BÀI THỰC HÀNH SỐ ????

Môn: MẬT MÃ & AN NINH MẠNG

-o0o-

**Họ tên: Lương Hữu Phú Lợi**

**MSSV: 1911545**

**Nhóm: L02**

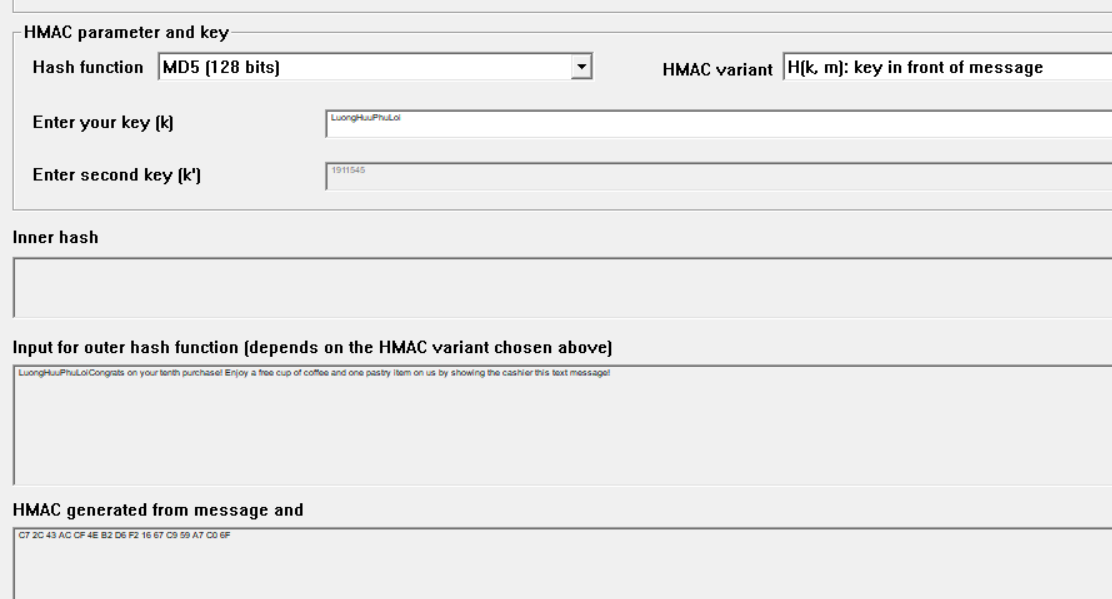
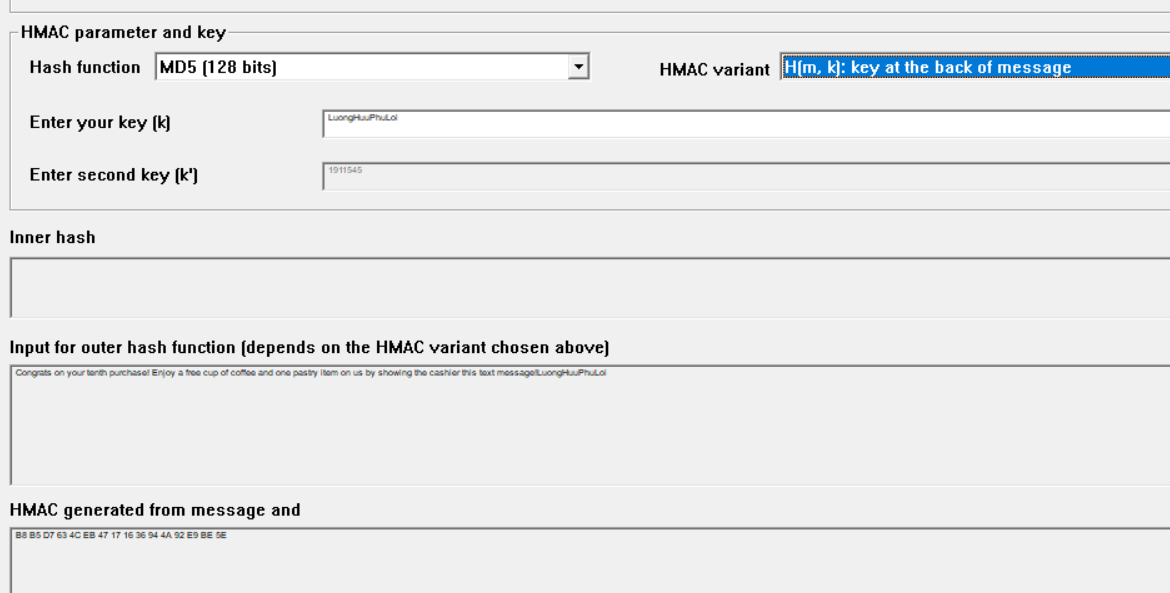
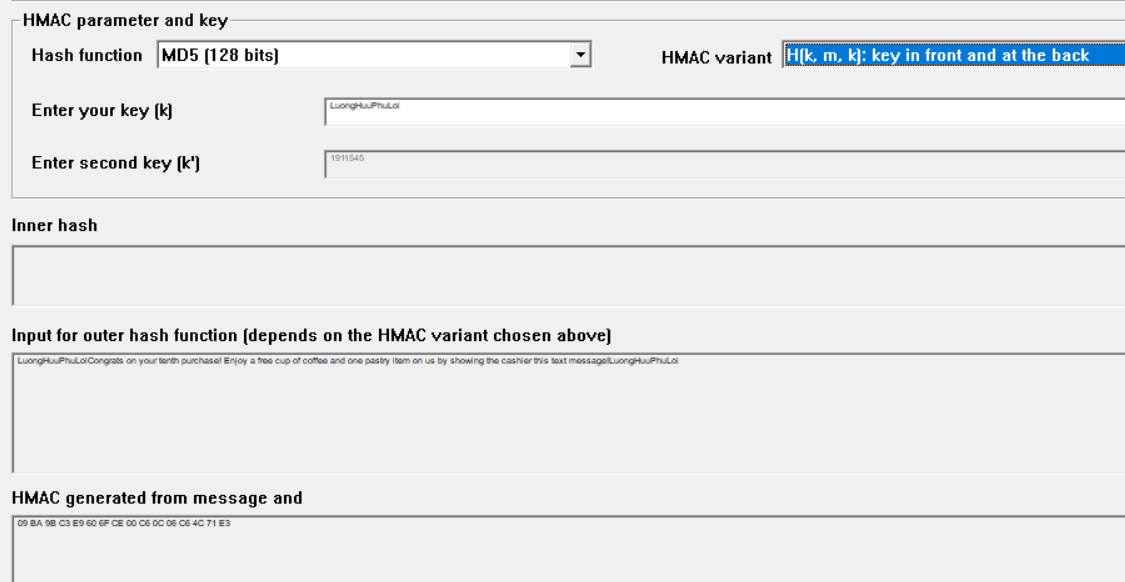
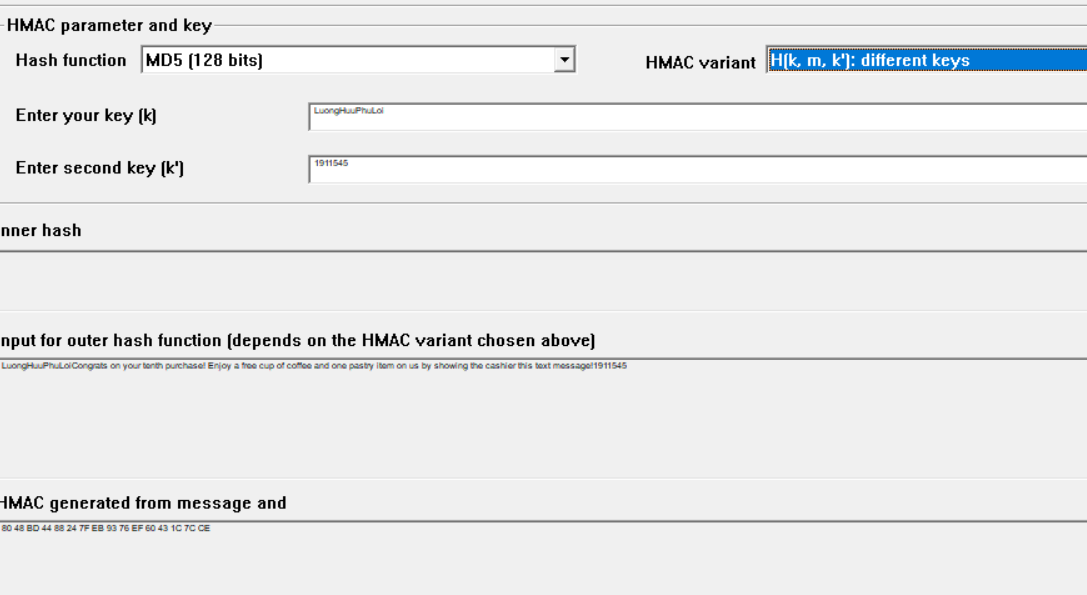
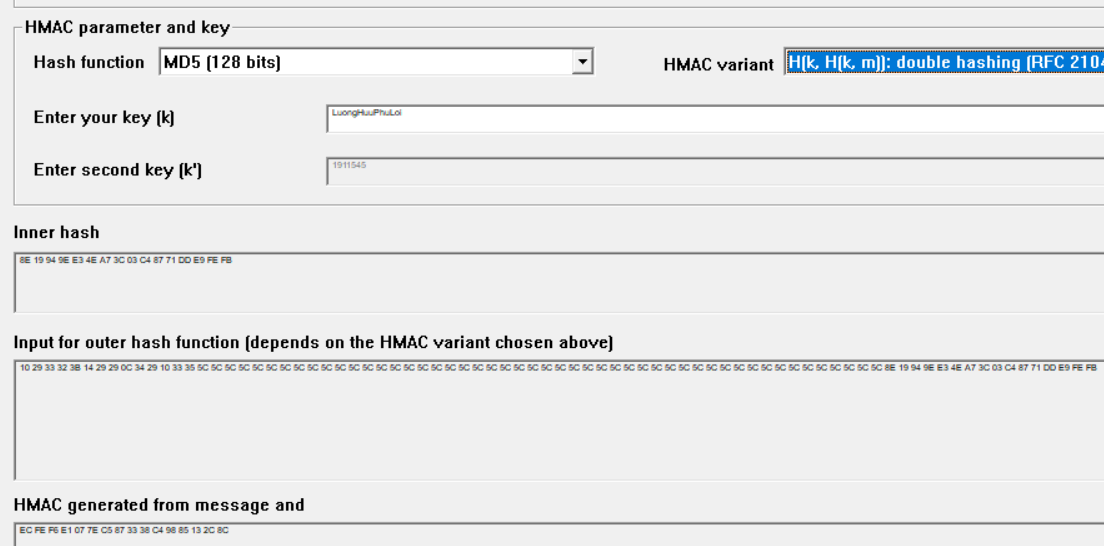
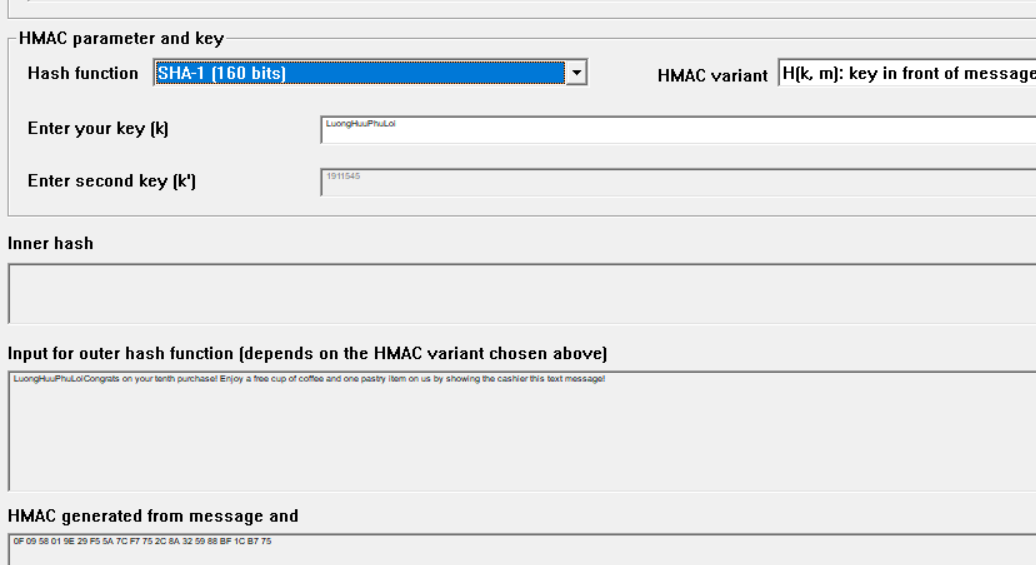
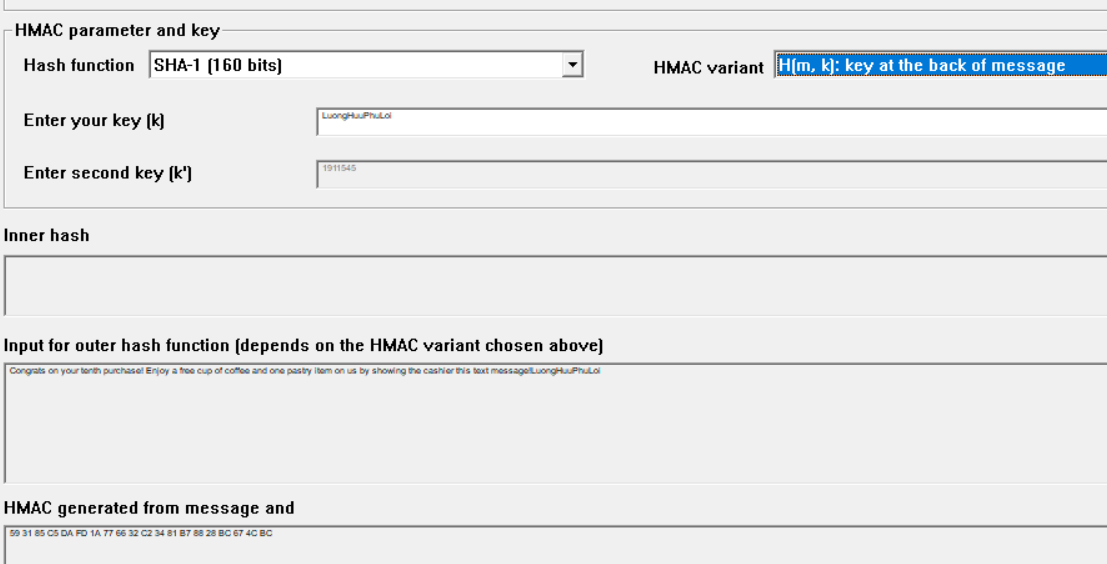
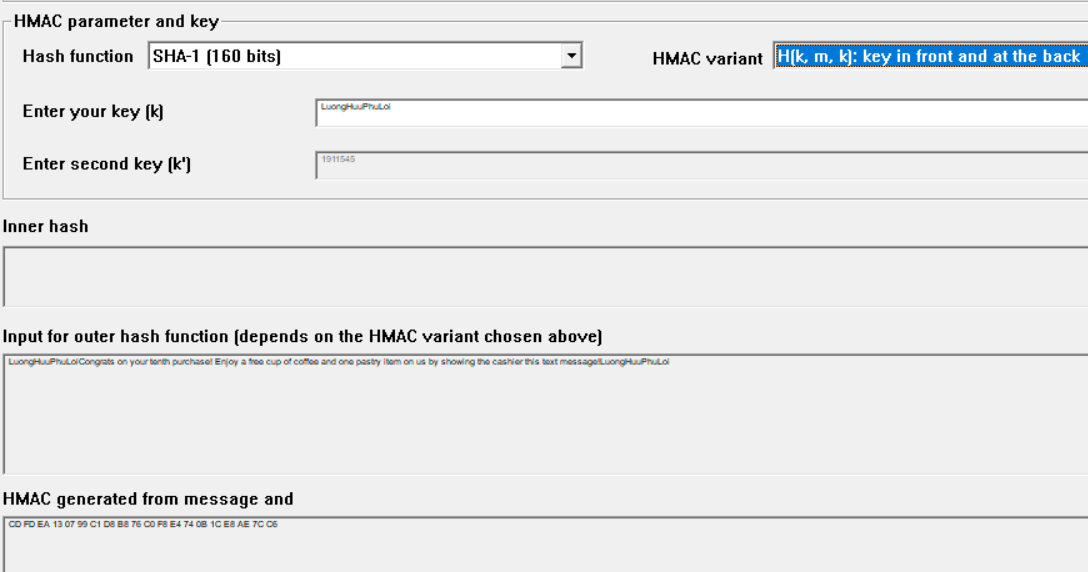
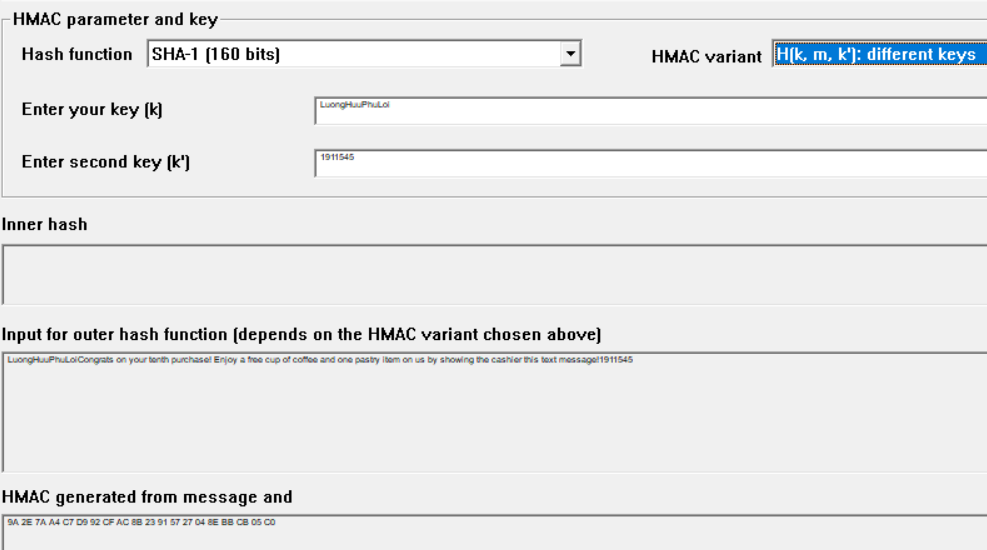
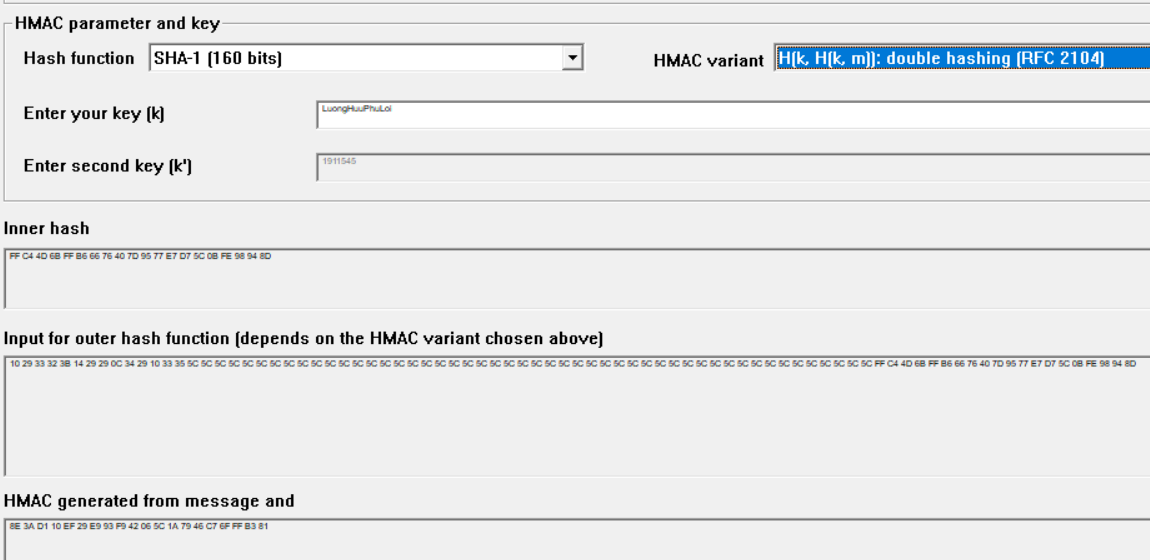
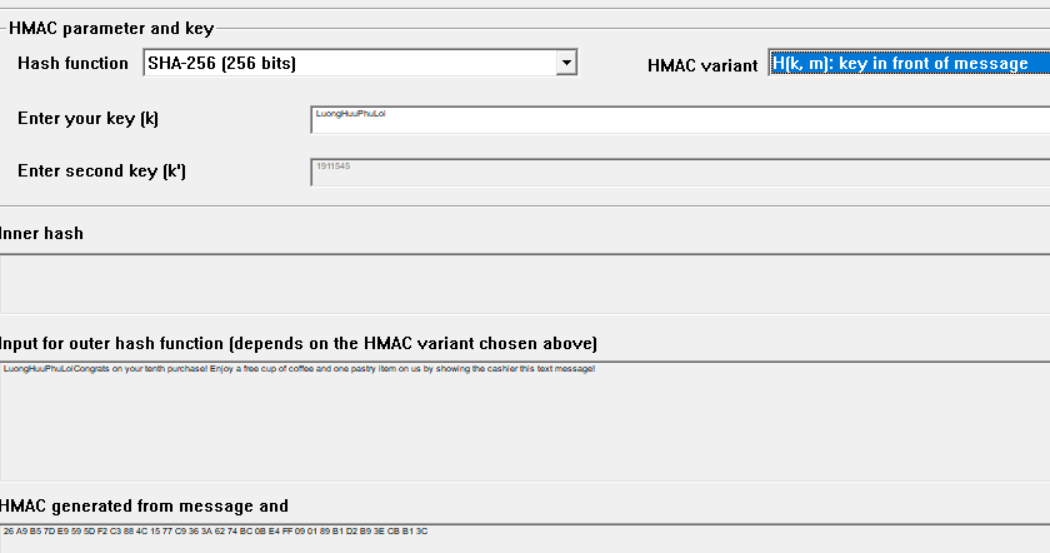
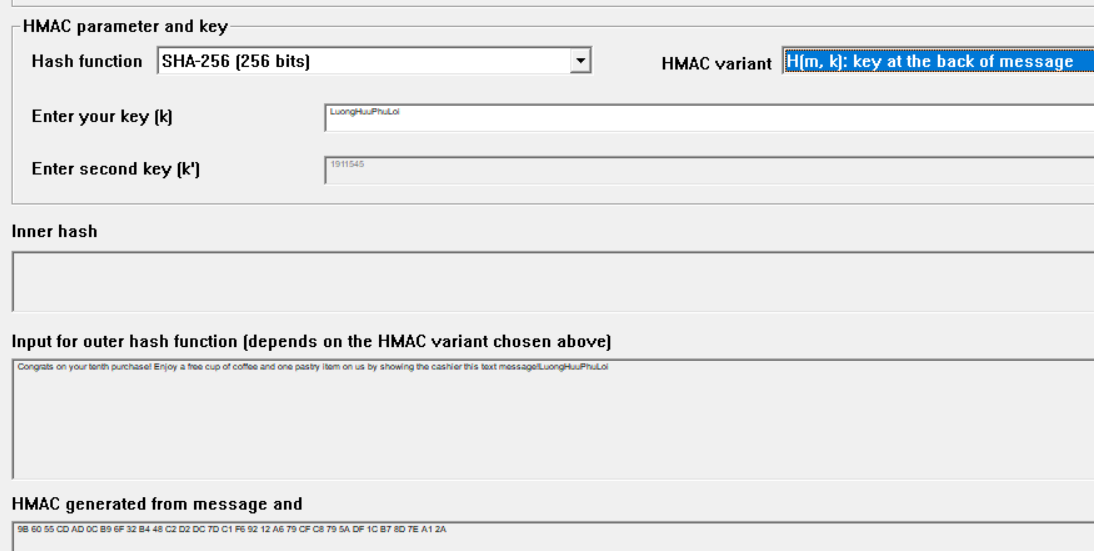
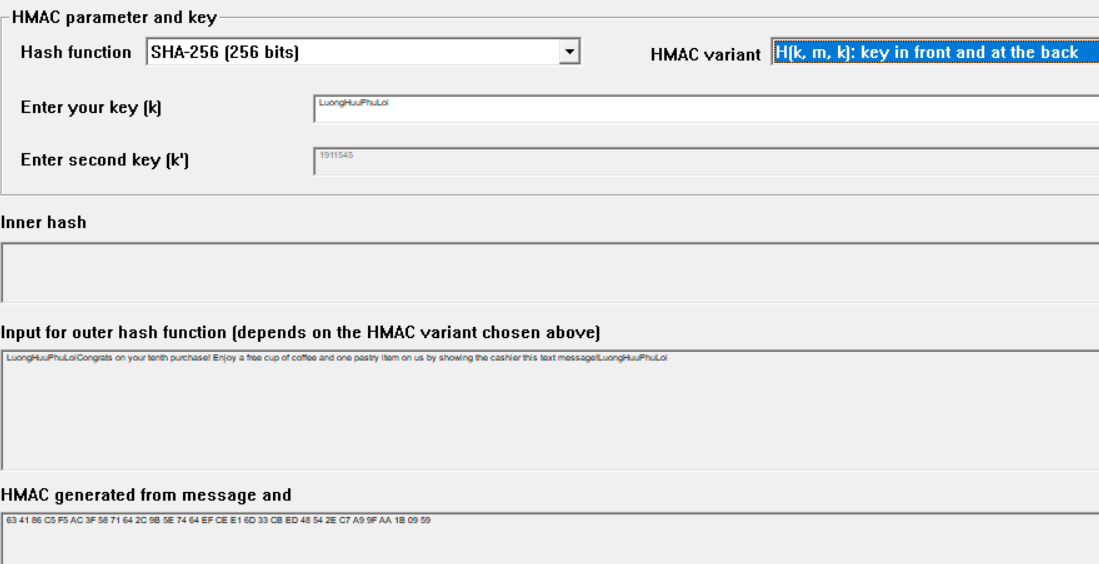
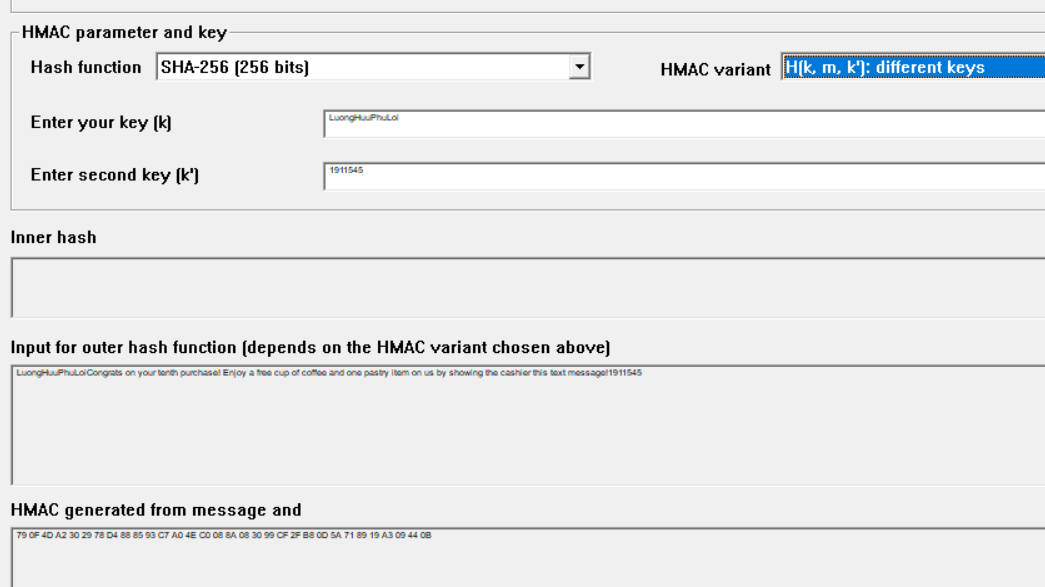
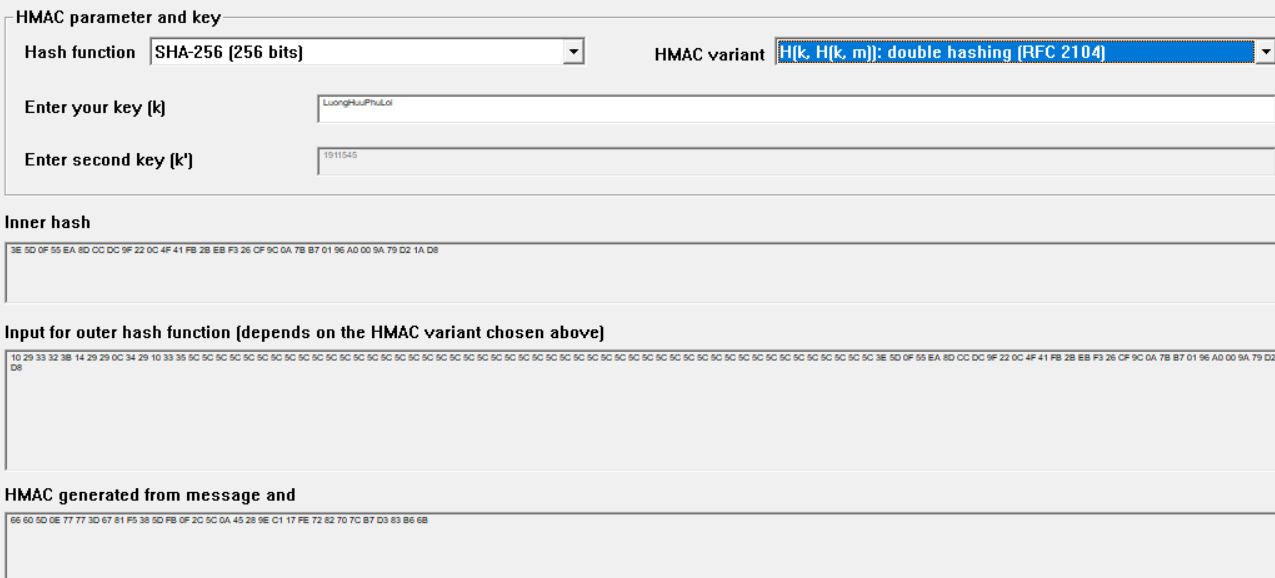
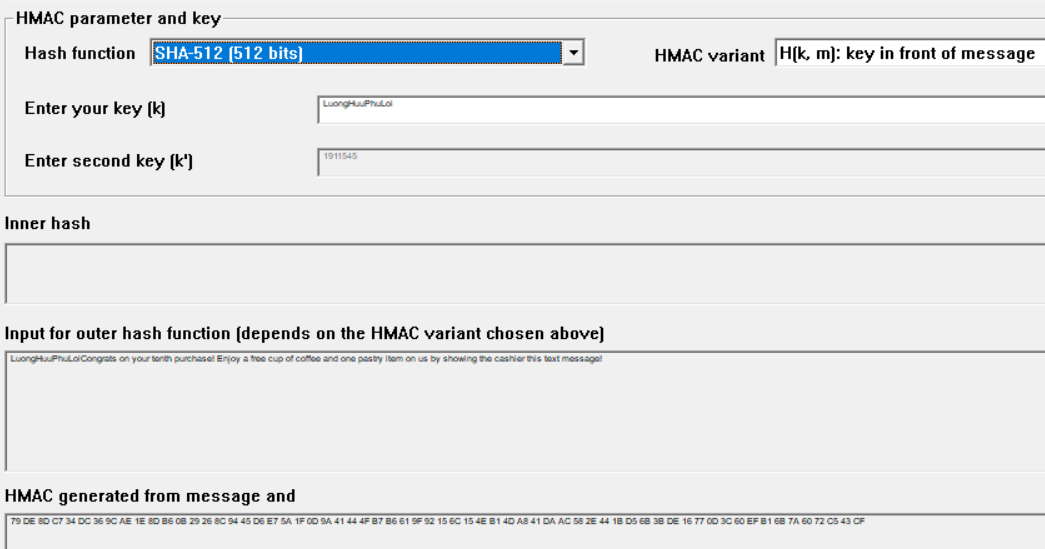
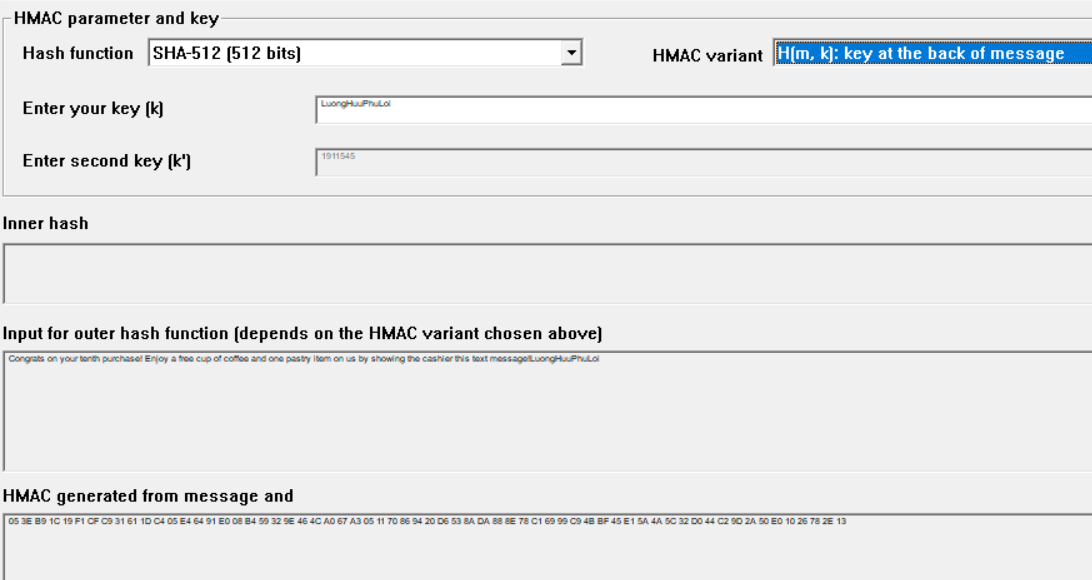
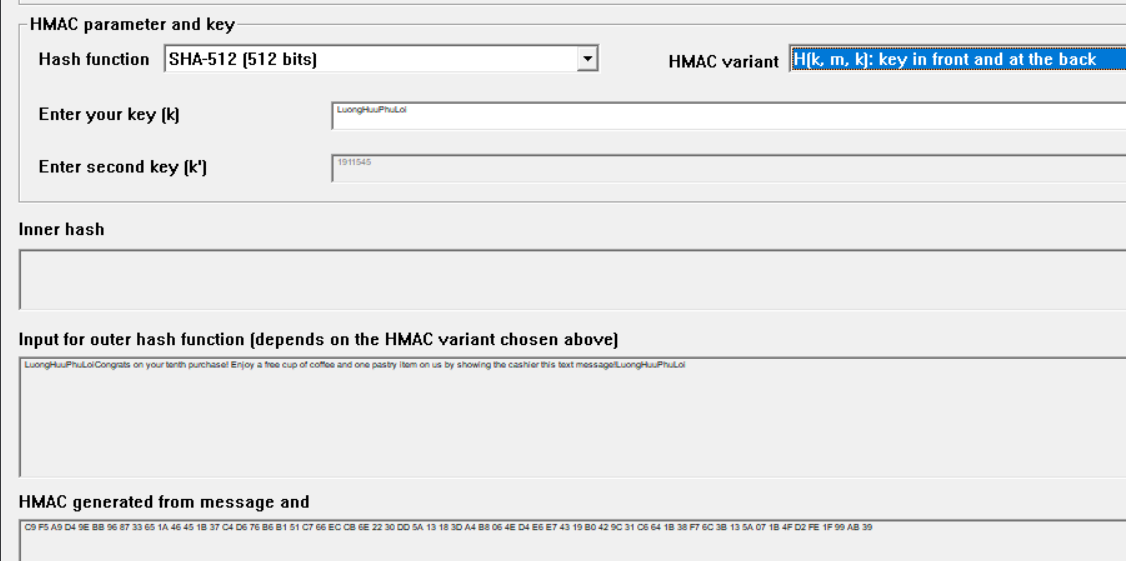
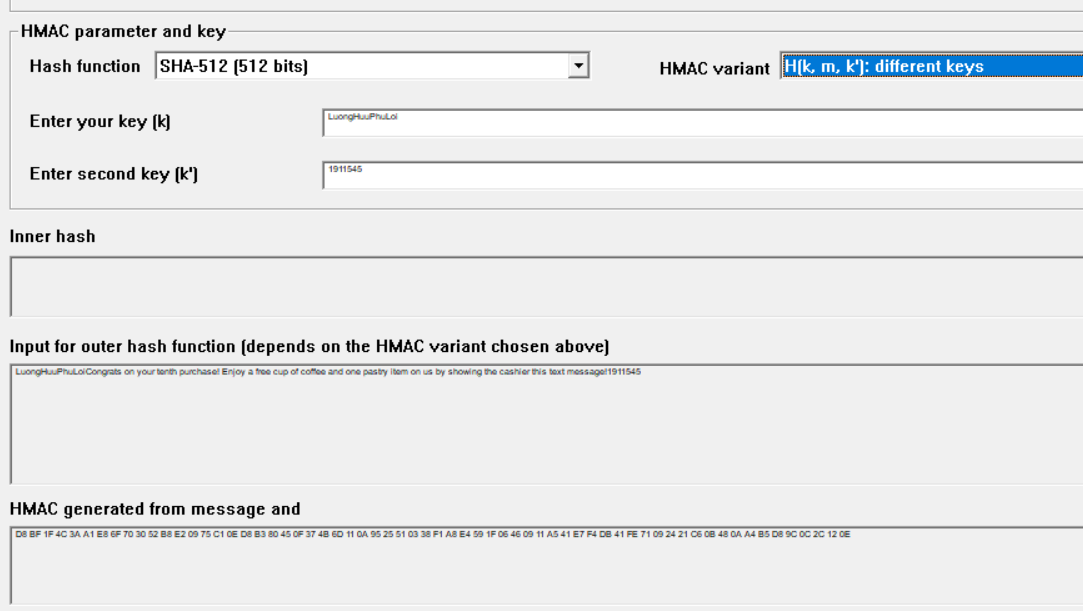
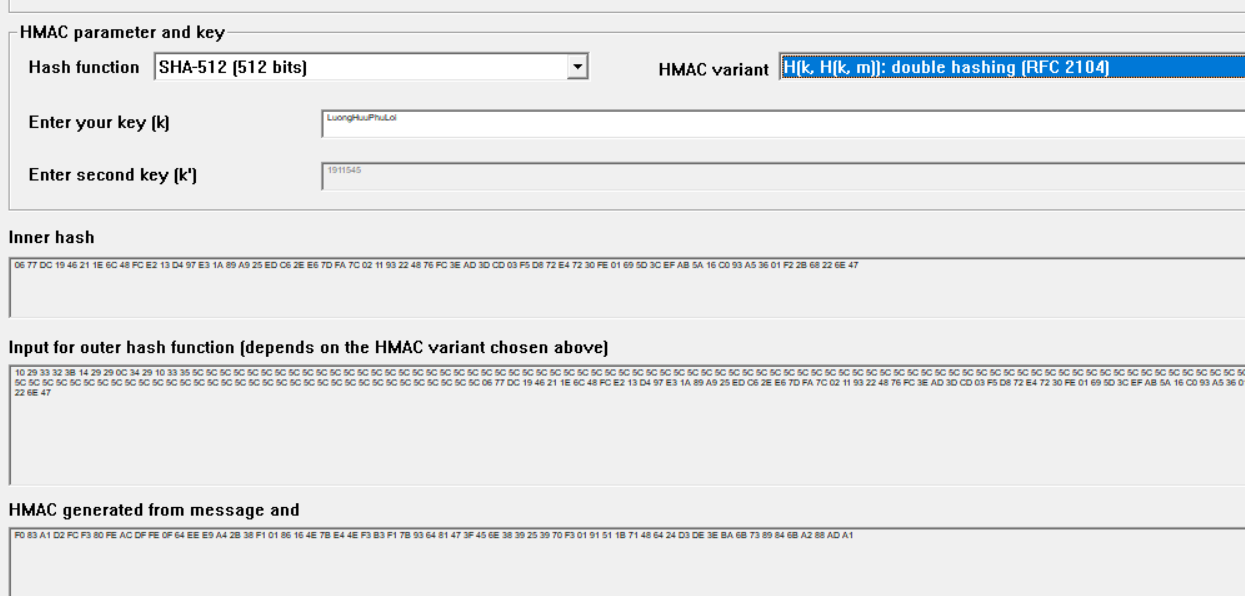
* + - * 1. **Mã xác thực thông điệp MAC**

**Câu 1.** Sử dụng công cụ Cryptool để tính toán HMAC cho một thông điệp theo các bước như bên dưới:

* **Thông điệp:**

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

Ta có k = LuongHuuPhuLoi k’ = 1911545

1. MD5
   1. H(k,m) key in front of messageC7 2C 43 AC CF 4E B2 D6 F2 16 67 C9 59 A7 C0 6F
   2. H(k,m) key at the back of messageB8 B5 D7 63 4C EB 47 17 16 36 94 4A 92 E9 BE 5E
   3. H(k,m) key in front and at the back09 BA 9B C3 E9 60 6F CE 00 C6 0C 06 C6 4C 71 E3
   4. H(k, m, k’) different keys80 48 BD 44 88 24 7F EB 93 76 EF 60 43 1C 7C CE
   5. H(k, H(k,m)) double hashing ( RFC 2104)EC FE F6 E1 07 7E C5 87 33 38 C4 98 85 13 2C 8C
2. SHA-1
   1. H(k,m) key in front of message0F 09 58 01 9E 29 F5 5A 7C F7 75 2C 8A 32 59 88 BF 1C B7 75
   2. H(k,m) key at the back of message59 31 85 C5 DA FD 1A 77 66 32 C2 34 81 B7 88 28 BC 67 4C BC
   3. H(k,m) key in front and at the backCD FD EA 13 07 99 C1 D8 B8 76 C0 F8 E4 74 0B 1C E8 AE 7C C6
   4. H(k, m, k’) different keys9A 2E 7A A4 C7 D9 92 CF AC 8B 23 91 57 27 04 8E BB CB 05 C0
   5. H(k, H(k,m)) double hashing ( RFC 2104)8E 3A D1 10 EF 29 E9 93 F9 42 06 5C 1A 79 46 C7 6F FF B3 81
3. SHA-256
   1. H(k,m) key in front of message26 A9 B5 7D E9 59 5D F2 C3 88 4C 15 77 C9 36 3A 62 74 BC 0B E4 FF 09 01 89 B1 D2 B9 3E CB B1 3C
   2. H(k,m) key at the back of message9B 60 55 CD AD 0C B9 6F 32 B4 48 C2 D2 DC 7D C1 F6 92 12 A6 79 CF C8 79 5A DF 1C B7 8D 7E A1 2A
   3. H(k,m) key in front and at the back63 41 86 C5 F5 AC 3F 58 71 64 2C 9B 5E 74 64 EF CE E1 6D 33 CB ED 48 54 2E C7 A9 9F AA 1B 09 59
   4. H(k, m, k’) different keys79 0F 4D A2 30 29 78 D4 88 85 93 C7 A0 4E C0 08 8A 08 30 99 CF 2F B8 0D 5A 71 89 19 A3 09 44 0B   
      |
   5. H(k, H(k,m)) double hashing ( RFC 2104)66 60 5D 0E 77 77 3D 67 81 F5 38 5D FB 0F 2C 5C 0A 45 28 9E C1 17 FE 72 82 70 7C B7 D3 83 B6 6B
4. SHA-512
   1. H(k,m) key in front of message79 DE 8D C7 34 DC 36 9C AE 1E 8D B6 0B 29 26 8C 94 45 D6 E7 5A 1F 0D 9A 41 44 4F B7 B6 61 9F 92 15 6C 15 4E B1 4D A8 41 DA AC 58 2E 44 1B D5 6B 3B DE 16 77 0D 3C 60 EF B1 6B 7A 60 72 C5 43 CF
   2. H(k,m) key at the back of message05 3E B9 1C 19 F1 CF C9 31 61 1D C4 05 E4 64 91 E0 08 B4 59 32 9E 46 4C A0 67 A3 05 11 70 86 94 20 D6 53 8A DA 88 8E 78 C1 69 99 C9 4B BF 45 E1 5A 4A 5C 32 D0 44 C2 9D 2A 50 E0 10 26 78 2E 13
   3. H(k,m) key in front and at the backC9 F5 A9 D4 9E BB 96 87 33 65 1A 46 45 1B 37 C4 D6 76 B6 B1 51 C7 66 EC CB 6E 22 30 DD 5A 13 18 3D A4 B8 06 4E D4 E6 E7 43 19 B0 42 9C 31 C6 64 1B 38 F7 6C 3B 13 5A 07 1B 4F D2 FE 1F 99 AB 39
   4. H(k, m, k’) different keysD8 BF 1F 4C 3A A1 E8 6F 70 30 52 B8 E2 09 75 C1 0E D8 B3 80 45 0F 37 4B 6D 11 0A 95 25 51 03 38 F1 A8 E4 59 1F 06 46 09 11 A5 41 E7 F4 DB 41 FE 71 09 24 21 C6 0B 48 0A A4 B5 D8 9C 0C 2C 12 0E
   5. H(k, H(k,m)) double hashing ( RFC 2104)F0 83 A1 D2 FC F3 80 FE AC DF FE 0F 64 EE E9 A4 2B 38 F1 01 86 16 4E 7B E4 4E F3 B3 F1 7B 93 64 81 47 3F 45 6E 38 39 25 39 70 F3 01 91 51 1B 71 48 64 24 D3 DE 3E BA 6B 73 89 84 6B A2 88 AD A1

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

- Thay thế (substitution)

- Giả danh (Masquerade)

- Tấn công phát lại (Reply attack)

- Phủ nhận (Repudiation)

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

|  |  |
| --- | --- |
| **Hàm băm (hash)** | **Mã xác thực thông điệp (MAC)** |
| - Tính toàn vẹn: Có  - Tính xác thực: Không  - Khóa : Không có | - Tính toàn vẹn: Có  - Tính xác thực: Có  - Khóa : Không đồng bộ |

**Phần 2. Chữ ký số**

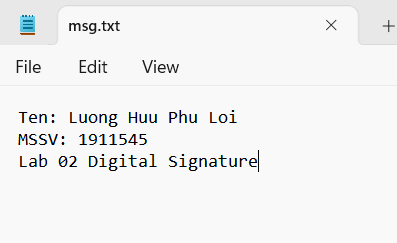
**Câu 1.** Mô phỏng chữ ký số bằng chương trình Cryptool, thực hiện theo các bước như hướng dẫn tham khảo bên dưới, với đầu vào là tập tin **msg.txt** chứa thông tên đầy đủ và mã số sinh viên. Chụp ảnh màn hình từng bước như phần tham khảo.

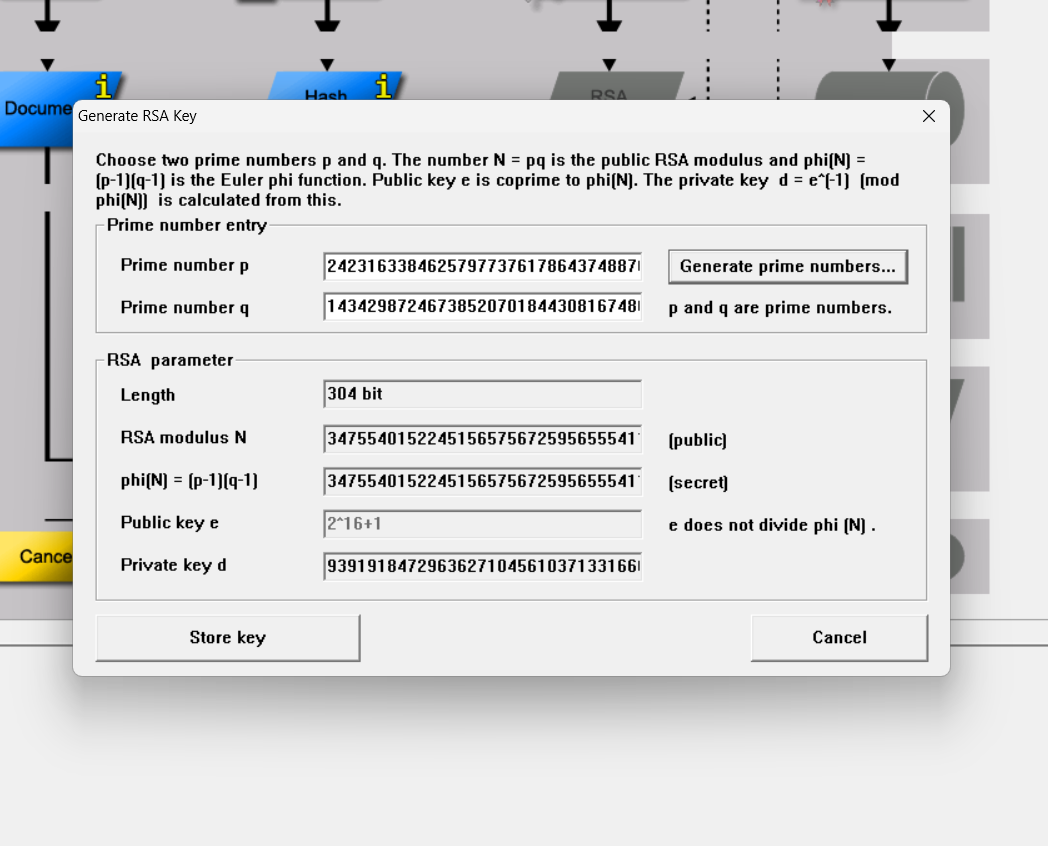
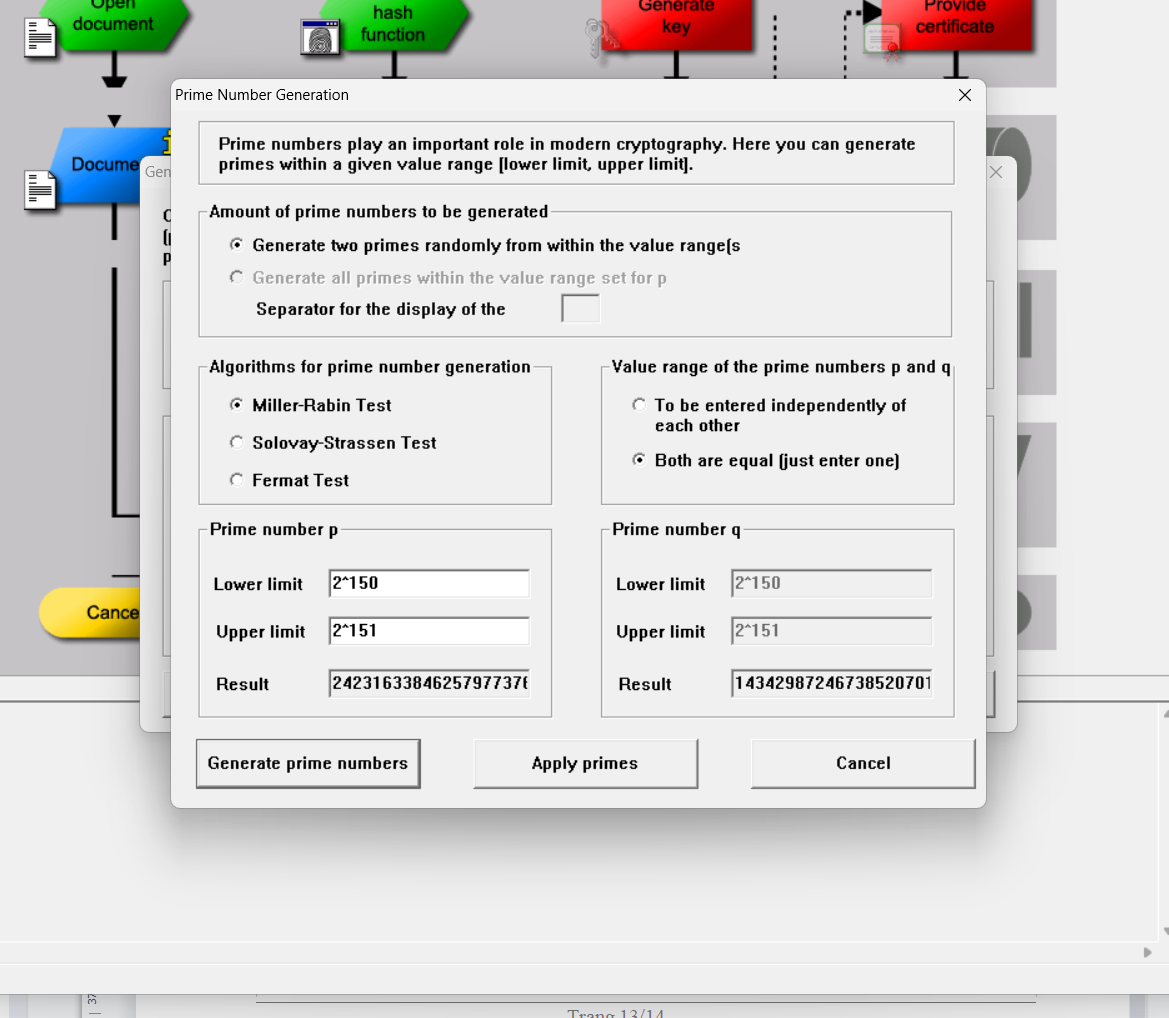
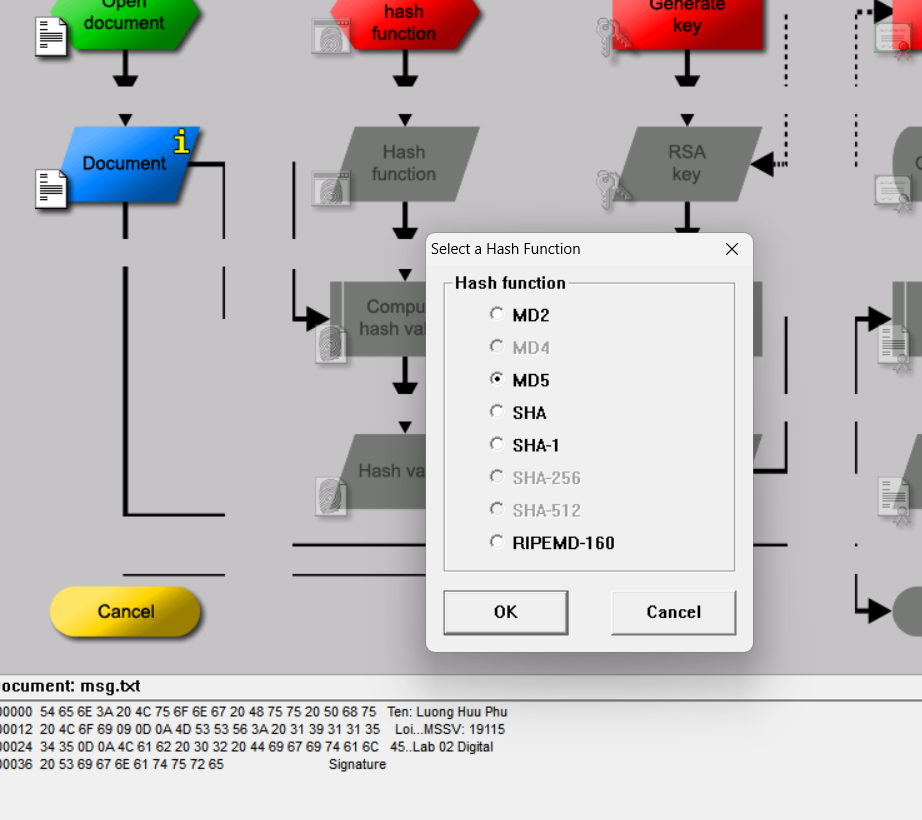
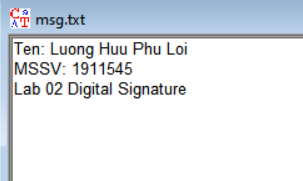
Tập tin **msg.txt** có nội dung như sau:

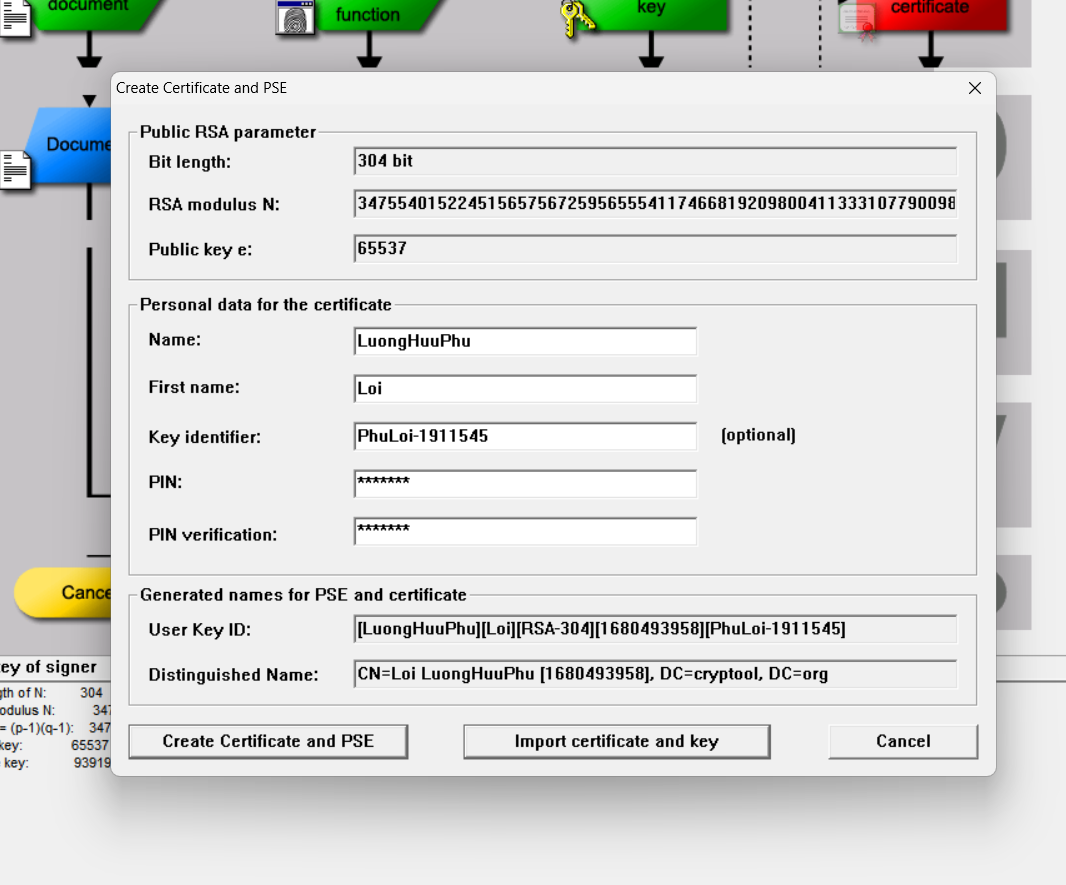
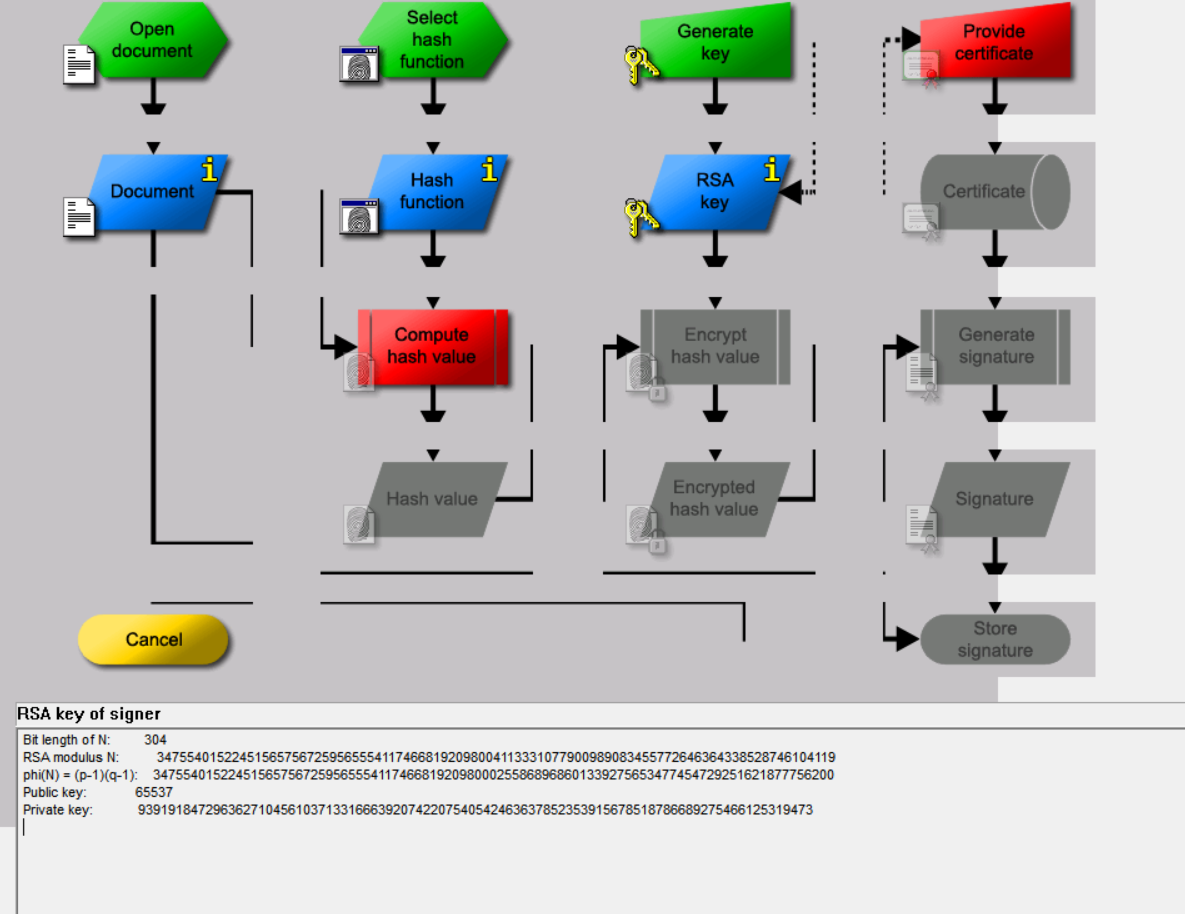
Ten: Luong Huu Phu Loi

MSSV: 1911545

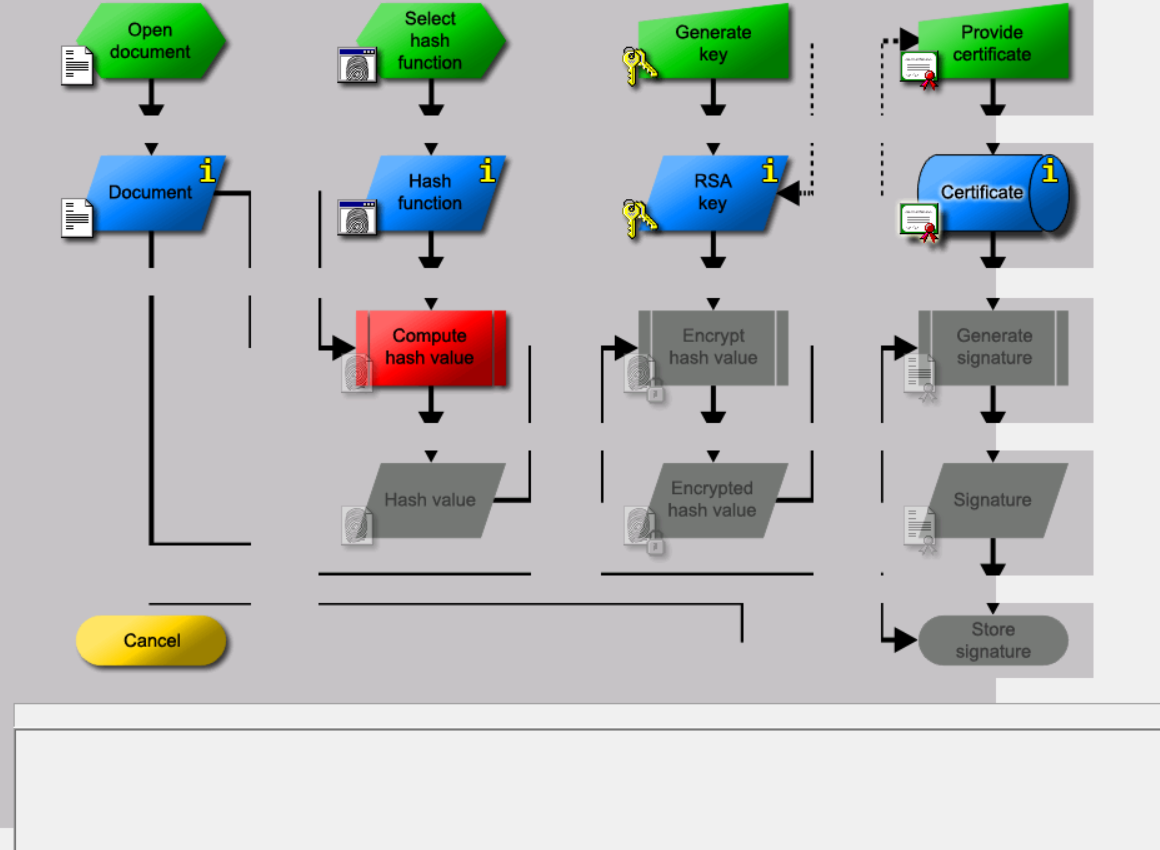
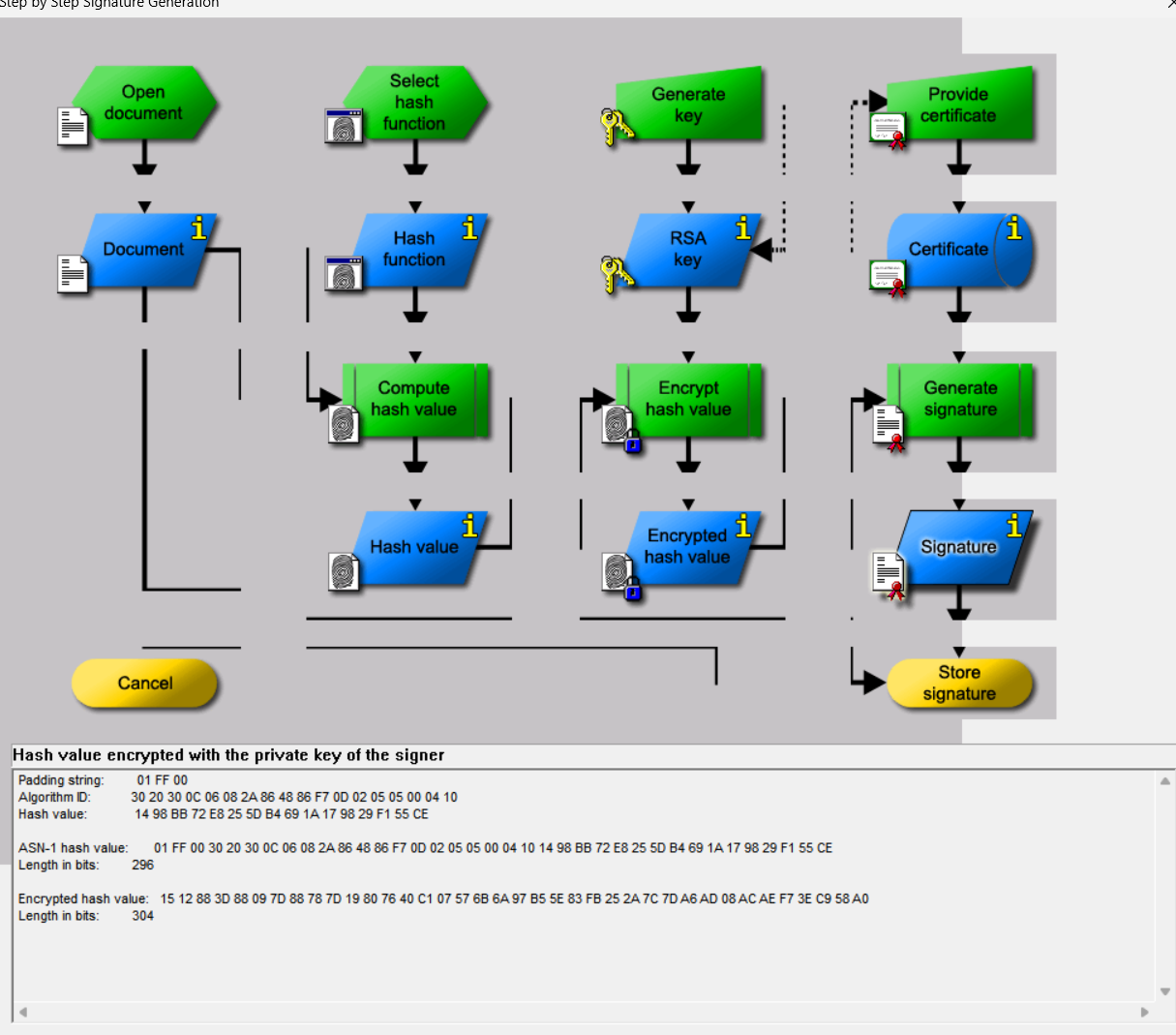
Lab 02 Digital Signature

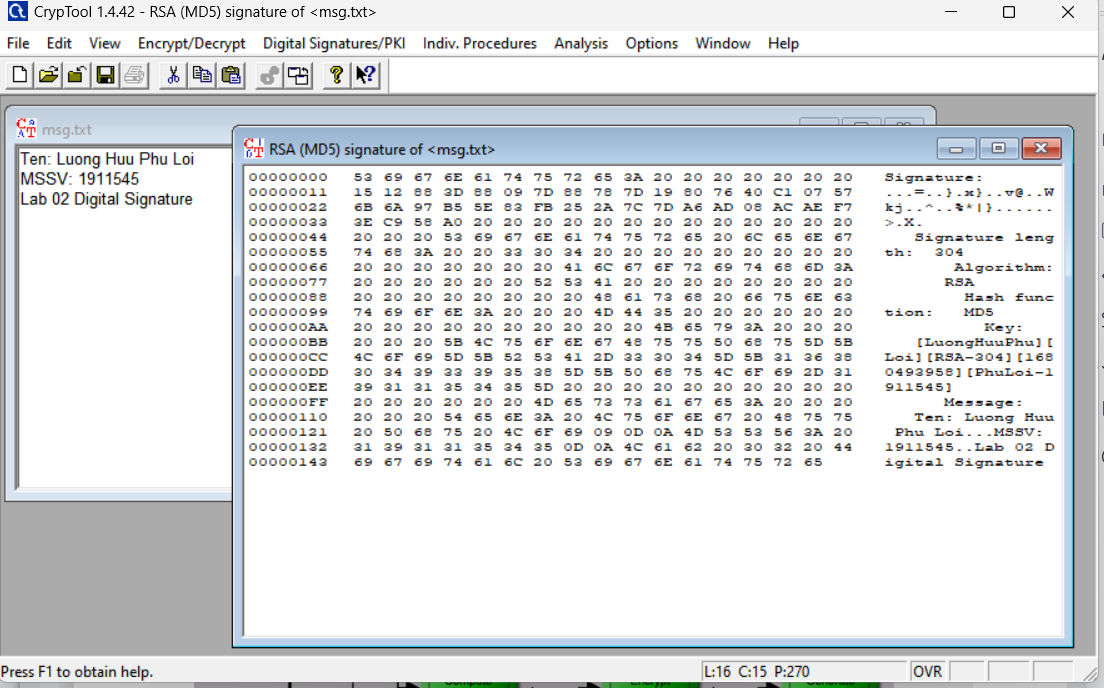






PIN là 1911545



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

Một số yêu cầu:

- Chữ ký phải mang đặc trưng của người tạo văn bản .

- Chữ ký không thể sử dụng lại .

- Văn bản đã ký không được sửa đổi. Nếu có thì cần phải thực hiện ký lại trên văn bản mới.

- Chữ ký phải là một mẫu bit phụ thuộc vào thông điệp được ký.

- Chữ kí phải sử dụng một số thông tin duy nhất cho người gửi để ngăn chặn giả mạo và từ chối.

- Phải tương đối dễ dàng để tạo chữ ký số.

- Phải tương đối để nhận biết và xác minh chữ ký số. - Phải giữ lại một bản sao của chữ kí số trong bộ nhớ.

- Phải được tính toán không khả thi để giả mạo chữ kí số bằng cách hoặc bằng cách xây dựng một tin nhắn mới cho một chữ ký số hiện có hoặc bằng cách xây dựng một chữ ký số lừa đảo cho một tin nhắn nhất định.

- Phải xác minh tác giả, ngày và thời gian của chữ ký.

- Phải xác thực nội dung tại thời điểm của chữ ký.

- Phải được bên thứ ba kiểm chứng, để giải quyết

**Câu 3.** Hãy giải thích 2 tranh chấp có thể xảy ra khi sử dụng mã xác thực thông điệp MAC (người gởi thoái thác đã gởi thông điệp, người nhận thoái thác đã nhận thông điệp), chữ ký số giúp giải quyết vấn đề này như thế nào?

Hai tranhh chấp có thể xảy ra khi sử dụng mã xác thực thông điệp MAC:

- Bên gửi từ chối hành vi gửi.

- Bên nhận từ chối hành vi nhận. 

Chữ ký số:

- Xác minh tác giả và thời điểm ký thông báo.

- Xác thực nội dung thông báo.

=> Là căn cứ để giải quyết tranh chấp bên gửi từ chối hành vi gian lận