BÀI THỰC HÀNH SỐ 4

Môn: MẬT MÃ & AN NINH MẠNG

-o0o-

**Họ tên: Lê Bảo Khánh**

**MSSV: 1911363**

**Phần 1. Mã xác thực thông điệp MAC**

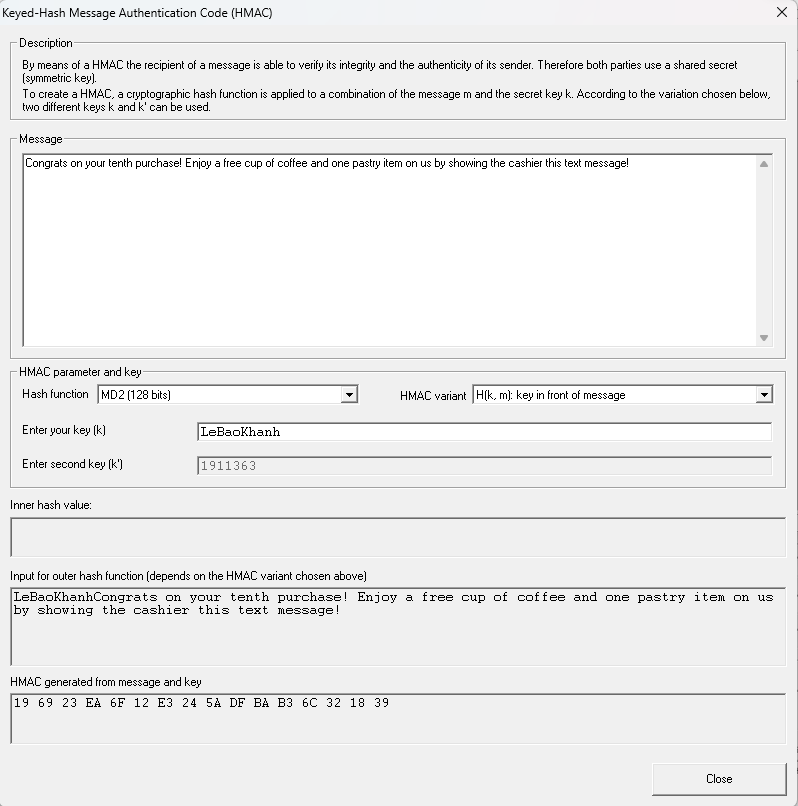
**Câu 1:**

**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!**

**Key k: Lê Bảo Khánh**

**Second Key k’ (nếu có): 1911363**



***Hash function: MD2 (128 bits)***

H(k,m) = 19 69 23 EA 6F 12 E3 24 5A DF BA B3 6C 32 18 39

H(m,k) = 66 E5 5B 6E 2A 6D 7C 47 02 71 A7 72 34 D6 AF 97

H(k,m,k) = A1 8A A0 EE ED 07 8C A6 B2 13 E1 D0 3A E0 C6 43

H(k,m,k’) = 9D 39 AB B1 F6 CE 5B 4A D3 0E 5F 37 87 3B A9 0F

H(k,H(k,m)) = FD C9 55 1E 2D 88 C2 D0 AD E4 D9 F2 3D 11 5E 0C

***Hash function: MD4 (128 bits)***

H(k,m) = 6D 48 13 75 7D 72 33 61 1A 18 00 39 39 AA D5 68

H(m,k) = 2D 8B BB 0E 01 F7 2B 4D 51 0F 44 82 B3 BE 6A 9C

H(k,m,k) = F9 A8 D2 C2 B9 15 F8 74 A1 CF 3D BB A6 50 41 73

H(k,m,k’) = D6 17 81 9C CB 25 89 10 DB 5B 69 1F 7B 34 FE 0E

H(k,H(k,m)) = 0E F0 A5 79 E6 CD 65 61 01 02 45 8E 9B 14 F5 66

***Hash function: MD5 (128 bits)***

H(k,m) = 10 4A F5 D1 C3 BB D1 FB F4 3A F7 17 3D 20 A7 AD

H(m,k) = 09 10 B6 E3 10 84 93 45 16 9D 16 F7 49 B1 9E 32

H(k,m,k) = 0D D0 80 A4 41 96 7A DB 50 EE 09 38 63 52 70 8F

H(k,m,k’) = 03 D4 EF 97 D3 79 13 06 B3 B0 DE 4F EF 06 8D 83

H(k,H(k,m)) = F2 78 75 7C 94 75 3C 6D 16 6A 77 C9 69 0E D2 84

***Hash function: SHA (160 bits)***

H(k,m) = 06 96 E8 2A 50 CF D2 E6 F7 23 A6 2A DD 17 A2 C0 4E 5D A6 04

H(m,k) = 1C 3E 2E D6 C0 01 9E E3 1E 88 29 B4 C1 35 E6 43 41 78 E5 31

H(k,m,k) = BE 5C 81 33 4E 17 15 2C 65 E9 22 FC CD E3 A3 E6 F1 99 A4 5F

H(k,m,k’) = 63 AA 4C 78 EC 6D 3F F7 26 9E AB E2 D0 1B ED E7 37 46 D1 D5

H(k,H(k,m)) = 20 43 CF 1B 1D 17 CA 45 4B 5C C2 C2 51 31 A5 77 20 54 17 5A

***Hash function: SHA-1 (160 bits)***

H(k,m) = 79 A5 B7 07 B9 9C 46 B3 9C 86 29 64 FB FD 61 BA C2 15 12 5C

H(m,k) = 68 A6 D1 4C 93 E3 0A 4A B3 77 A1 BB FB A2 7B A7 36 D4 17 22

H(k,m,k) = 5B A8 17 AF 41 0F 46 84 04 E1 E7 51 59 33 C2 05 A3 22 A1 C5

H(k,m,k’) = 39 AC B7 3D 3F 18 09 56 72 7F EB AF 06 92 D4 F8 2D 6B 22 11

H(k,H(k,m)) = 30 C3 A7 CC 1F 18 AB 67 61 E9 8D 28 50 B0 E7 06 EE 4C C9 F9

***Hash function: SHA-256 (160 bits)***

H(k,m) = 1A E6 1D 37 56 50 7D 1A 0F 19 23 27 59 2C E3 BC F4 EC 08 36 02 B3 BD B0 4C 99 94 F7 95 10 AB AE

H(m,k) = 3E 10 63 F2 86 F3 08 2A A9 BD 1F DF 53 5A 91 21 06 4B A9 17 69 E0 D5 5F 21 D8 E8 21 64 DD 25 D9

H(k,m,k) = A6 6C 9E 31 AD DE 45 02 1F 3A C6 DC 22 57 77 8C C7 3B C9 E5 BB DF 56 7A F0 29 CE 9D 88 D0 4E 04

H(k,m,k’) = 8B 64 B7 EC 98 5B 10 A0 FF C6 29 B9 3E 51 62 4D C0 A1 C2 71 84 68 3C 67 78 0E EE 91 E0 8E 0E F4

H(k,H(k,m)) = 38 34 FD CE C4 4D 76 FC 13 78 87 FD 77 AF FE 0B 70 AB DD 04 36 B8 1F 80 5B 45 EC 06 8D 95 74 44

***Hash function: SHA-512 (256 bits)***

H(k,m) = DD 4A BF C5 A5 51 4C 60 C6 27 C6 2E 6E 3A 25 A5 EB C6 15 53 4E 09 BC 38 05 05 EF B1 CF F2 49 8A D5 67 EE 56 8F 19 C4 45 57 9F 3B AD 44 3A 30 B7 F7 05 6D 00 ED F2 3D 42 20 1D 4A 41 33 A6 3E 7B

H(m,k) = 65 1D 5F AA CC 58 98 B0 85 31 9B A7 E7 DC ED 8F FE ED DD AC 5B 10 38 E0 B6 ED E6 93 89 6D 39 DC 92 A3 2E 52 81 2F 42 99 40 84 FB D6 3E 74 F5 2E 65 B9 40 01 E5 91 7C F3 D6 11 18 E3 D2 AD 92 E9

H(k,m,k) = 9E 9A DD D8 83 AF 5E 82 A7 AF 16 D7 98 78 9A 8C 35 5E DB C6 D2 9A 26 8D F2 41 09 93 F9 3C 08 8E BA 54 A1 C9 0B C0 03 DE 22 9B 7F AA B0 9C 79 2A ED 3C 1C 72 34 B4 71 A5 A4 6E 68 0A 1E D7 2C 0A

H(k,m,k’) = 4A C6 35 40 DF 99 88 24 BD 7F D4 6A 93 98 6B E6 69 23 33 8E 3D 04 BB 4A 3F 98 7A FD D8 0D 89 87 CE B5 94 80 22 C3 A4 71 0E E3 41 DD 06 FF 49 29 04 58 8F EA 90 76 3E 69 1B B1 EB A5 C3 EA 64 42

H(k,H(k,m)) = 69 BF 01 CE 4F 2C 16 54 49 76 CC 43 C9 F5 C2 81 47 30 D6 44 86 80 50 11 84 B4 83 32 83 EA C2 1F 8B 23 97 2D 88 17 E9 2C 09 B2 3A 4F 2F 66 42 72 2C C2 77 CF 16 EB 62 A0 C5 8D 28 CA 77 17 17 55

***Hash function: RIPEMD-160 (160 bits)***

H(k,m) = 74 18 FB 05 A4 C6 47 C0 3C FD 2F 2C 9D 3A DD 84 22 8C E4 B1

H(m,k) = 92 AE E7 CF A2 BA 86 F7 0E E1 0D 31 21 A5 17 88 1C 3B 2B 66

H(k,m,k) = 7C 3A 0E BE D1 BA 03 E7 86 C6 11 B0 B1 1E A4 EA FF DE DA 62

H(k,m,k’) = E7 F8 3B 5A E2 D8 75 F1 AE 4C AE BD 29 A6 DB B7 A6 EE 10 EA

H(k,H(k,m)) = 4B FA A2 26 3B 61 05 01 99 7A 1D D6 91 0F D7 4D D9 70 91 E6

**Câu 2:**

***Tấn công ngày sinh nhật:***

* Kẻ tấn công tạo 2m/2 phiên bản của một thông điệp hợp lệ với cùng một nghĩa như nhau.
* Kẽ tấn công cũng tạo ra 2m/2 phiên bản thông điệp giả mạo.
* Hai tập thông điệp này được so sánh để tìm ra một cặp cùng giá trị băm(xác xuất là > 0.5).
* Người dùng ký trên văn bản hợp lệ thì chữ ký cũng hợp lệ trên văn bản giả mạo.

***Tấn công brute-force:***

* Có đề xuất phần cứng để bẻ gãy MD5
* Giá trị băm 128 bits dễ bị tổn thương vì vậy nên dùng giá trị băm 160 bits thì tốt hơn.
* MAC với các cặp (thông điệp, MAC) được biết:

+ Có thể tấn công tìm kiếm khóa hay MAC

+ MAC phải có chiều dài ít nhất 128 bits mới an toàn

***Tấn công phân tích mã khai thác cấu trúc:***

Có một số tấn công phân tích mã trên hàm băm lặp:

* CVi = f[CVi-1, Mi]; H(M)=CVN
* Như mã hóa khối cũng có các vòng
* Tập trung vào các đụng độ trong hàm f
* Khai thác các thuộc tính của hàm f

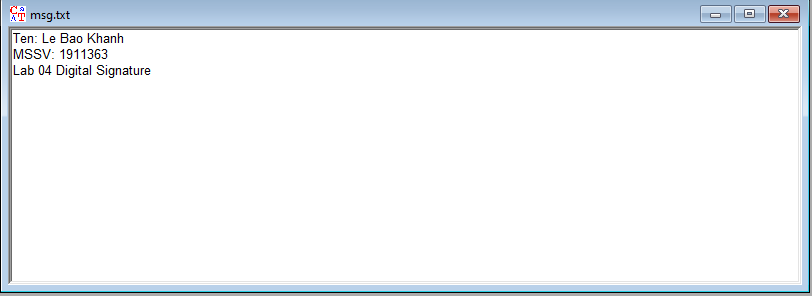
**Câu 3:**

|  |  |  |
| --- | --- | --- |
| Yếu tố | Mã xác thực thông điệp (MAC) | Hàm băm  (HASH) |
| Cách tạo | MAC = CK (M) | h = H(M) |
| Mục đích | Được sử dụng để đảm bảo tính xác thực và toàn vẹn. | Được sử dụng để đảm bảo tính toàn vẹn. |
| Khóa K | Có sử dụng | Không sử dụng |

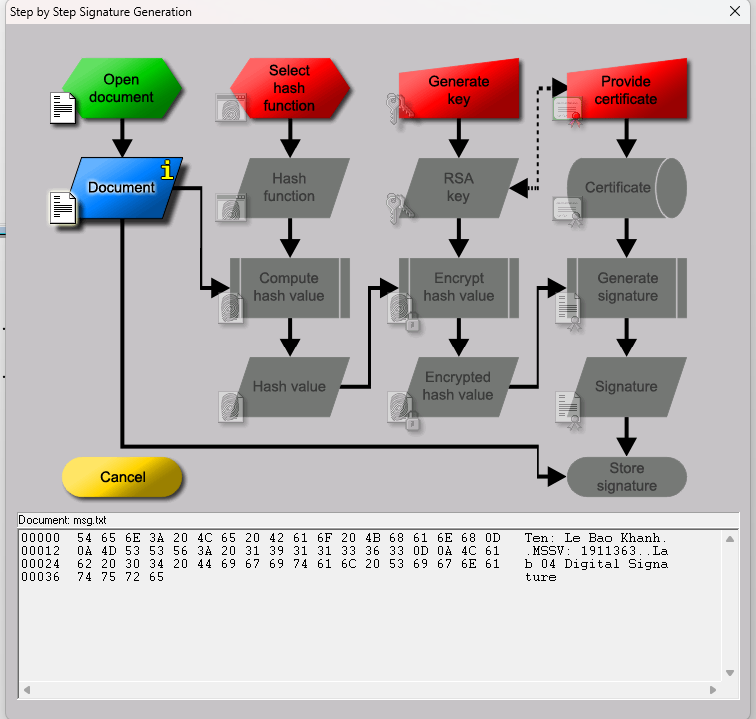
**Phần 2. Chữ ký số**

**Câu 1:**

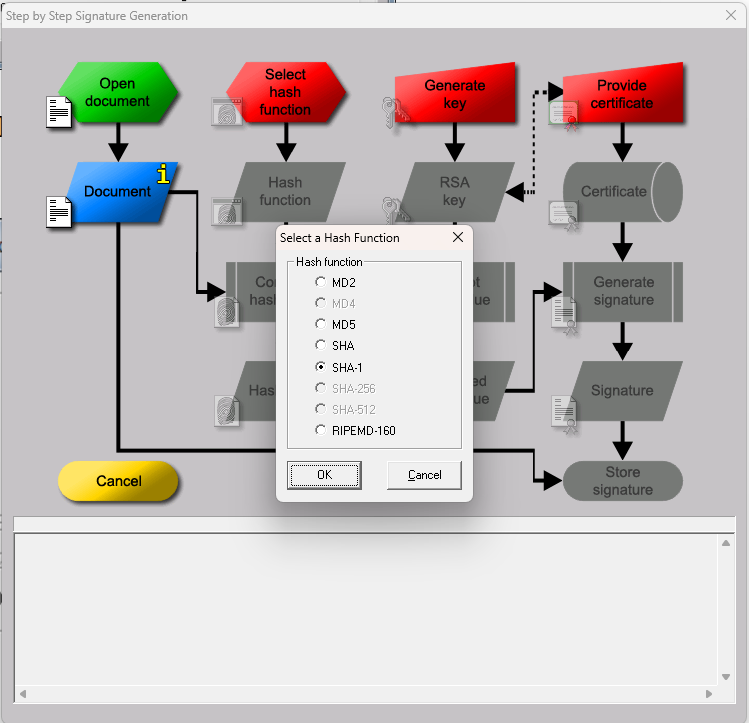
Message:

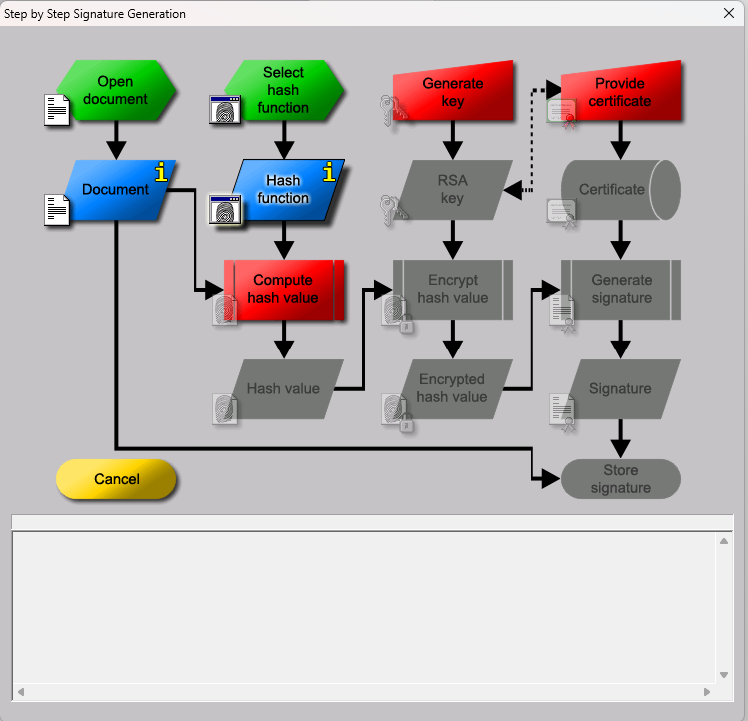


1. **“**Digital Signatures/PKI” -> “Signature Demonstration (Signature Generation)

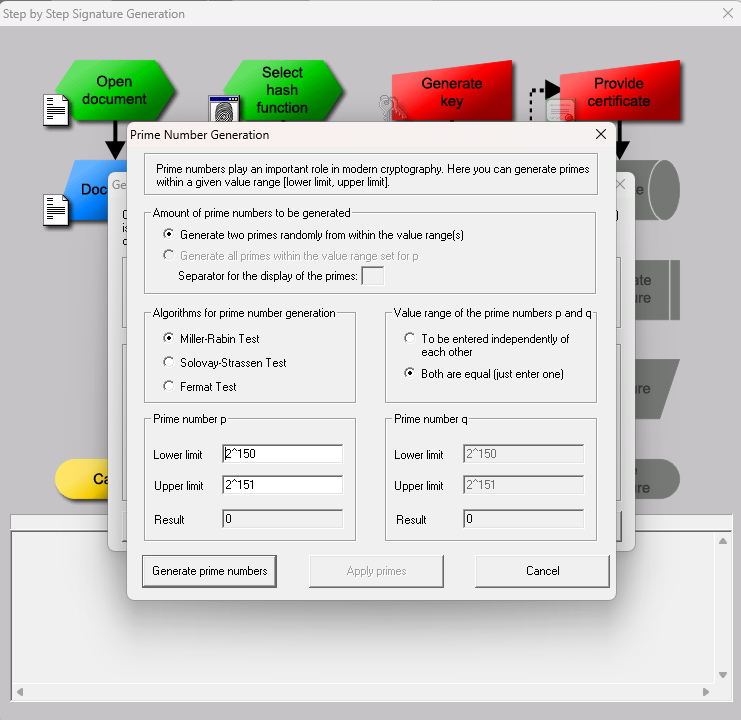


2**. “**Select hash function**”**

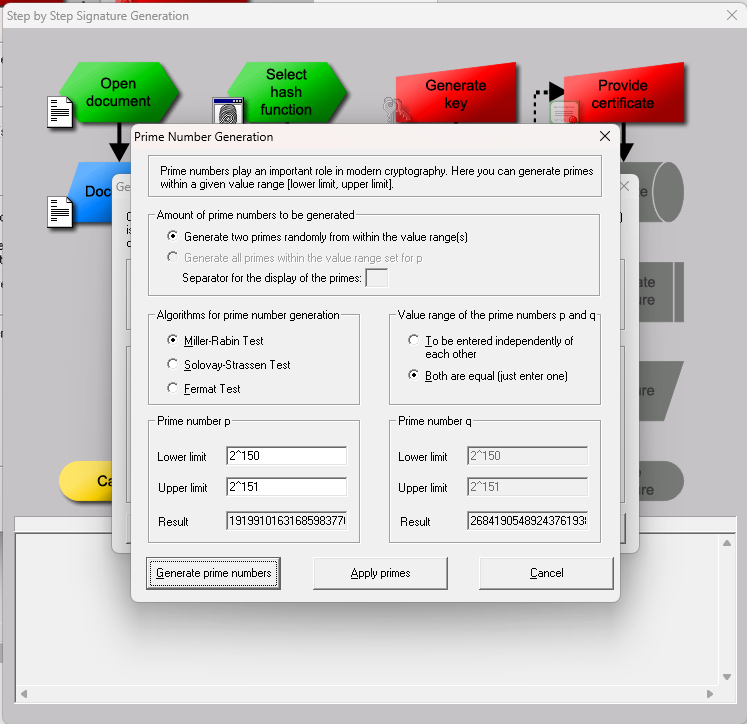
****

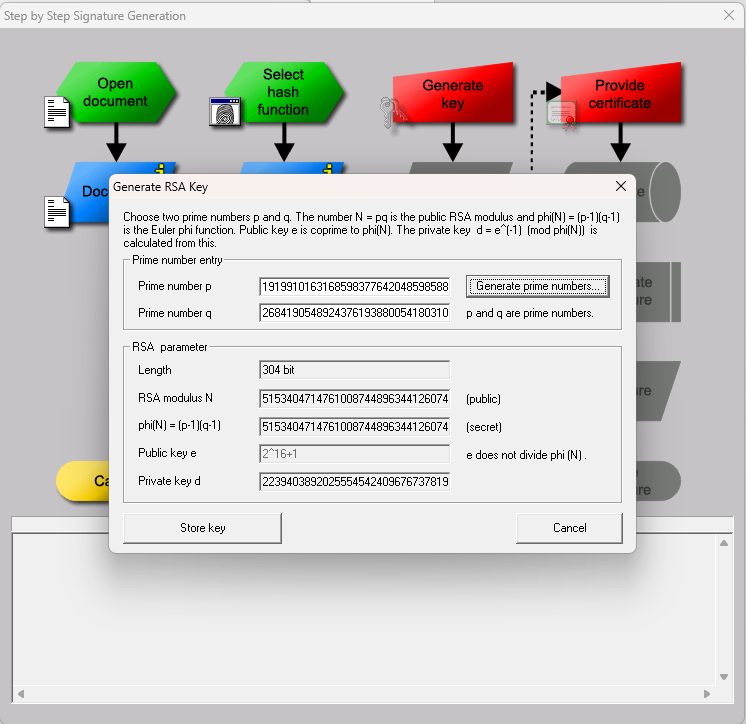
****

3**. “**Generate Key**” -> “**Generate prime numbers**”**

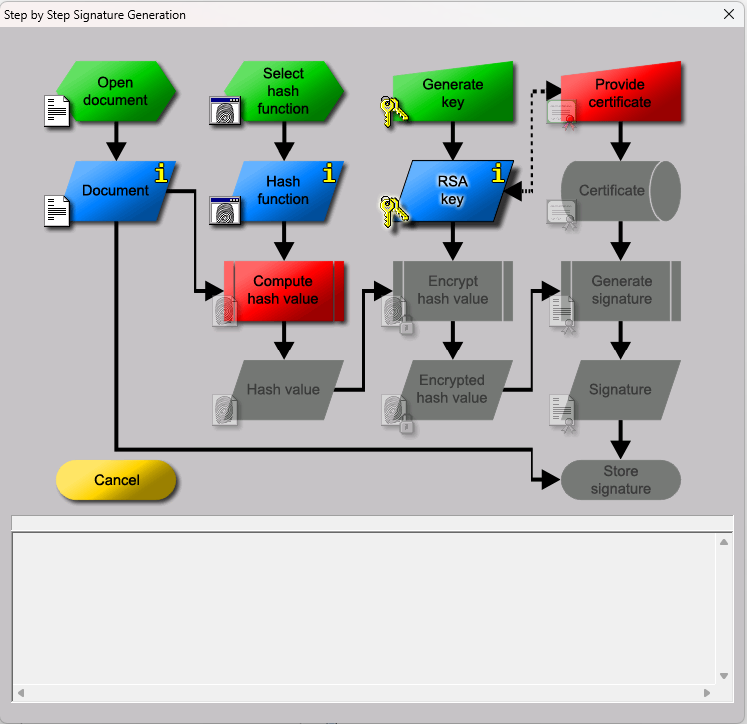
****

4. “Generate prime numbers” và “apply primes”

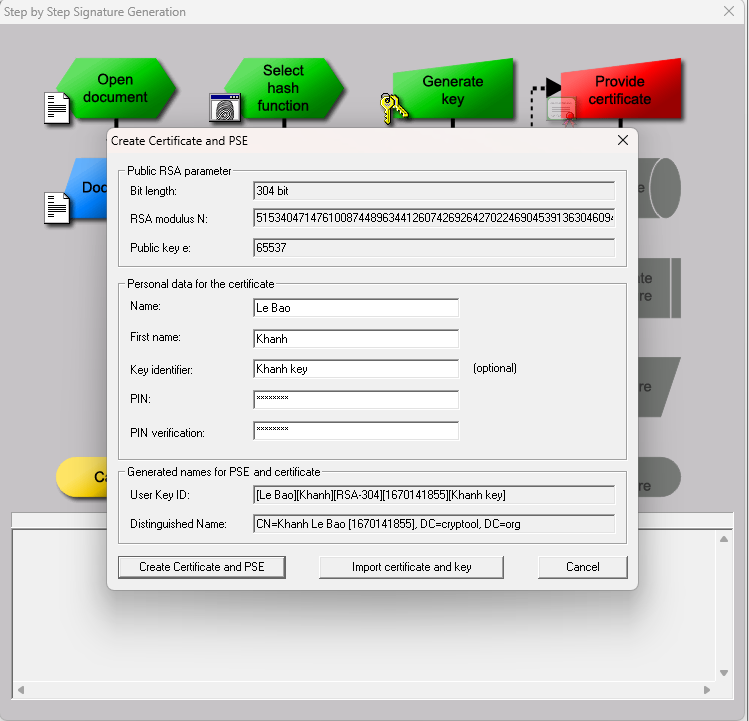




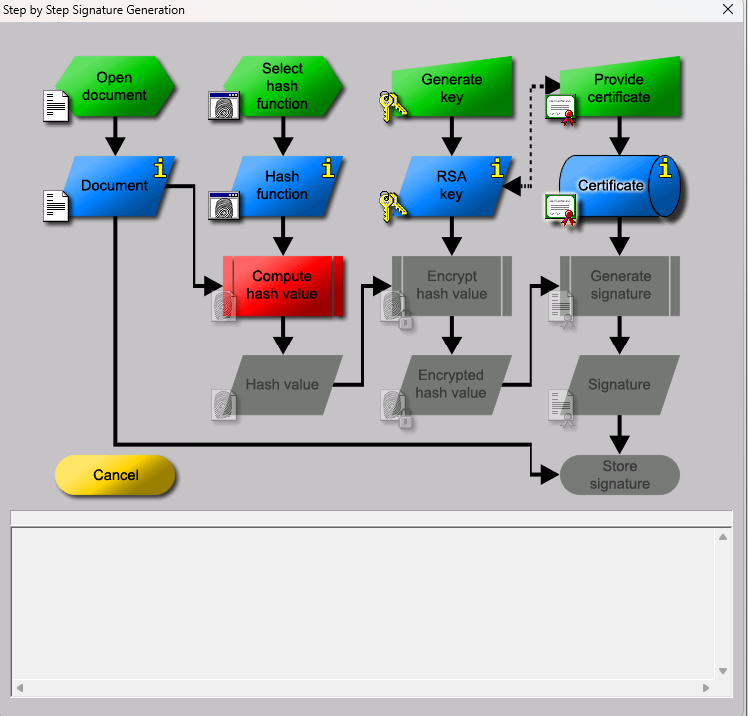
5. “Store key”



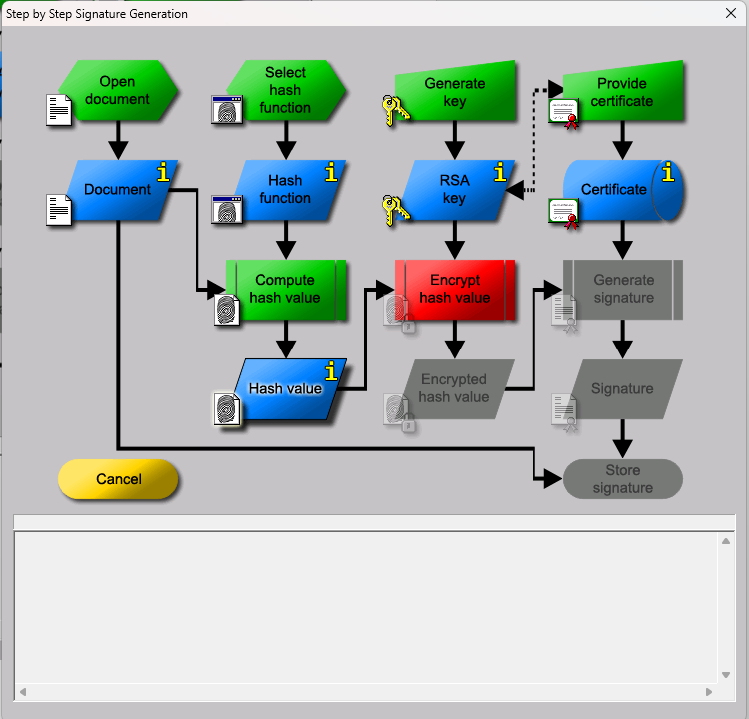
6. “Provide certificate”



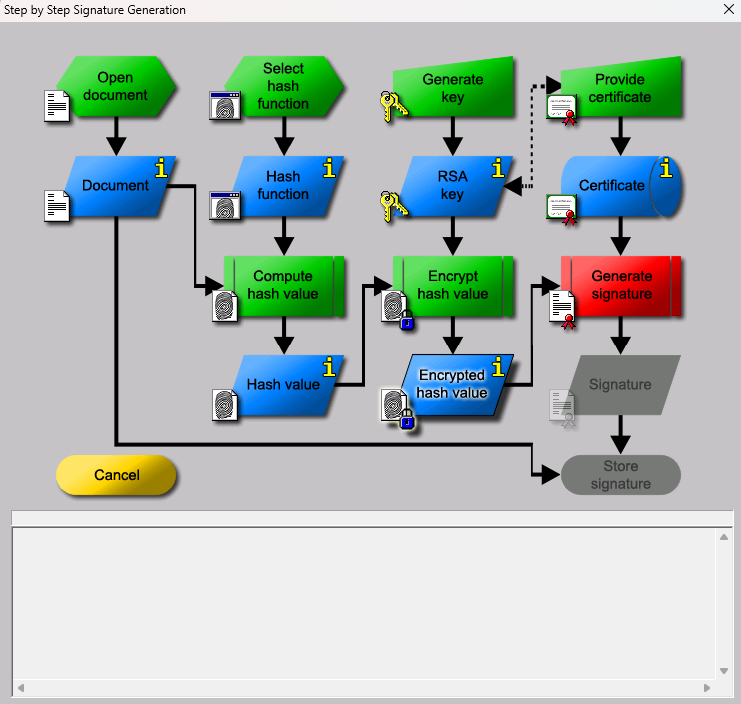
7**. “**Create Certificate and PSE**”**

****

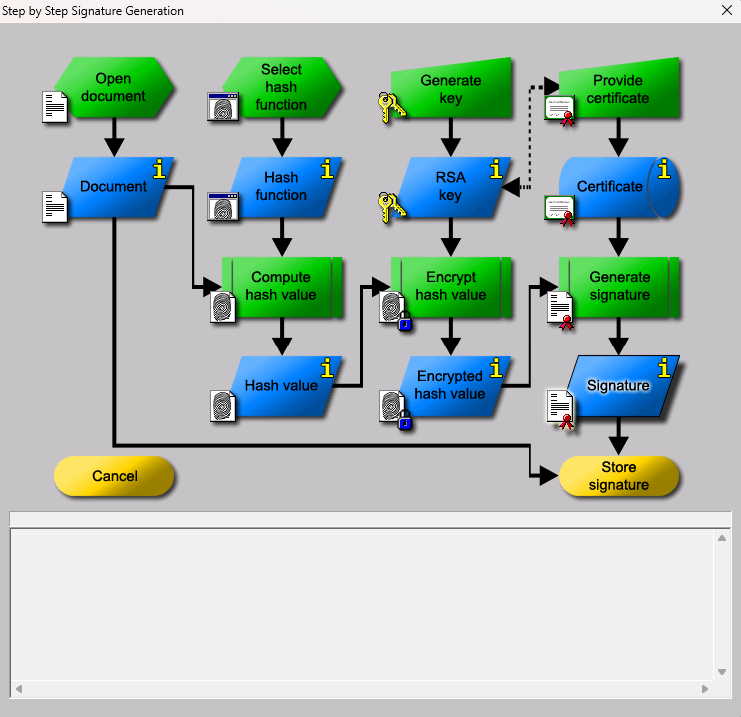
8**. “**Compute hash value**”**

****

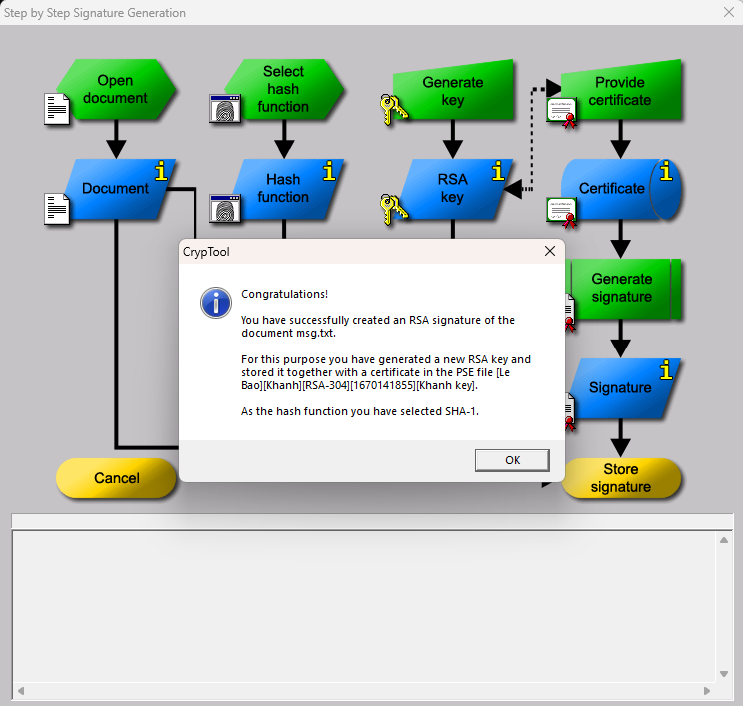
9**. “**Encrypt hash value**”**

****

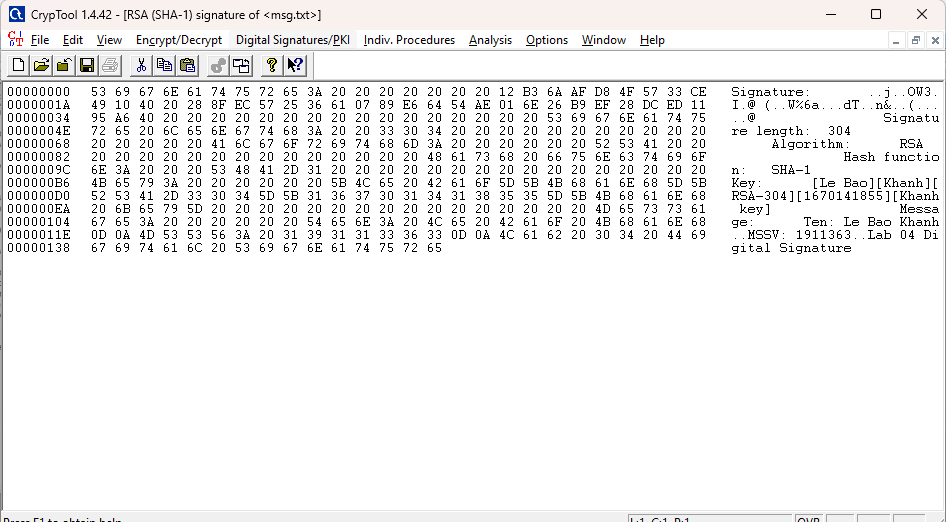
10**. “**Generate signature**”**

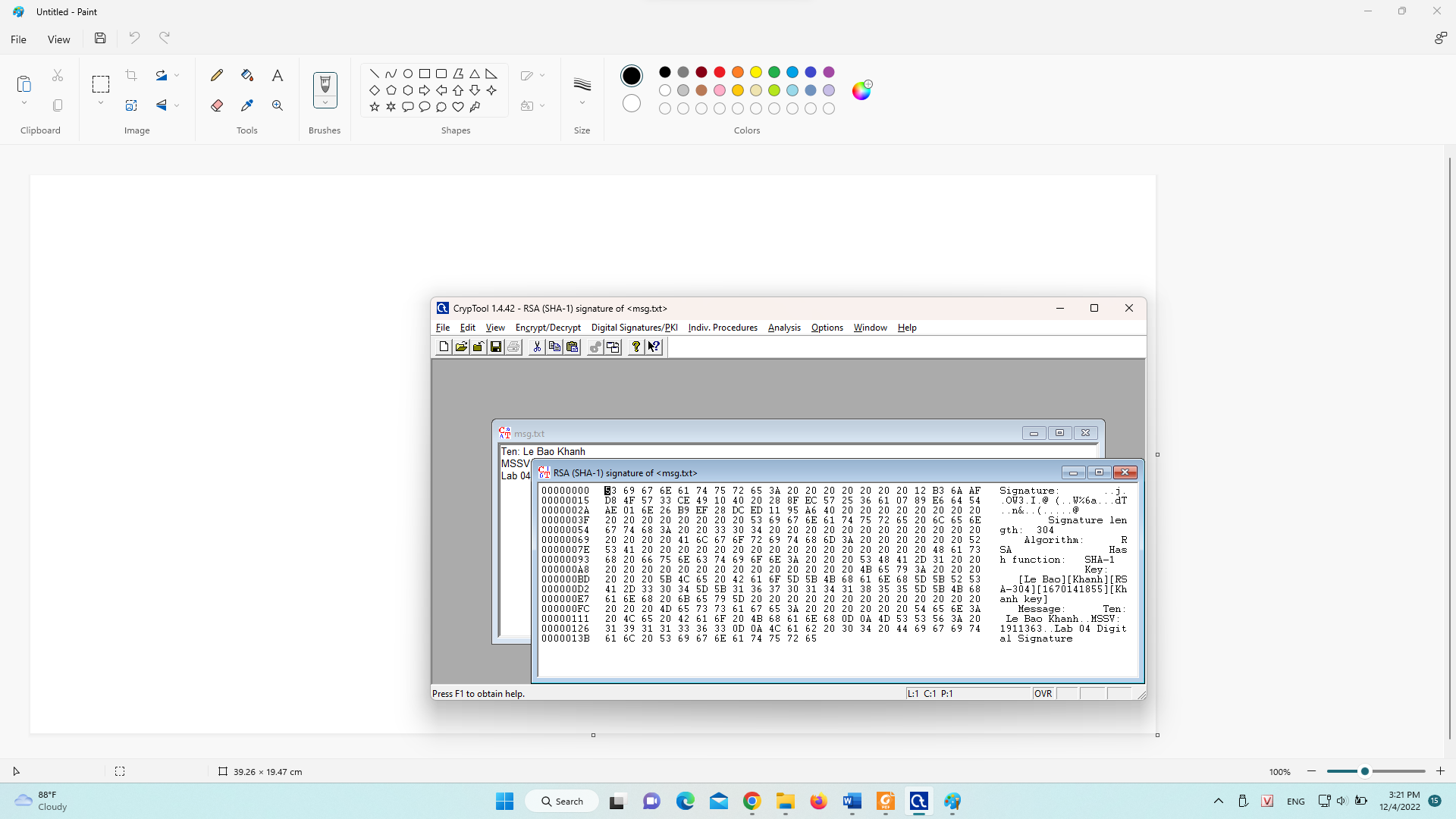
****

11. **“**Store signature**”**



12. “OK”, ta thu được thông điệp và chữ ký số như bên dưới





**Câu 2:**

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

* Có thể lưu trữ chữ ký số trong thực tế

**Câu 3:**

Mã xác thực thông điệp (MAC) chỉ bảo vệ bên gửi và bên nhận khỏi bên thứ ba (third-party), nhưng lại không thể bảo vệ họ khỏi bên còn lại.

Ví dụ: Khi John gửi thông điệp cho Marry

* **Mary có thể thoái thác đã nhận thông điệp** bằng cách làm một thông điệp giả và tuyên bố rằng nó được gửi tới từ John. Mary đơn giản chỉ cần tạo 1 thông điệp và chèn thêm MAC sử dụng key mà Mary và John chia sẻ
* **John có thể thoái thác đã gửi thông điệp** vì Mary có khả năng đã làm giả thông điệp, nên không có cách nào chứng minh John thực sự đã gửi thông điệp đó

Chữ ký số là một cơ chế xác thực nhằm xác nhận danh tính của người tạo ra thông điệp và chống thoái thác về xuất xứ (giải quyết tranh chấp). Chữ ký số được tính toán trên giá trị băm của thông điệp và mã hóa bằng khóa riêng của người gửi.

Chữ ký số cung cấp khả năng:

* Xác minh tác giả, ngày giờ đã ký
* Toàn vẹn thông điệp
* Được xác minh bởi một tổ chức thứ 3 để giải quyết tranh chấp