Congrats on your tenth purchase! Enjoy a free cup of coffee and one pastry item on us by showing the cashier this text message!

HMAC parameter and key

Hash function: MD5 (128 bits) HMAC variant: $H(k, m, k')$: different keys

Enter your key (k): DauXuanThanh

Enter second key (k'): 2014486

Inner hash value:

Input for outer hash function (depends on the HMAC variant chosen above)

DauXuanThanhCongrats on your tenth purchase! Enjoy a free cup of coffee and one pastry item on us by showing the cashier this text message!
2014486

HMAC generated from message and key

7A F4 6F 25 65 F4 E1 E9 8E 2D FD 64 11 1E 94 E8

Close

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

Description

By means of a HMAC the recipient of a message is able to verify its integrity and the authenticity of its sender. Therefore both parties use a shared secret (symmetric key).
To create a HMAC, a cryptographic hash function is applied to a combination of the message m and the secret key k. According to the variation chosen below, two different keys k and k' can be used.

Message

Congrats on your tenth purchase! Enjoy a free cup of coffee and one pastry item on us by showing the cashier this text message!

HMAC parameter and key

Hash functionMD5 (128 bits)

HMAC variantH(k, H(k, m)): double hashing (RFC 2104)

Enter your key (k)DauXuanThanh

Enter second key (k')2014486

Inner hash value:

1D DC 5A 46 BE 82 4E FE 69 F9 B3 4B 79 09 15 31

Input for outer hash function (depends on the HMAC variant chosen above)

18 3D 29 04 29 3D 32 08 34 3D 32 34 5C 5C 5C 5C 5C 5C 5C 5C 5C 5C 5C 5C 5C 5C 5C 5C 5C 5C
5C
1D DC 5A 46 BE 82 4E FE 69 F9 B3 4B 79 09 15 31

HMAC generated from message and key

21 6D D3 D7 EA 6A D6 BF 60 9E 6B 73 E4 CE 59 05

Close

1.1.2. Tính Hmac cho hàm SHA-256

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

Keyed-Hash Message Authentication Code (HMAC)

Description

By means of a HMAC the recipient of a message is able to verify its integrity and the authenticity of its sender. Therefore both parties use a shared secret (symmetric key).
To create a HMAC, a cryptographic hash function is applied to a combination of the message m and the secret key k. According to the variation chosen below, two different keys k and k' can be used.

Message

Congrats on your tenth purchase! Enjoy a free cup of coffee and one pastry item on us by showing the cashier this text message!

HMAC parameter and key

Hash function: SHA-256 (256 bits) HMAC variant: $H(k, m)$: key in front of message

Enter your key (k): DauXuanThanh

Enter second key (k'): HSSV

Inner hash value:

Input for outer hash function (depends on the HMAC variant chosen above)

DauXuanThanhCongrats on your tenth purchase! Enjoy a free cup of coffee and one pastry item on us by showing the cashier this text message!

HMAC generated from message and key

23 0C 4D 16 8F 8F 57 ED A0 CE C9 59 15 B5 46 28 9B 29 0D A1 FA 9A 04 57 48 50 04 D3 05 D0 FF CE

Close

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

Keyed-Hash Message Authentication Code (HMAC)

Description

By means of a HMAC the recipient of a message is able to verify its integrity and the authenticity of its sender. Therefore both parties use a shared secret (symmetric key).
To create a HMAC, a cryptographic hash function is applied to a combination of the message m and the secret key k . According to the variation chosen below, two different keys k and k' can be used.

Message

Congrats on your tenth purchase! Enjoy a free cup of coffee and one pastry item on us by showing the cashier this text message!

HMAC parameter and key

Hash function: SHA-256 (256 bits) HMAC variant: $H(m, k)$: key at the back of message

Enter your key (k): DauXuanThanh

Enter second key (k'): MSSV

Inner hash value:

Input for outer hash function (depends on the HMAC variant chosen above)

Congrats on your tenth purchase! Enjoy a free cup of coffee and one pastry item on us by showing the cashier this text message!
DauXuanThanh

HMAC generated from message and key

89 15 5B 21 31 05 7B 54 14 AA 96 64 CA C7 0E B8 C3 2E F2 A1 85 9E 2C 4C DD B8 F8 4D E2 FA 8A 79

Close

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

Keyed-Hash Message Authentication Code (HMAC)

Description

By means of a HMAC the recipient of a message is able to verify its integrity and the authenticity of its sender. Therefore both parties use a shared secret (symmetric key).
To create a HMAC, a cryptographic hash function is applied to a combination of the message m and the secret key k . According to the variation chosen below, two different keys k and k' can be used.

Message

Congrats on your tenth purchase! Enjoy a free cup of coffee and one pastry item on us by showing the cashier this text message!

HMAC parameter and key

Hash function: SHA-256 (256 bits) HMAC variant: $H(k, m, k)$: key in front and at the back

Enter your key (k): DauXuanThanh

Enter second key (k'): MSSV

Inner hash value:

Input for outer hash function (depends on the HMAC variant chosen above)

DauXuanThanhCongrats on your tenth purchase! Enjoy a free cup of coffee and one pastry item on us by showing the cashier this text message!
DauXuanThanh

HMAC generated from message and key

3C 7B 75 24 7C 3C 18 39 F1 1E 4F 4D 79 EB 37 29 57 E2 F6 2F 4D A7 E4 70 B7 00 7B 16 20 60 F2 A9

Close

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

Keyed-Hash Message Authentication Code (HMAC)

Description

By means of a HMAC the recipient of a message is able to verify its integrity and the authenticity of its sender. Therefore both parties use a shared secret (symmetric key).
To create a HMAC, a cryptographic hash function is applied to a combination of the message m and the secret key k . According to the variation chosen below, two different keys k and k' can be used.

Message

Congrats on your tenth purchase! Enjoy a free cup of coffee and one pastry item on us by showing the cashier this text message!

HMAC parameter and key

Hash function: SHA-256 (256 bits) HMAC variant: $H(k, m, k')$: different keys

Enter your key (k): DauXuanThanh

Enter second key (k'): 2014486

Inner hash value:

Input for outer hash function (depends on the HMAC variant chosen above)

DauXuanThanhCongrats on your tenth purchase! Enjoy a free cup of coffee and one pastry item on us by showing the cashier this text message!
2014486

HMAC generated from message and key

8E AC 63 24 A3 BC 27 F4 68 A5 51 89 67 00 09 DE 28 66 36 41 0E 35 D6 F2 0F C3 77 CE 14 36 69 91

Close

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

Description

By means of a HMAC the recipient of a message is able to verify its integrity and the authenticity of its sender. Therefore both parties use a shared secret (symmetric key).
To create a HMAC, a cryptographic hash function is applied to a combination of the message m and the secret key k. According to the variation chosen below, two different keys k and k' can be used.

Message

Congrats on your tenth purchase! Enjoy a free cup of coffee and one pastry item on us by showing the cashier this text message!

HMAC parameter and key

Hash functionSHA-256 (256 bits)

HMAC variantH(k, H(k, m)): double hashing (RFC 2104)

Enter your key (k)DauXuanThanh

Enter second key (k')2014486

Inner hash value:

BE 34 E4 7D EA DA 69 1B 41 8E 77 AA 55 26 22 51 A4 D9 D3 A3 54 27 6C 6A 68 57 08 C7 B4 5D 9B 5C

Input for outer hash function (depends on the HMAC variant chosen above)

18 3D 29 04 29 3D 32 08 34 3D 32 34 5C
5C
BE 34 E4 7D EA DA 69 1B 41 8E 77 AA 55 26 22 51 A4 D9 D3 A3 54 27 6C 6A 68 57 08 C7 B4 5D 9B 5C

HMAC generated from message and key

51 0F C9 41 40 E0 E6 0F DD 12 44 16 8A B1 9C E9 B4 64 85 98 B7 3F E6 A6 FD A9 FF 80 39 98 F4 C8

Close

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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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 $H(y)=H(x)$

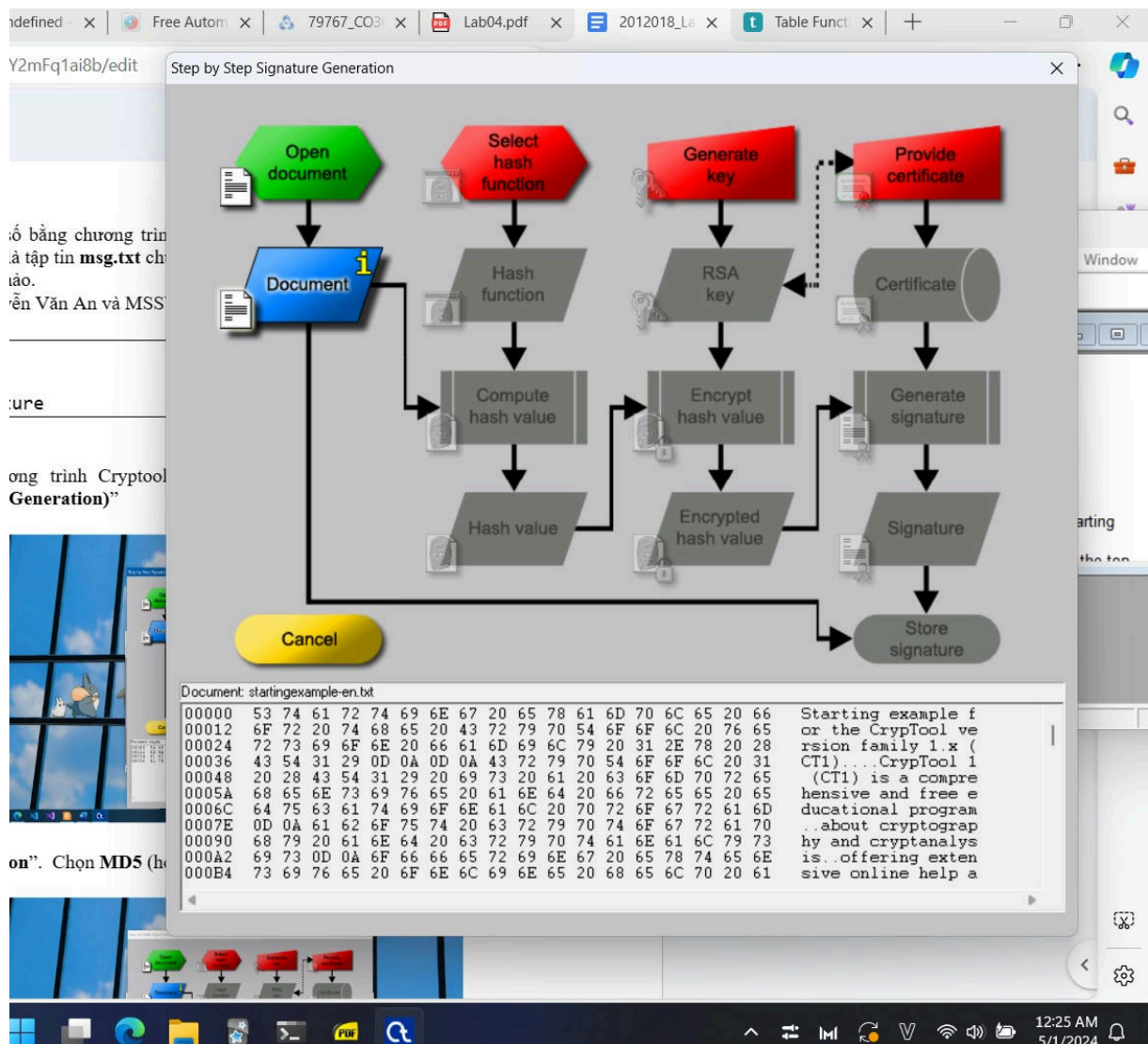
2. Chữ ký số

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 tin đầy đủ và mã số sinh viên. Chụp ảnh màn hình từng bước như phần tham khảo.

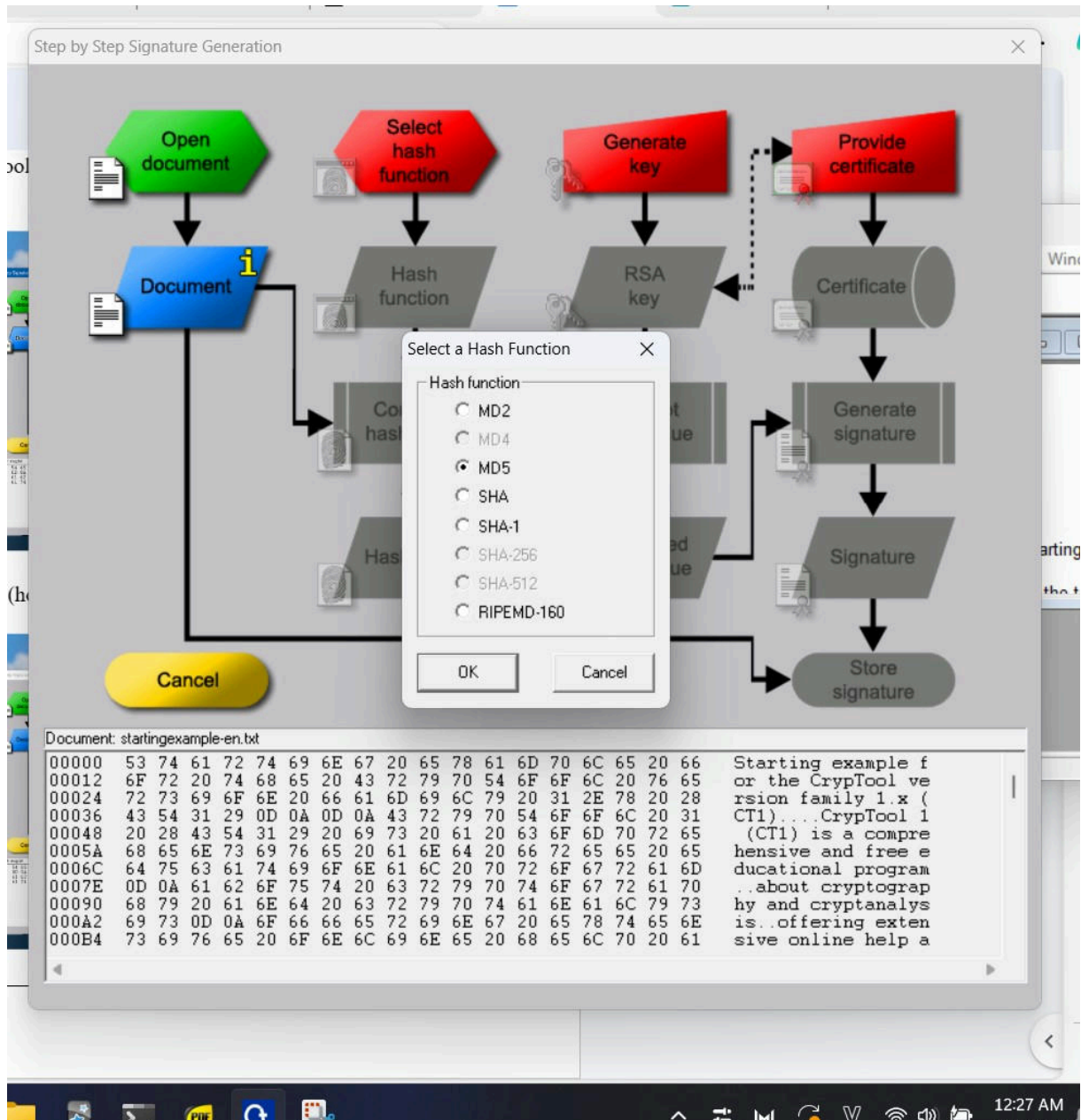
Ví dụ: sinh viên có tên Nguyễn Văn An và MSSV là 123456789, tập tin msg.txt có nội dung như sau:

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

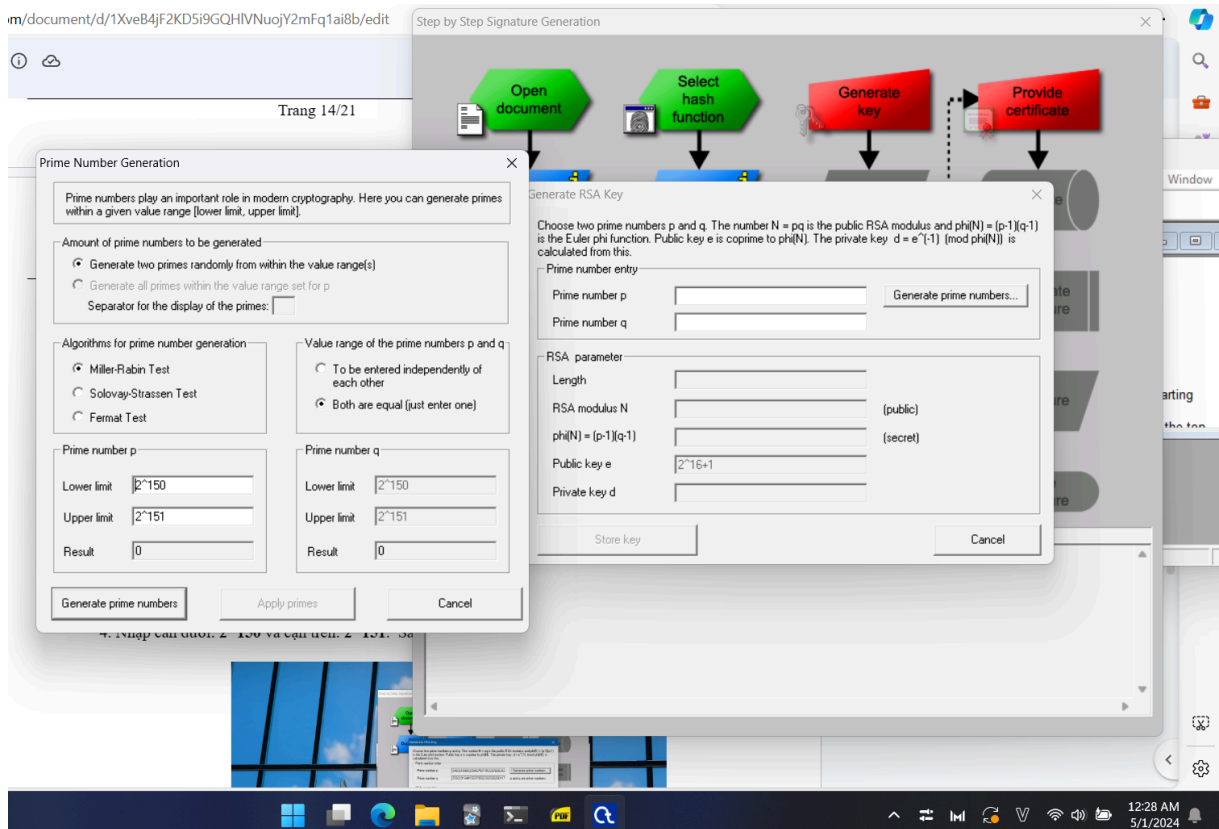
- Bước 1: Từ giao diện của chương trình Cryptool, chọn menu “Digital Signatures/PKI” → “Signature Demonstration (Signature Generation)”



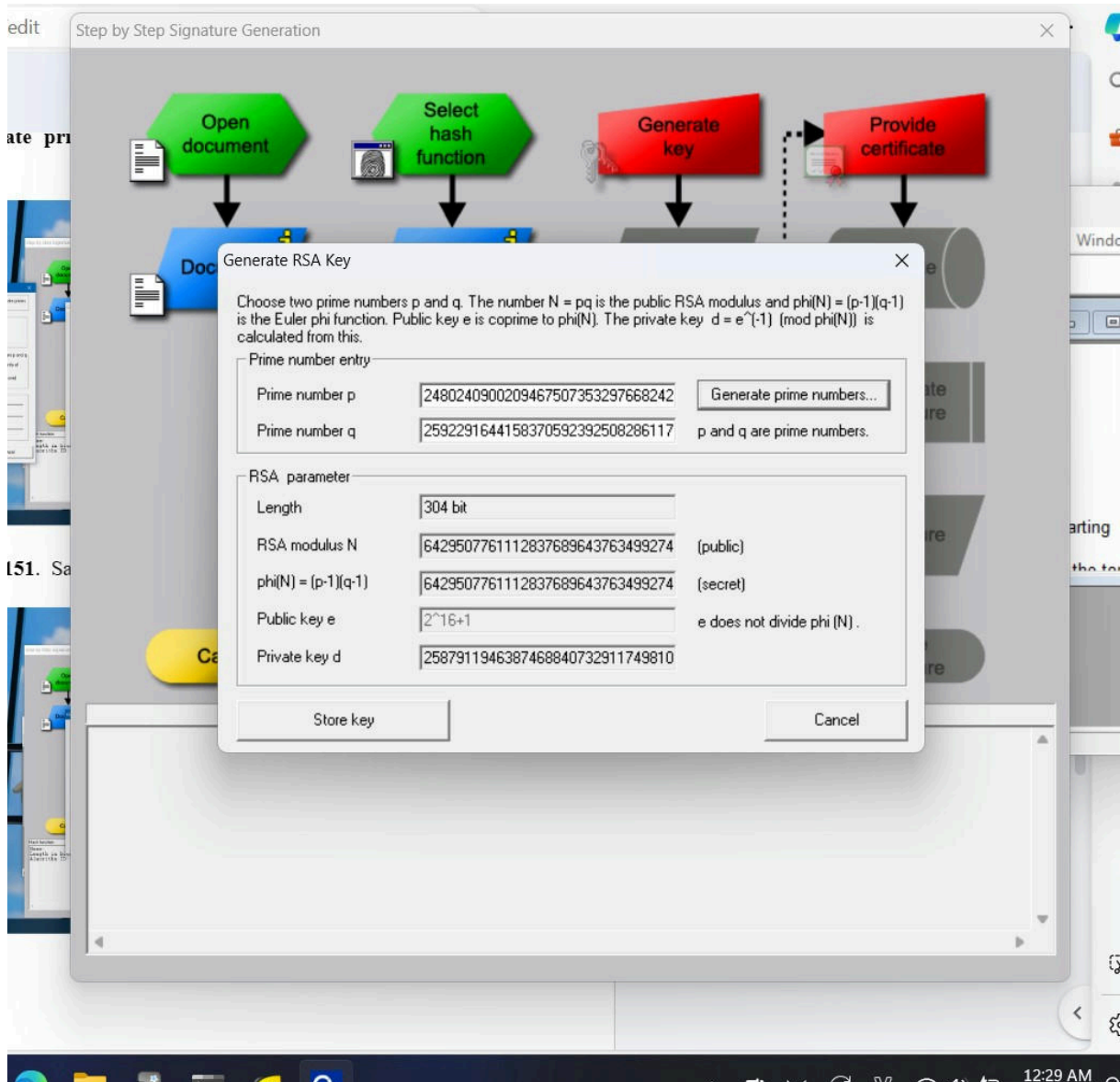
- Bước 2: Chọn “Select hash function”. Chọn MD5 (hoặc một giải thuật hash khác) và nhấn OK.



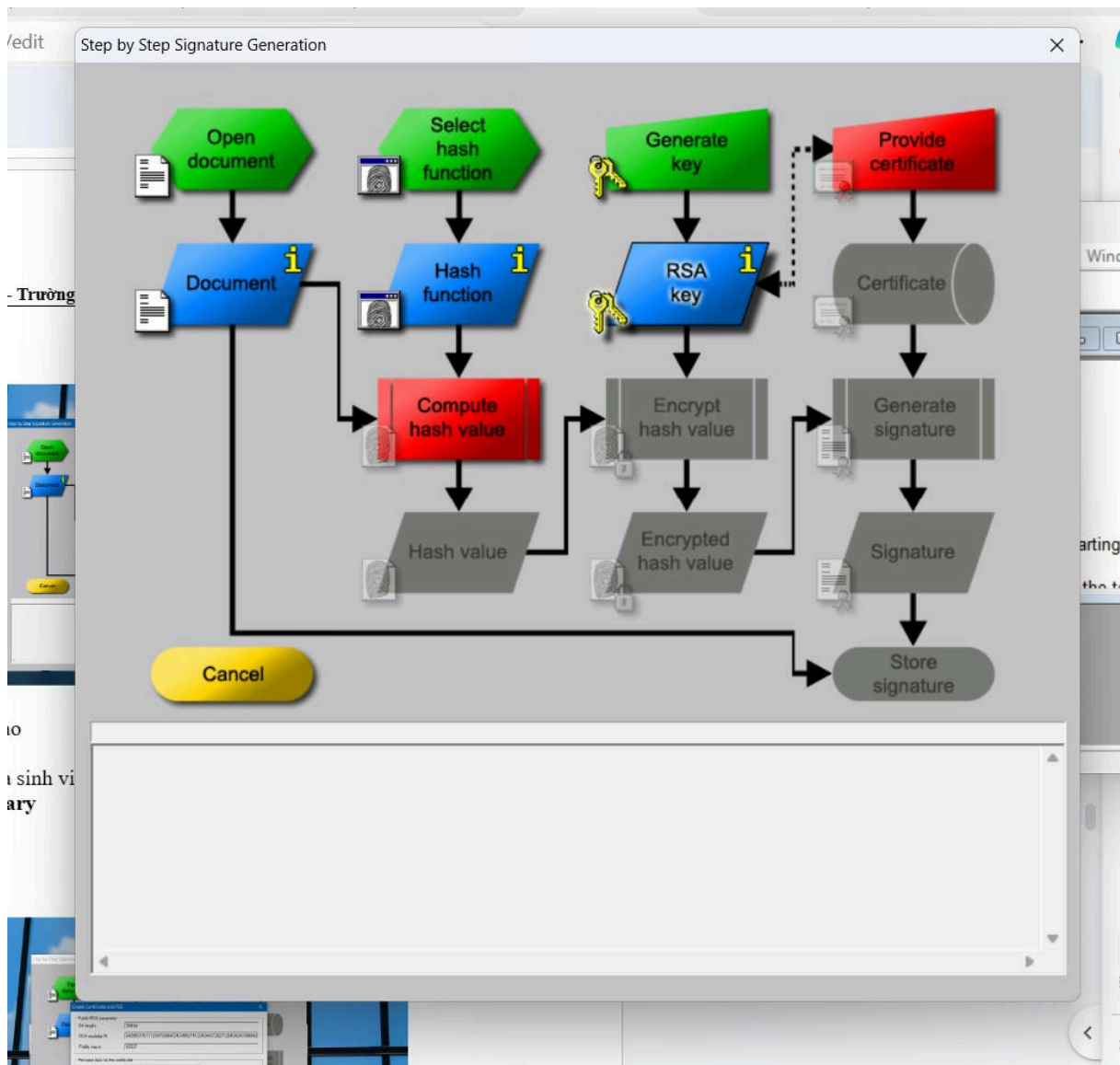
- Chọn “Generate Key” và “Generate prime numbers” trong hộp thoại step by step Signature Generation



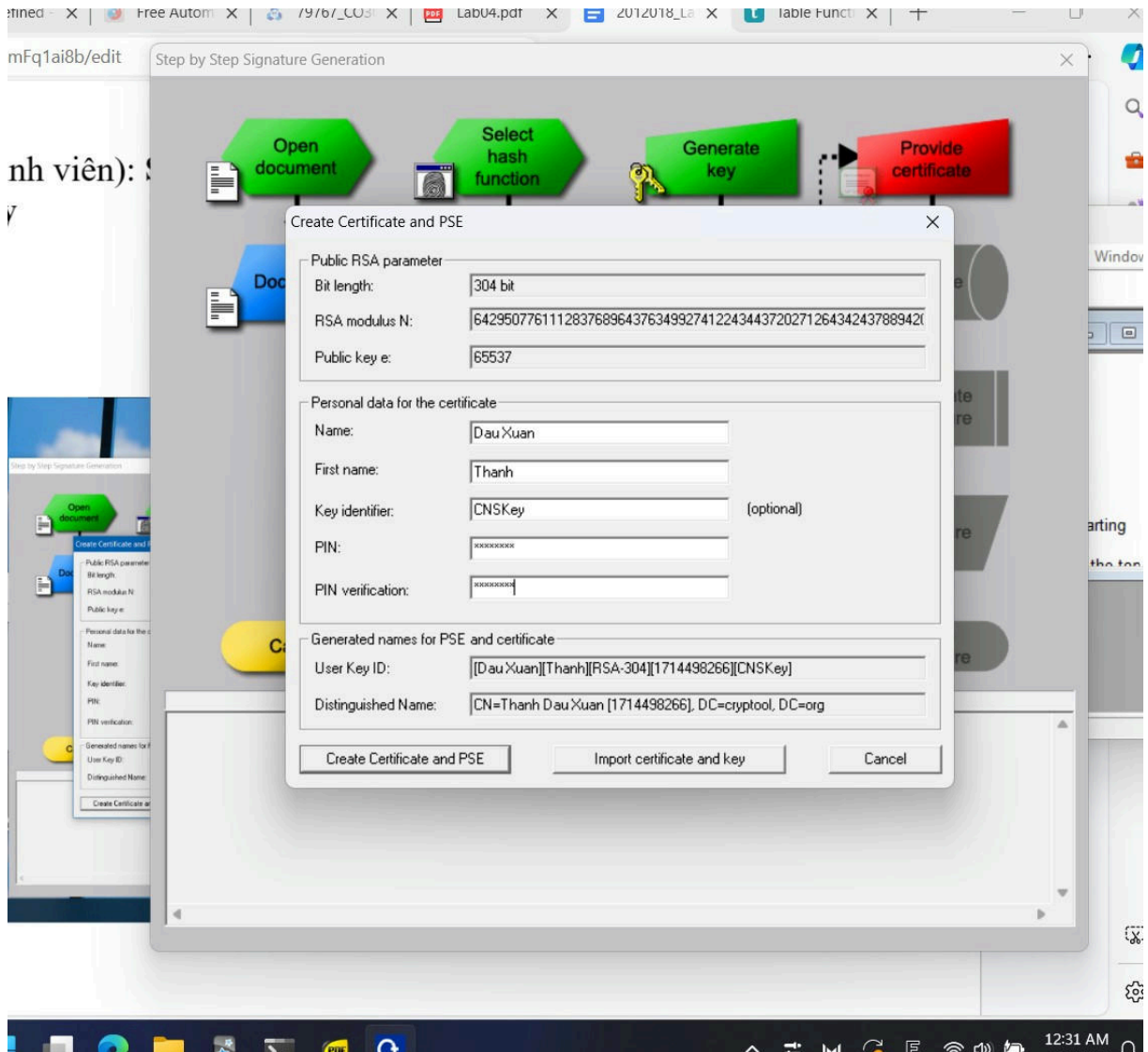
- Nhập cân dưới: 2^{150} và cân trên: 2^{151} . Sau đó nhấn nút Generate prime numbers và apply primes.



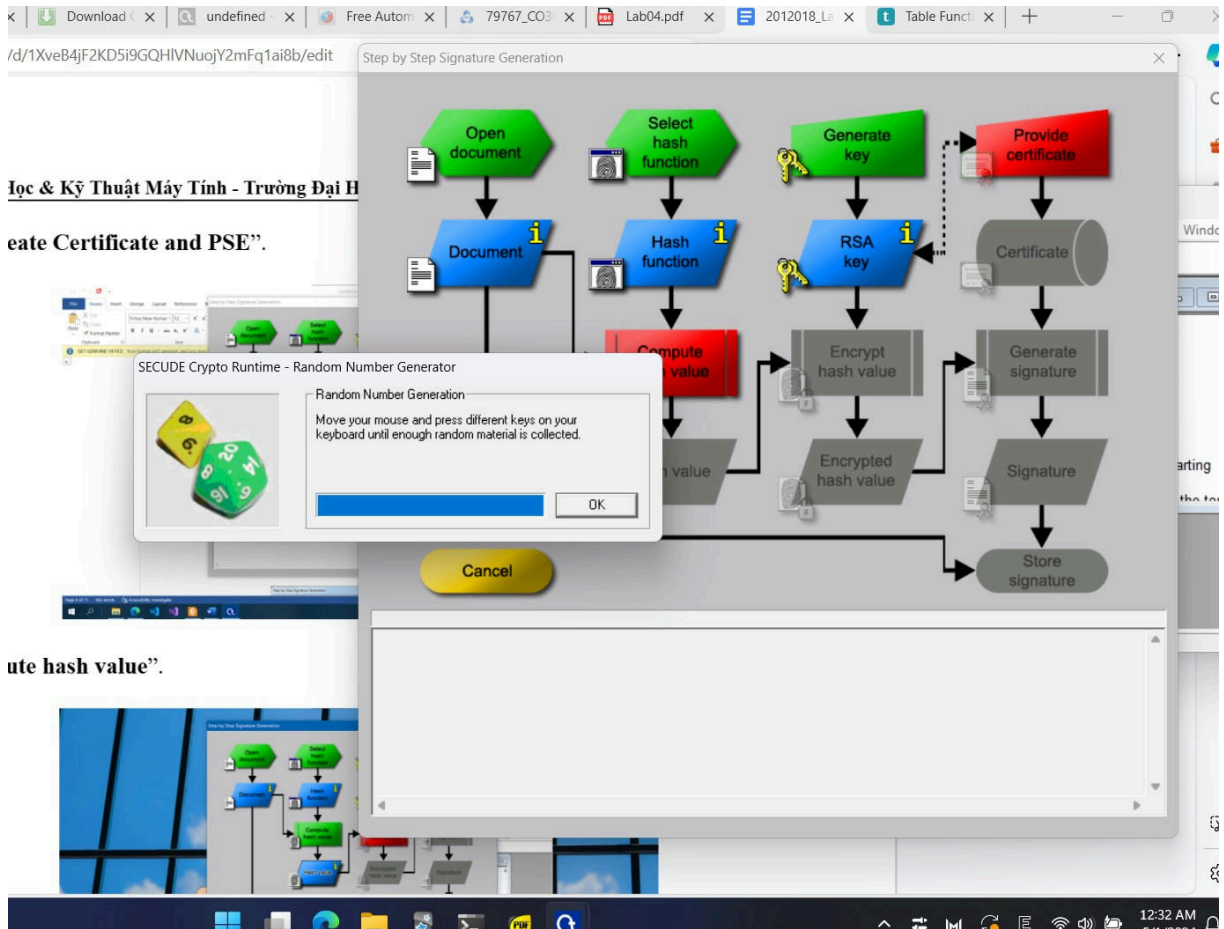
- Nhấn nút Store key



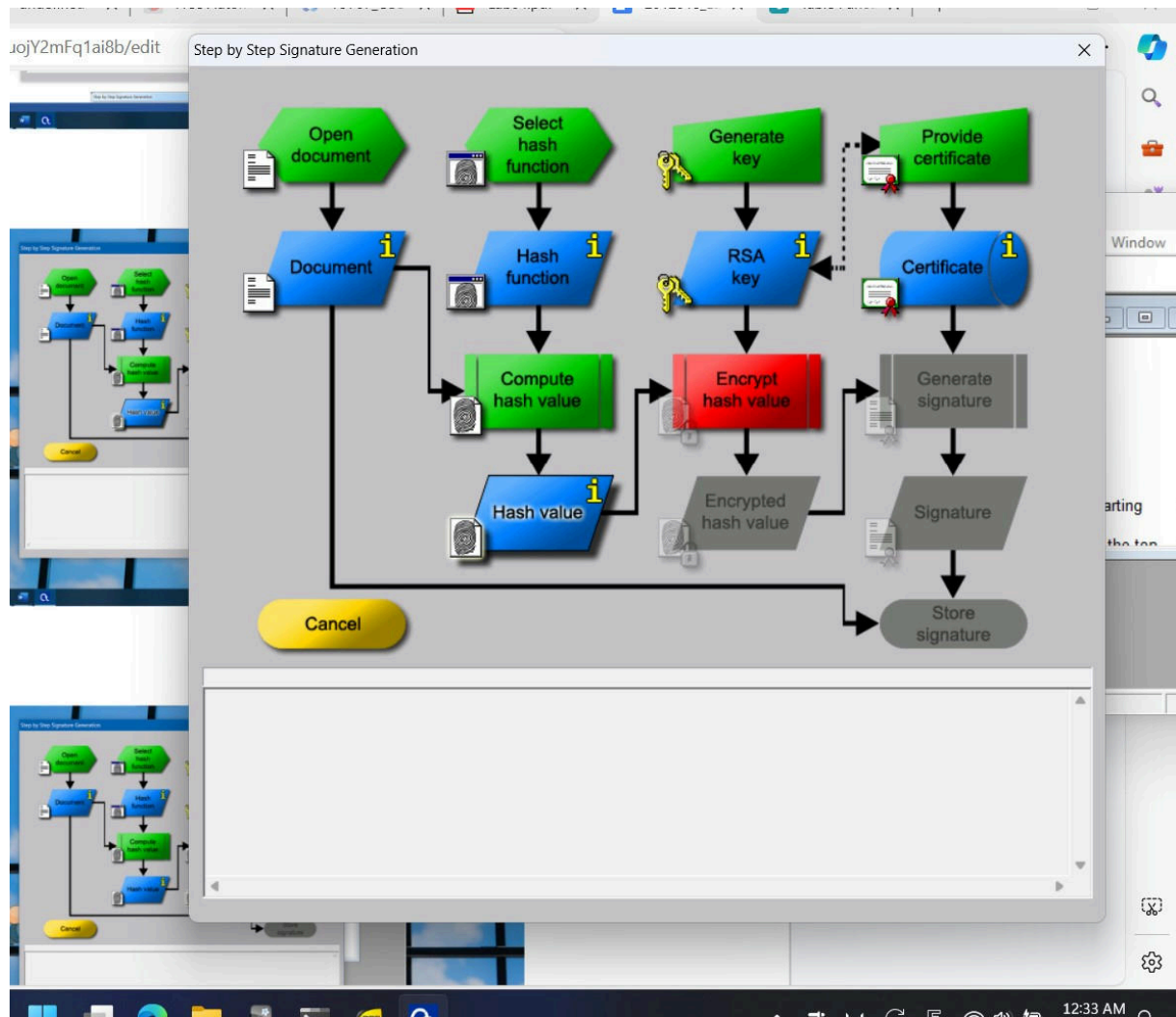
- Nhấn nút Provide certificate, nhập vào
 - Name (nhập thông tin họ và chữ lót của sinh viên): Smith
 - First name (nhập tên của sinh viên): Mary
 - Key identifier (key): Mary key
 - PIN: cryptool
 - PIN verification: cryptool



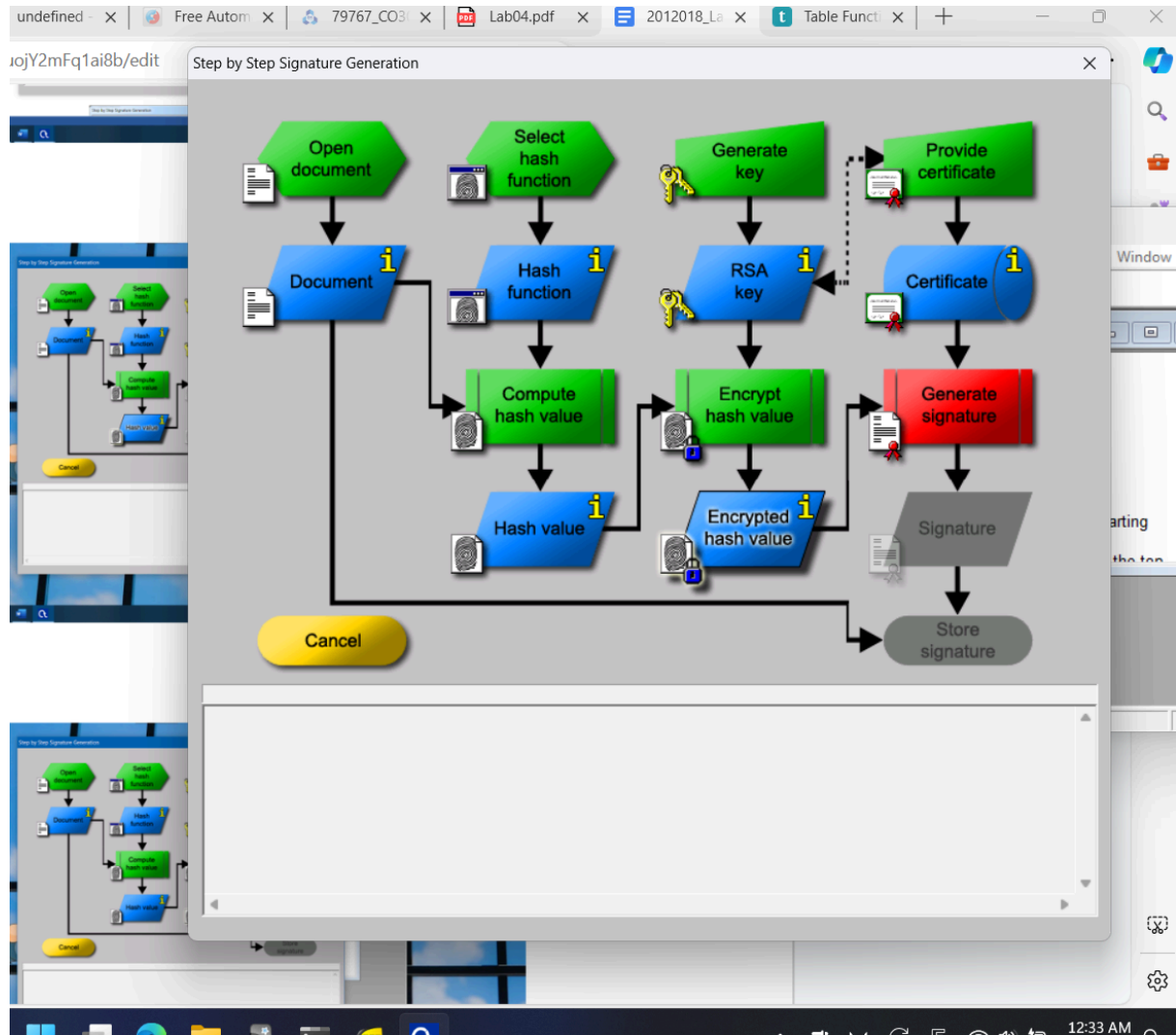
- Nhấn nút “Create Certificate and PSE”.



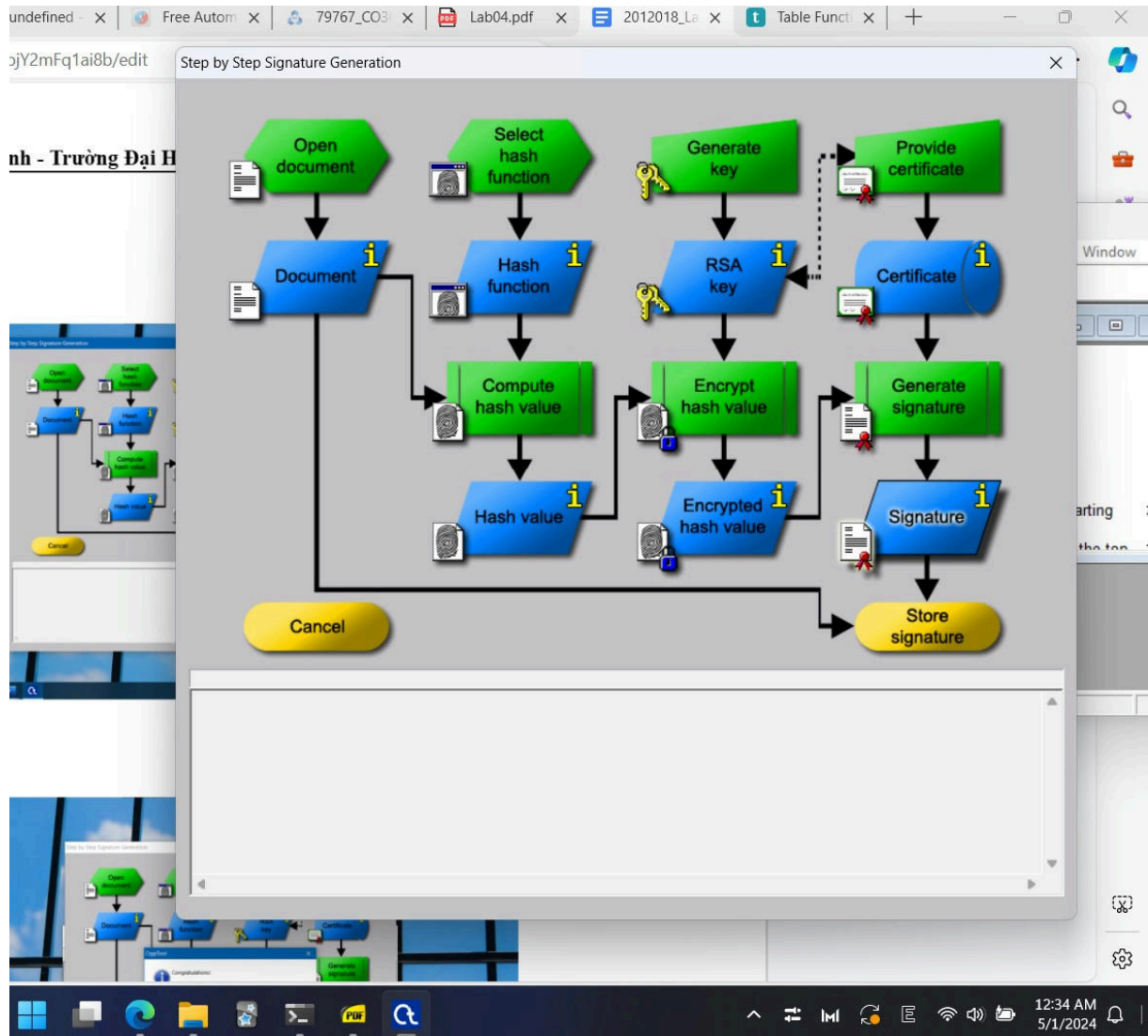
- Chọn “Compute hash value”.



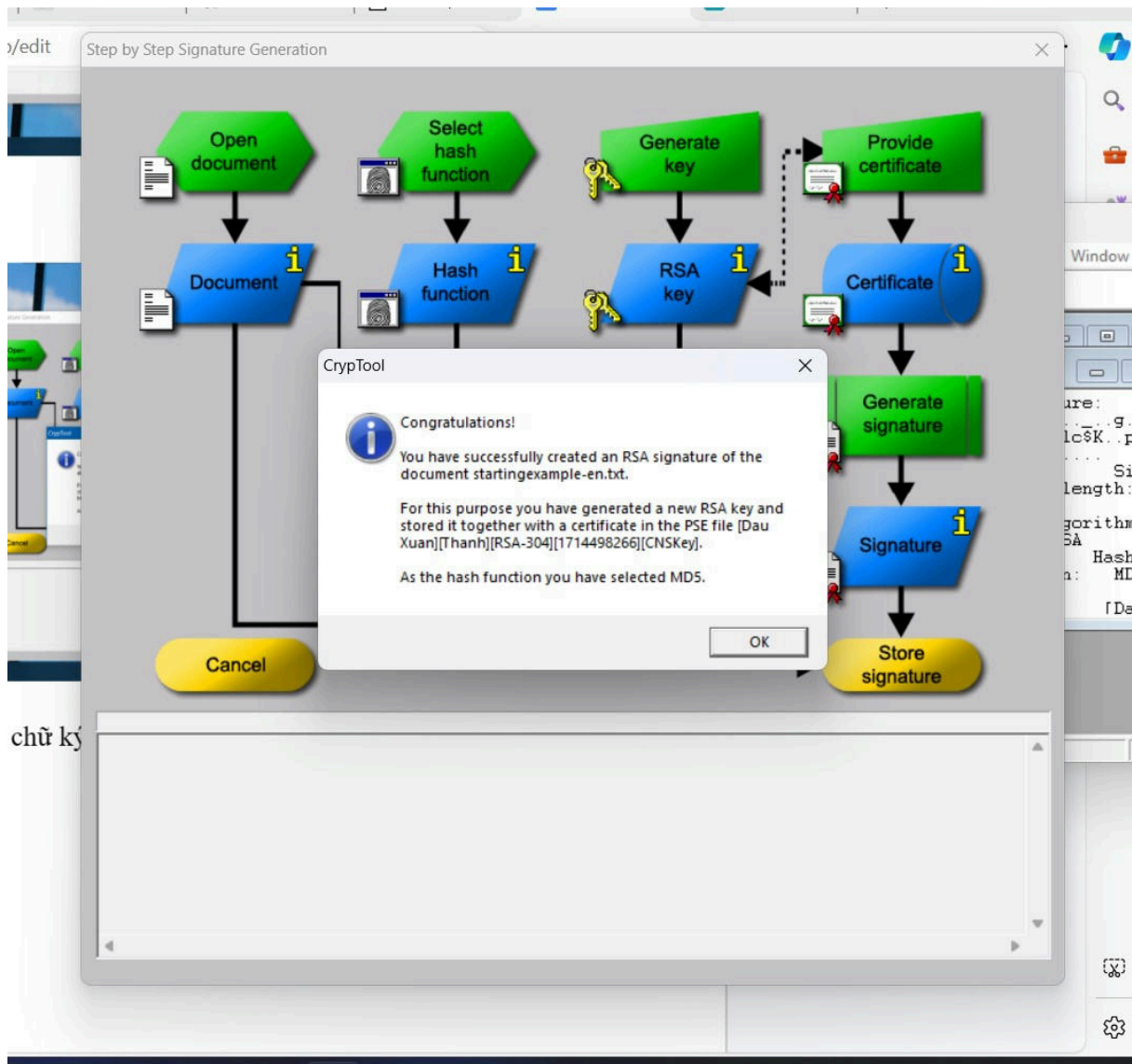
- Chọn “Encrypt hash value”.



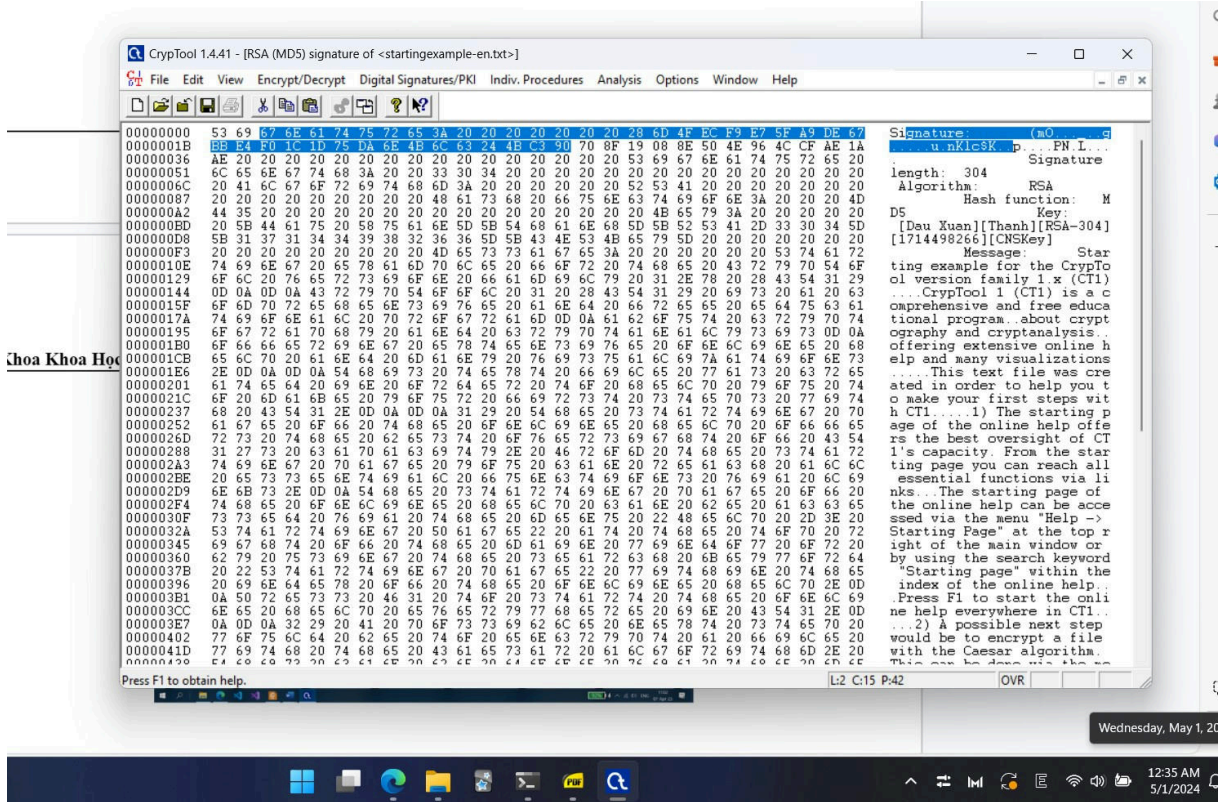
- Chọn “Generate signature”



- 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