

DFSC1316: Digital Forensic and Information Assurance I

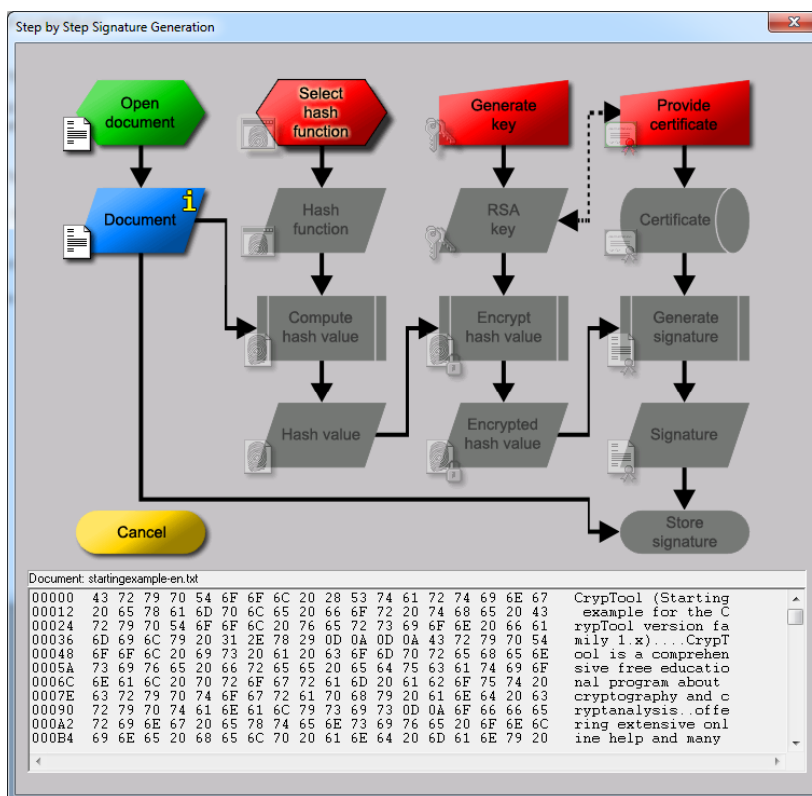
Lab 4 Digital Signature

In this lab, you will go through how digital signature works with a visual demonstration. The overall system is based on Hash algorithm and public key cryptography.

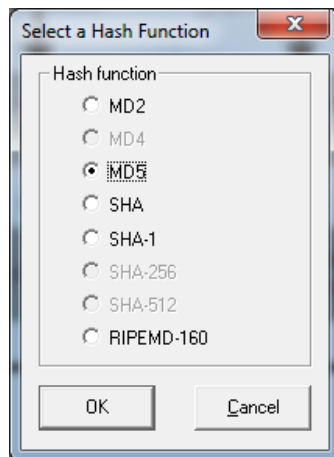
Similar to signature in the real world, digital signature is used to digitally “sign” a document. The signed document provides authenticity – no one can forge the signature except the private key owner, and non-repudiation – signer cannot deny that he/she has signed the document.

Digital signature is also of great value to digital forensics, because it technically identifies the ownership of a digital document.

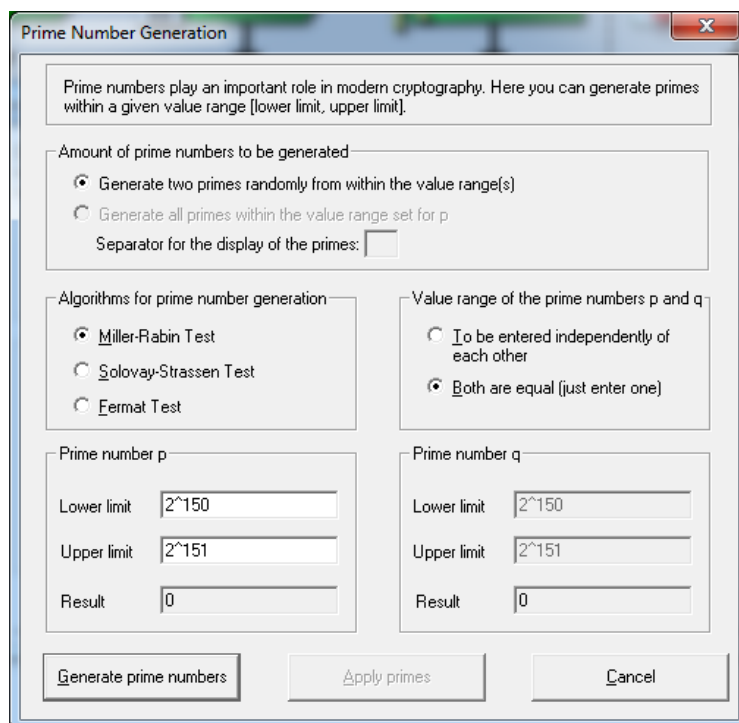
1. Select from menu of CrypTool “**Digital Signatures/PKI**” \ “**Signature Demonstration (Signature Generation)**”



2. Click on “**Select hash function**”. Choose **MD5** (or others) and click **OK**.



3. Click **“Generate Key”** and **“Generate prime numbers”** in **step by step Signature Generation** dialog.
 (Note: we did not explain the details of public cryptography algorithm in class. The whole system is based on, or start with, two very large prime numbers. And here this program is to generate two such numbers, and then the public-private key pair).



4. Enter **2¹⁵⁰** as the lower limit and **2¹⁵¹** as upper limit. And click **Generate prime numbers** and **apply primes**.

Generate RSA Key

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

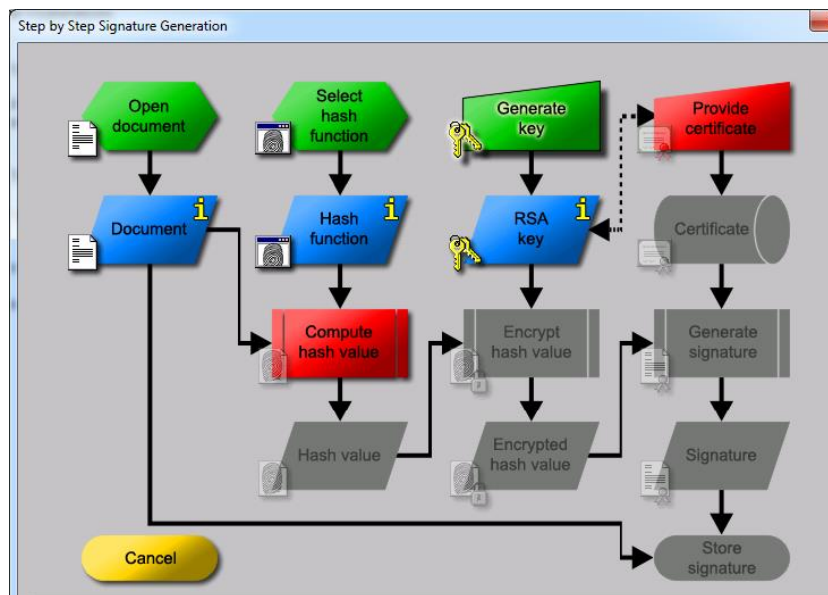
RSA modulus N (public)

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

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

Private key d

5. Click **Store key** button.



6. Click **Provide certificate** button. Enter

Name: **Smith**

First name: **Mary**

Key identifier: **Mary key**

PIN: **cryptool**

PIN verification: **cryptool**

Create Certificate and PSE

Public RSA parameter

Bit length: 304 bit

RSA modulus N: 61425563540125238857993543215982771994478329288704561664193

Public key e: 65537

Personal data for the certificate

Name: Smith

First name: Mary

Key identifier: Mary key (optional)

PIN: xxxxxxxx

PIN verification: xxxxxxxx

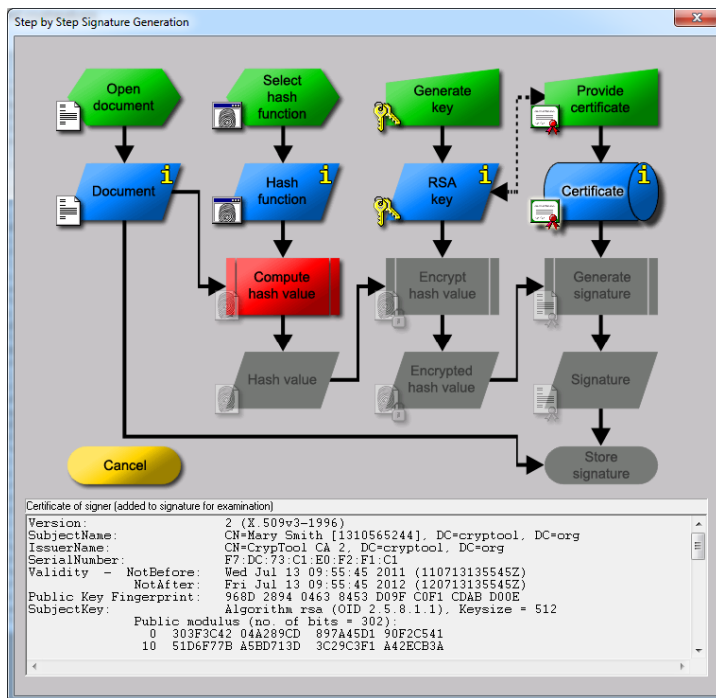
Generated names for PSE and certificate

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

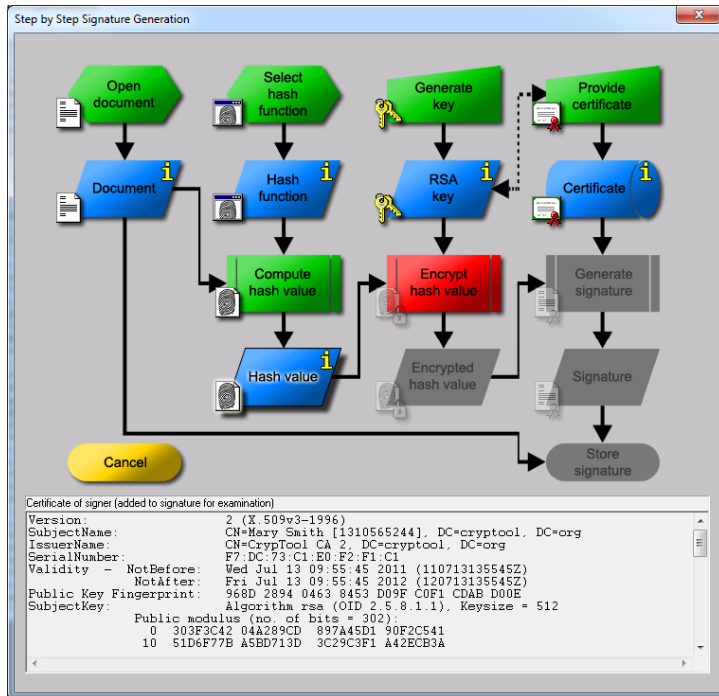
Distinguished Name: CN=Mary Smith [1310565244], DC=cryptool, DC=org

Create Certificate and PSE Import certificate and key Cancel

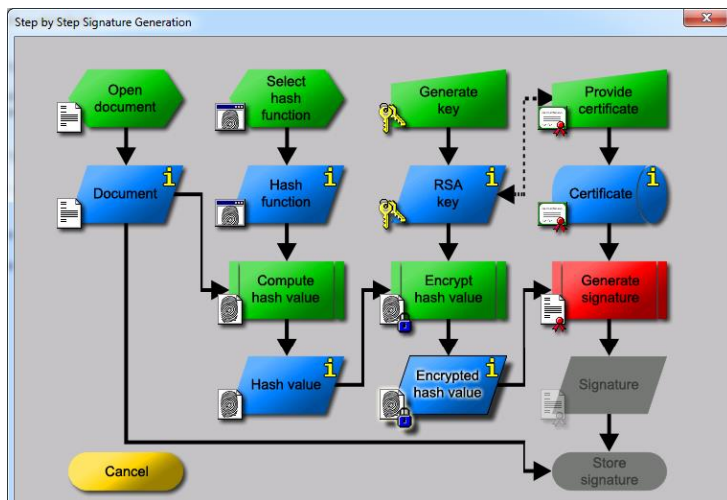
7. And click “Create Certificate and PSE”.



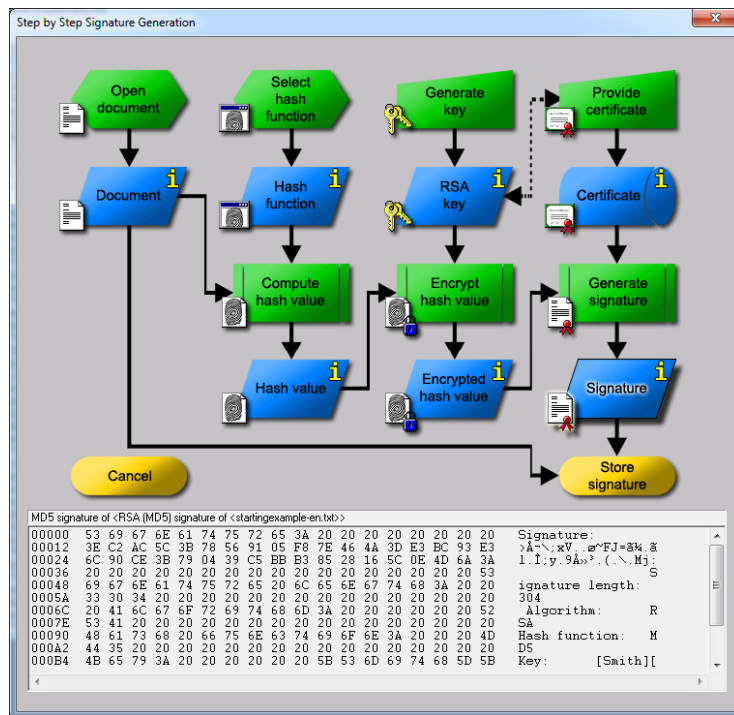
8. click “Compute hash value”.



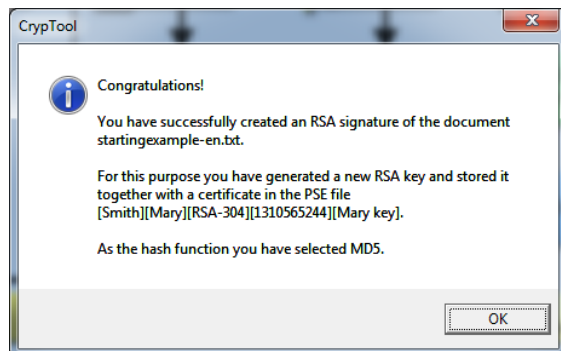
9. Click “Encrypt hash value”.



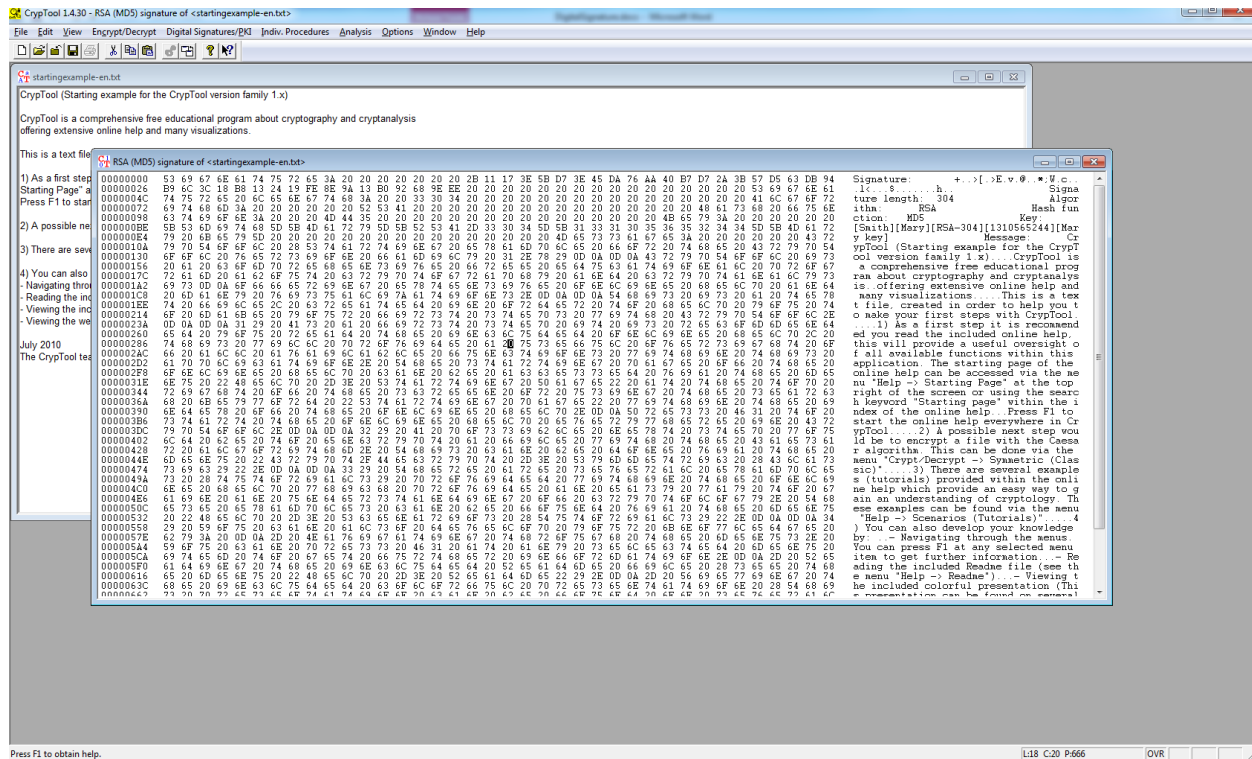
10. Click “Generate signature”.



11. Click “Store signature”.



12 click “OK”, you will see RSA (md5)signature of <startingexample-en.txt>.



Question (120 pts total) :

In the above demonstration, except the “Open Document” and “Document” block, there are totally 12 function blocks. For each of these 12 function blocks, explain the following:

1. What is the function provided by this block. For example, for a function block, you could explain what is the input, what is the output, and how the input is transformed to the output.
2. Why do we need this function block for this digital signature application?

(we mentioned *certificate* in class, but did not touch details. You will need to do some online search to find how *certificate* works.)