



BÀI THỰC HÀNH SỐ 4

Môn: MẬT MÃ & AN NINH MẠNG

-o0o-

I. MỤC TIÊU

- Cung cấp kiến thức về mã xác thực thông điệp MAC, tạo mã xác thực thông điệp sử dụng hàm hash (HMAC) sử dụng công cụ Cryptool.
- Cung cấp kiến thức về chữ ký số, demo các bước tạo chữ ký số trên thông điệp sử dụng công cụ Cryptool.

II. CHUẨN BỊ TRƯỚC KHI THỰC HIỆN BÀI THỰC HÀNH

- Sinh viên ôn tập lại phần lý thuyết chương 4 và chương 5
- Cài đặt công cụ CrypTool 1 (version: 1.4.31 Beta 06 - English), sinh viên có thể sử dụng công cụ Cryptool phiên bản mới hơn, giao diện tương tự.
<https://www.cryptool.org/en/ct1-downloads>

III. CÁCH THỨC VÀ HẠN CHÓT NỘP BÀI

- Sinh viên trả lời tất cả các câu hỏi trong bài thực hành vào file <MSSV>_Lab04.docx (sử dụng mẫu file trả lời được đính kèm) và nộp bài theo deadline của bài Lab04 ở Bkel, không nhận bài nộp qua email hay các hình thức khác.
- Thời gian để thực hiện bài Lab là 14 ngày.

IV. NỘI DUNG THỰC HIỆN

Phần 1. Mã xác thực thông điệp MAC

1.1. Tìm hiểu mã xác thực thông điệp MAC

- **Mã xác thực thông điệp**, là một thông tin ngắn được sử dụng để **xác thực một thông điệp**, nói cách khác, mã xác thực thông điệp được sử dụng để xác nhận rằng tin nhắn đến từ người gửi đã nêu (tính xác thực) và không bị thay đổi (tính toàn vẹn).
- **Phân loại mã xác thực thông điệp:**
 - o **CMAC (hay CBC MAC)**: được tạo ra dựa trên thuật toán **mã hoá đối xứng** (AES và Triple-DES) theo chế độ **CBC**, dùng đầu ra của khối cuối như là MAC

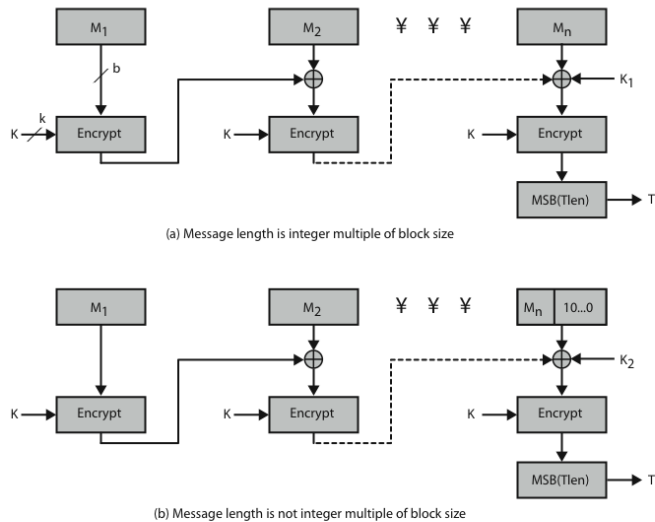
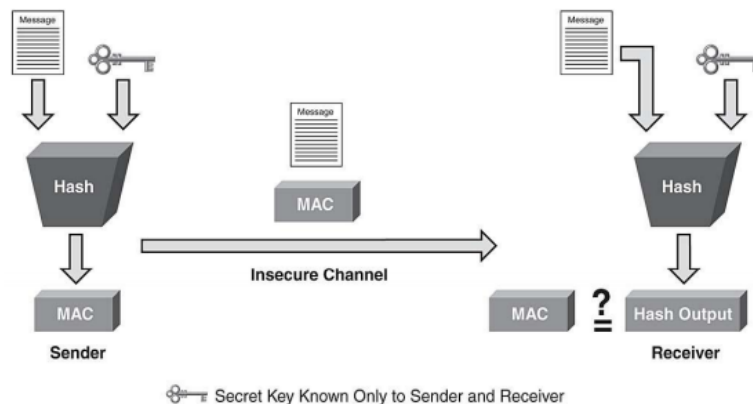


Figure 12.12 Cipher-Based Message Authentication Code (CMAC)

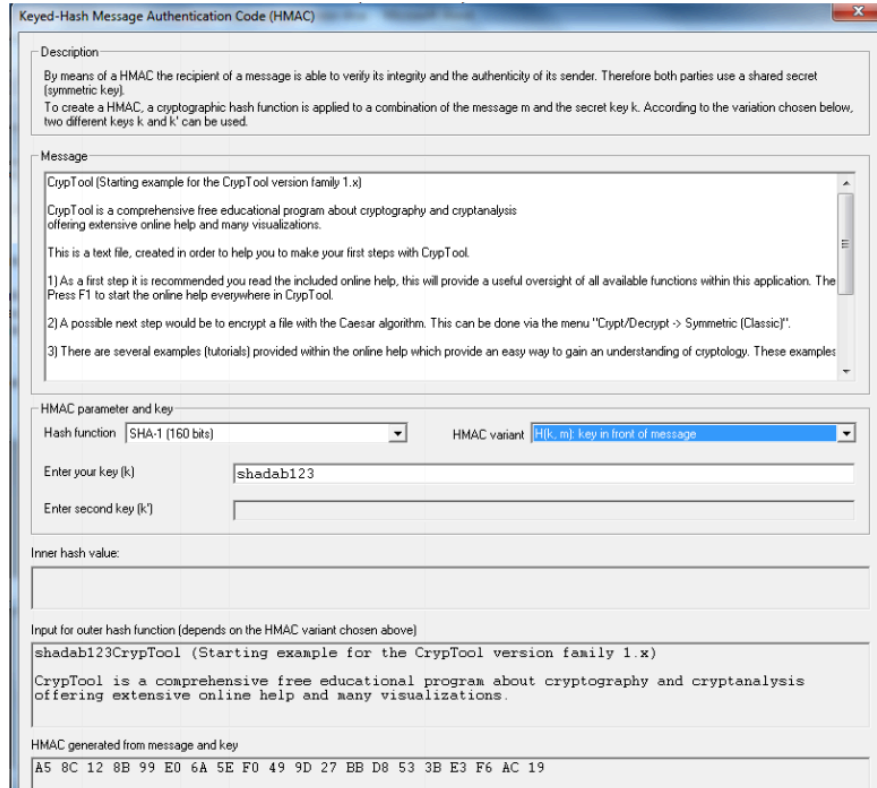
- **HMAC** (keyed-hash message authentication code): sử dụng hàm băm mật mã (**hash**) cùng với một **khoá đối xứng**



1.2. Bài tập

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

- Bước 1.** Trong cửa sổ chương trình Cryptool, chọn menu **Indiv. Procedures** → **Hash** → **Generation of HMACs...**
- Bước 2.** Chọn hàm Hash tương ứng
- Bước 3.** Chọn biến thể HMAC (variant)
- Bước 4.** Nhập khoá (một hoặc nhiều khoá tùy theo biến thể HMAC đã chọn)
- Bước 5.** HMAC được tạo ra tự động sau khi nhập các thông số cần thiết



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
CrypTool (Starting example for the CrypTool version family 1.x)
CrypTool is a comprehensive free educational program about cryptography and cryptanalysis offering extensive online help and many visualizations.
This is a text file, created in order to help you to make your first steps with CrypTool.
1) As a first step it is recommended you read the included online help, this will provide a useful oversight of all available functions within this application. The Press F1 to start the online help everywhere in CrypTool.
2) A possible next step would be to encrypt a file with the Caesar algorithm. This can be done via the menu "Crypt/Decrypt -> Symmetric (Classic)".
3) There are several examples (tutorials) provided within the online help which provide an easy way to gain an understanding of cryptography. These examples

HMAC parameter and key
Hash function: SHA-1 (160 bits) HMAC variant: H(k, m): key in front of message
Enter your key (k): shadab123
Enter second key (k'):

Inner hash value:

Input for outer hash function (depends on the HMAC variant chosen above)
shadab123CrypTool (Starting example for the CrypTool version family 1.x)
CrypTool is a comprehensive free educational program about cryptography and cryptanalysis offering extensive online help and many visualizations.

HMAC generated from message and key
A5 8C 12 8B 99 E0 6A 5E F0 49 9D 27 BB D8 53 3B E3 F6 AC 19

Bạn hãy sử dụng hướng dẫn như bên trên để thực hiện tính HMAC cho thông điệp và các thông tin bên dưới, ghi lại kết quả vào file trả lời và nhận xét về độ dài của các HMAC thu được:

- **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!

- **Hàm Hash:**

Chọn các loại hàm hash: MD5, SHA-1, SHA-256, SHA-512

- **Biến thể (variant):**

Chọn tất cả biến thể có trong danh sách ứng với từng hàm hash lựa chọn ở trên.

- **Nhập khoá:**

k: tên đầy đủ của sinh viên viết liền (ví dụ: NguyenVanAn)

k' (nếu có): nhập mã số sinh viên

HMAC attack

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

Tấn công ngày sn

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

Slide 5 - Slide 9 Chương IV

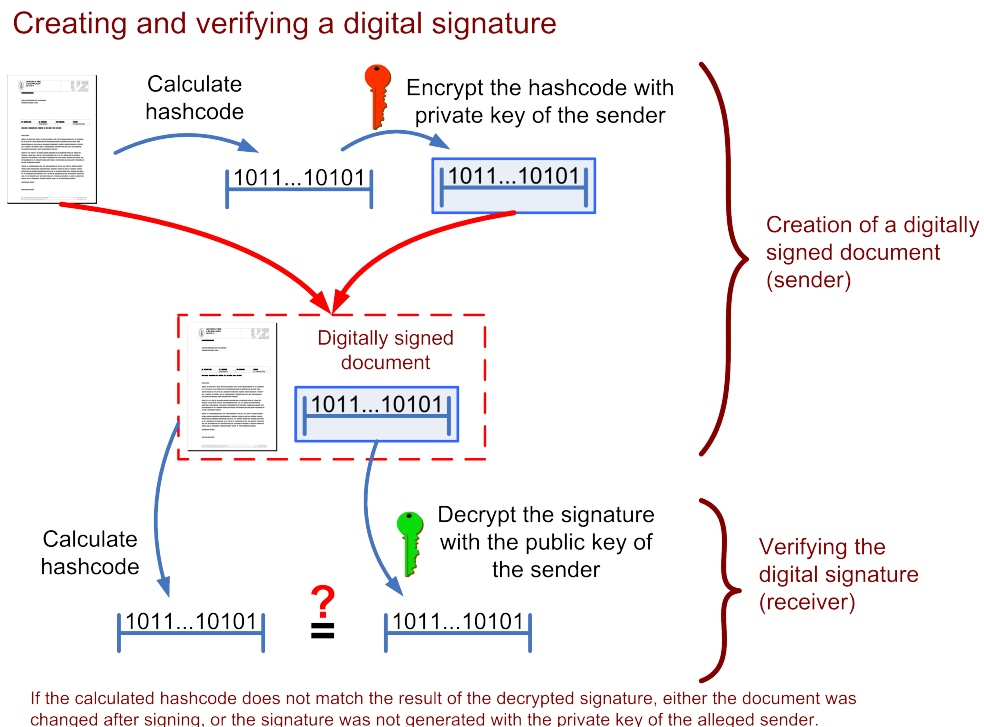
Phần 2. Chữ ký số

2.1. Tìm hiểu chữ ký số

Chữ ký số là một sơ đồ toán học để chứng minh tính xác thực của các thông điệp hoặc tài liệu kỹ thuật số, Chữ ký số cung cấp khả năng:

- Xác minh tác giả, ngày giờ đã ký (xác thực)
- Toàn vẹn thông điệp (toàn vẹn)
- Được xác minh bởi một tổ chức thứ 3 để giải quyết tranh chấp (chống thoái thác)

Chữ ký số được tạo ra theo sơ đồ như sau:



2.2. Bài tập

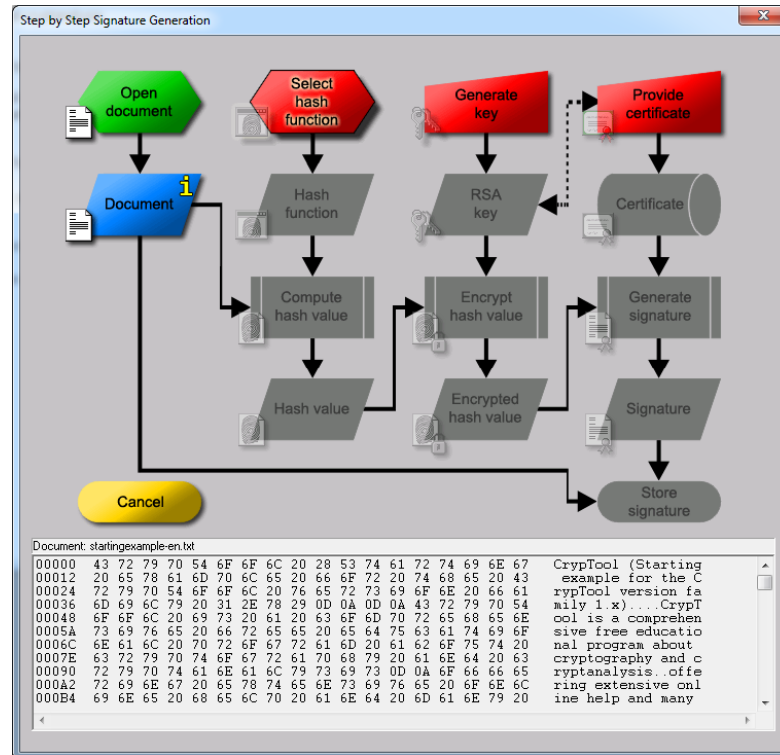
Câu 1. Mô phỏng chữ ký số bằng chương trình Cryptool, thực hiện theo các bước như hướng dẫn tham khảo bên dưới, với đầu vào là tập tin **msg.txt** chứa thông tin đầy đủ và mã số sinh viên. **Chụp ảnh màn hình** từng bước như phần tham khảo.

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

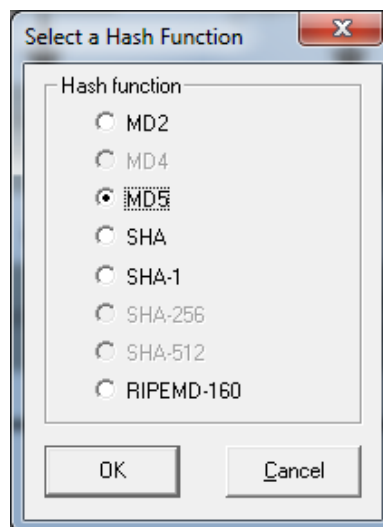
Ten: Nguyen Van An
MSSV: 123456789
Lab 04 Digital Signature

Các bước tham khảo:

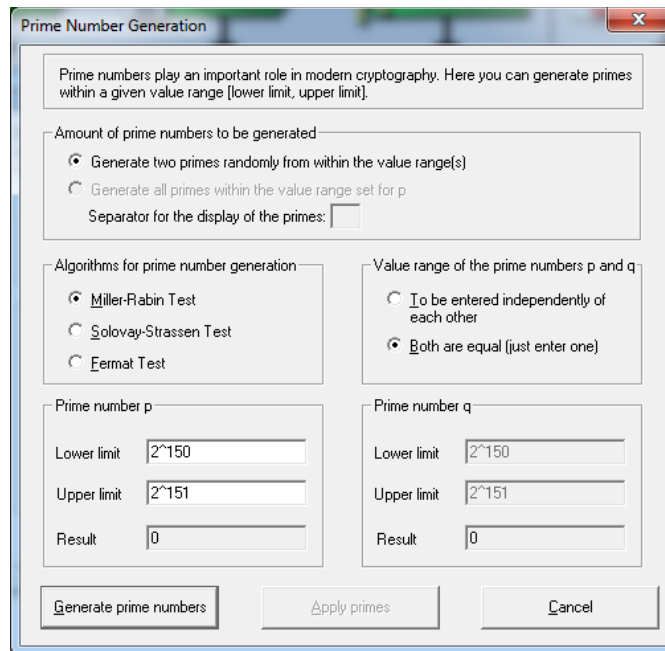
1. Từ giao diện của chương trình Cryptool, chọn menu “**Digital Signatures/PKI**” → “**Signature Demonstration (Signature Generation)**”



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



3. Chọn “**Generate Key**” và “**Generate prime numbers**” trong hộp thoại **step by step Signature Generation**



Prime numbers play an important role in modern cryptography. Here you can generate primes within a given value range [lower limit, upper limit].

Amount of prime numbers to be generated

- ☒ Generate two primes randomly from within the value range(s)
- ☐ Generate all primes within the value range set for p

Separator for the display of the primes:

Algorithms for prime number generation

- ☒ Miller-Rabin Test
- ☐ Solovay-Strassen Test
- ☐ Fermat Test

Value range of the prime numbers p and q

- ☐ To be entered independently of each other
- ☒ Both are equal (just enter one)

Prime number p

Lower limit:

Upper limit:

Result:

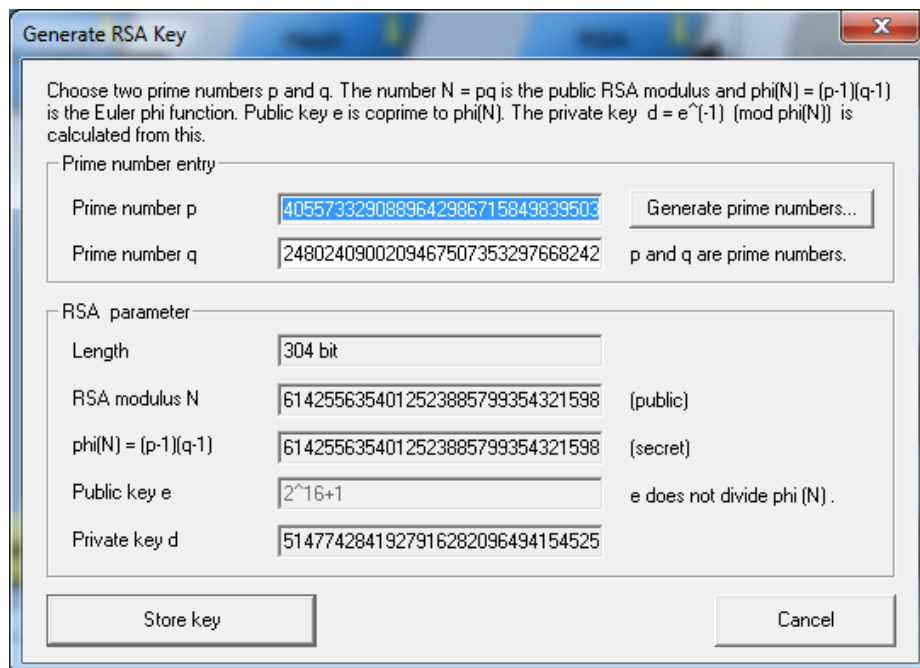
Prime number q

Lower limit:

Upper limit:

Result:

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



Choose two prime numbers p and q. The number $N = pq$ is the public RSA modulus and $\phi(N) = (p-1)(q-1)$ is the Euler phi function. Public key e is coprime to $\phi(N)$. The private key $d = e^{-1} \pmod{\phi(N)}$ is calculated from this.

Prime number entry

Prime number p:

Prime number q: p and q are prime numbers.

RSA parameter

Length:

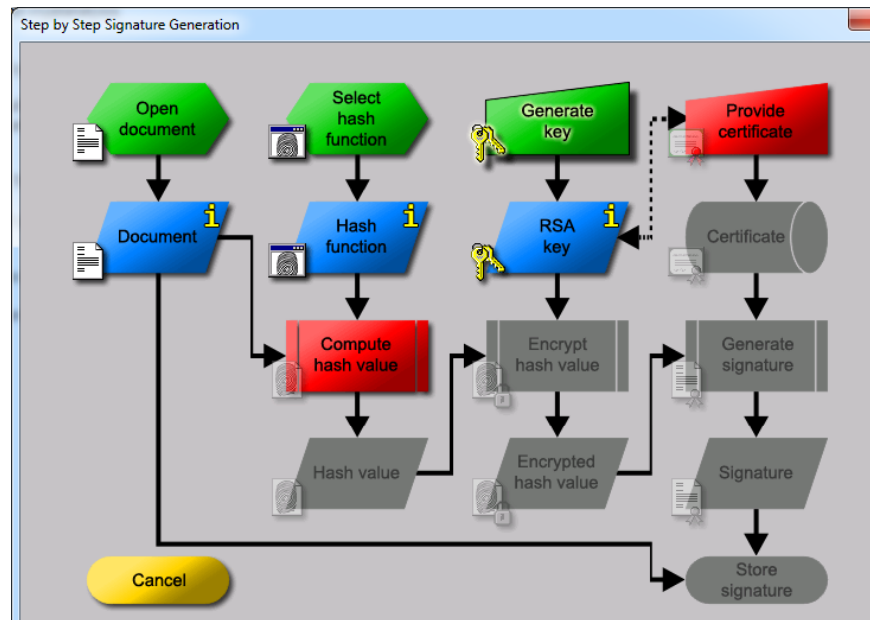
RSA modulus N: (public)

$\phi(N) = (p-1)(q-1)$: (secret)

Public key e: e does not divide $\phi(N)$.

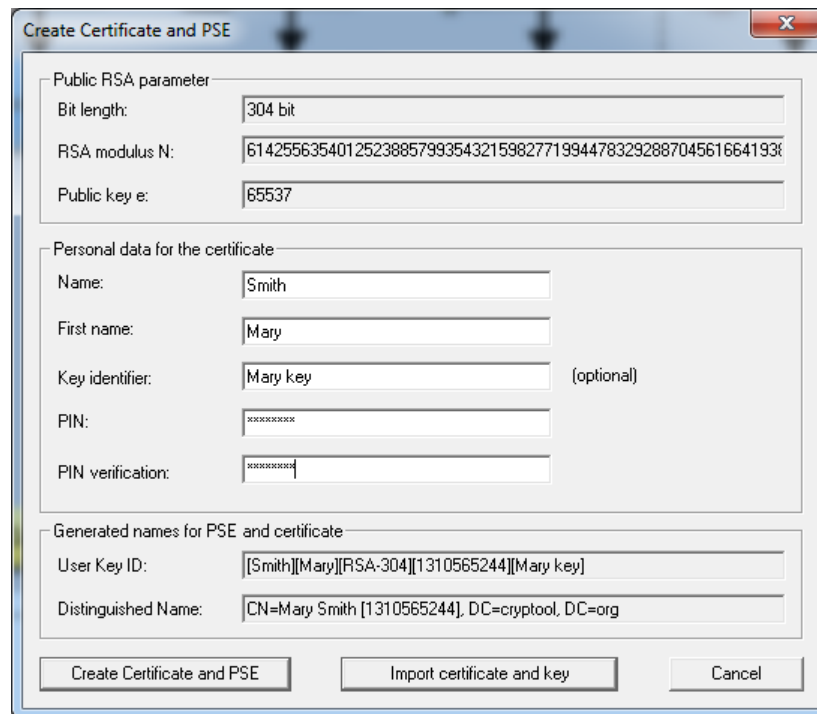
Private key d:

5. Nhấn nút **Store key**



6. 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 (<tên> key): **Mary key**
- PIN: **cryptool**
- PIN verification: **cryptool**



Create Certificate and PSE

Public RSA parameter

Bit length: 304 bit

RSA modulus N: 614255635401252388579935432159827719944783292887045616641936

Public key e: 65537

Personal data for the certificate

Name: Smith

First name: Mary

Key identifier: Mary key (optional)

PIN: xxxxxxxxxxxx

PIN verification: xxxxxxxxxxxx

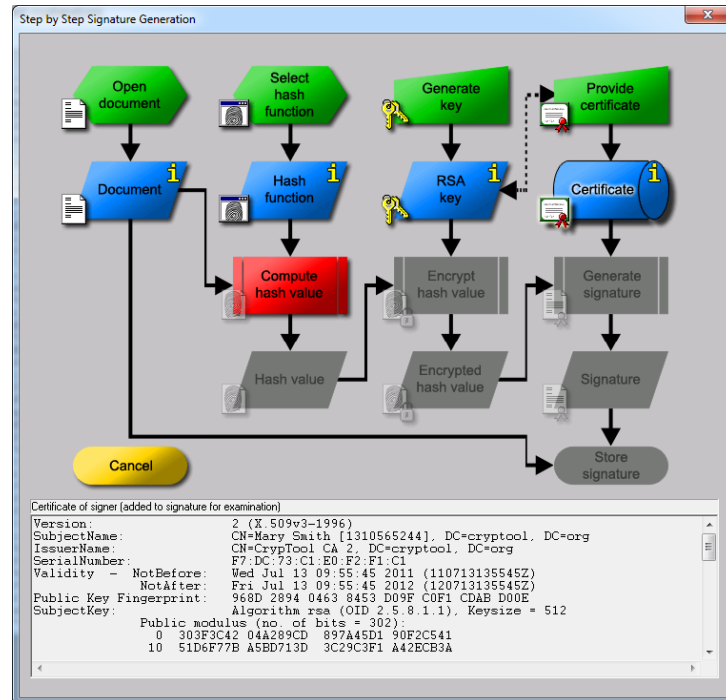
Generated names for PSE and certificate

User Key ID: [Smith][Mary][RSA-304][1310565244][Mary key]

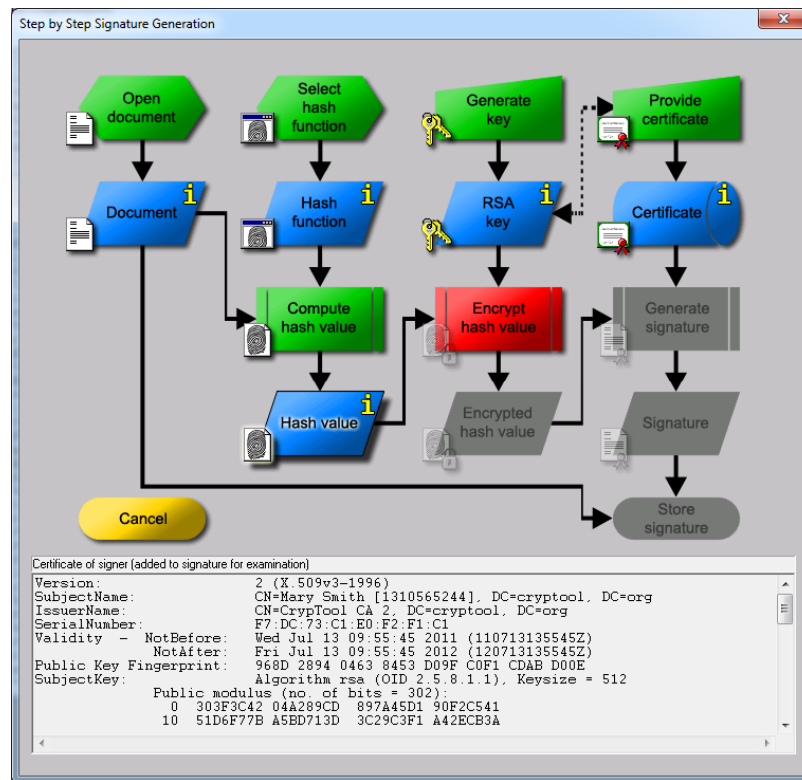
Distinguished Name: CN=Mary Smith [1310565244], DC=cryptool, DC=org

Create Certificate and PSE Import certificate and key Cancel

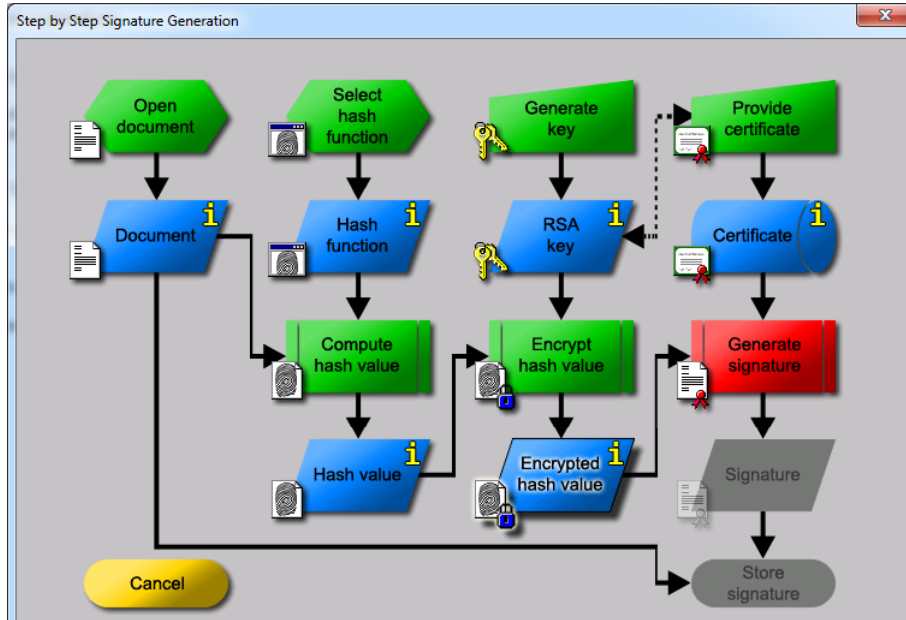
7. Nhấn nút “Create Certificate and PSE”.



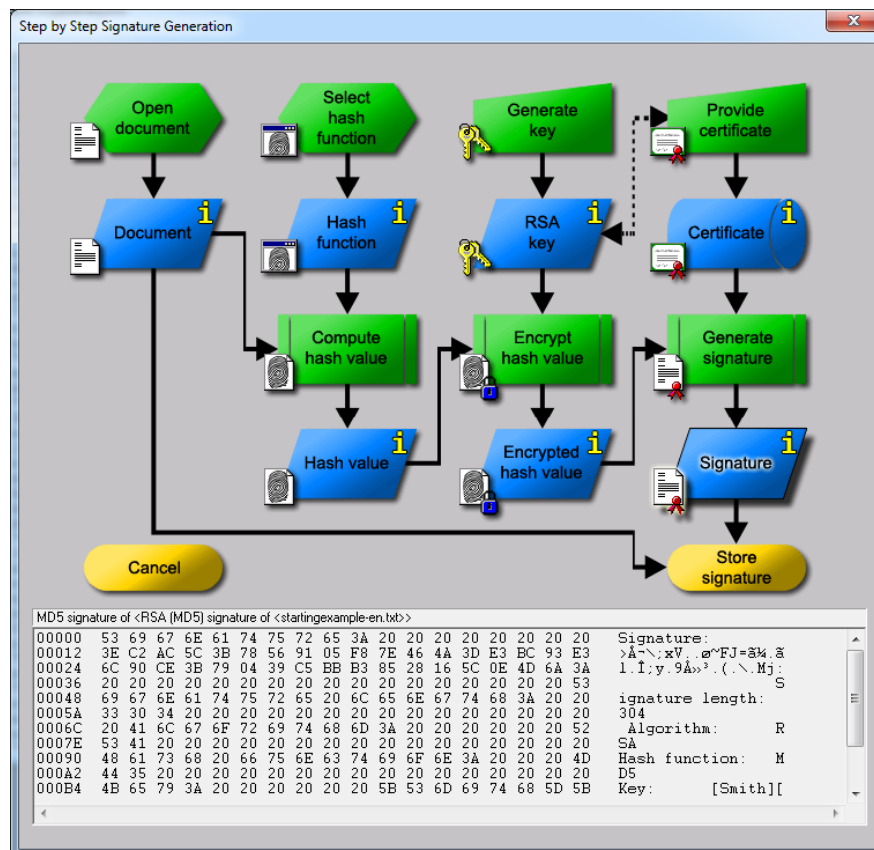
8. Chọn “Compute hash value”.



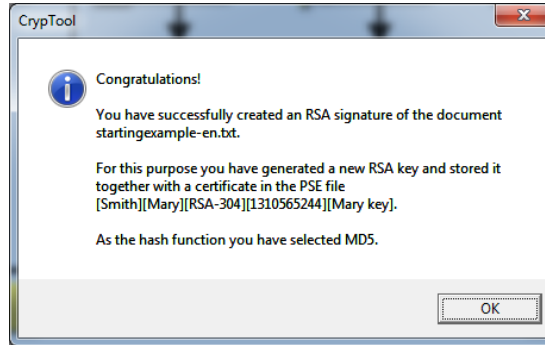
9. Chọn “Encrypt hash value”.



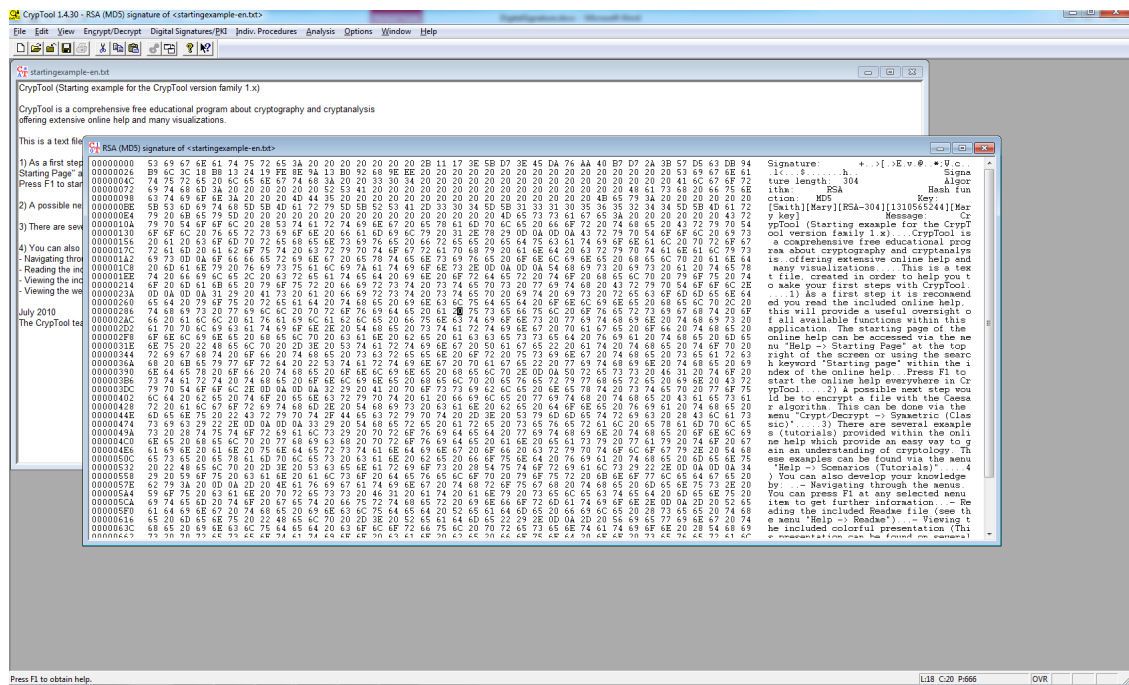
10. Chọn “Generate signature”.



11. Chọn “Store signature”.



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



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

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?

tranh chấp nào?

-HẾT-