DFSC1316: Digital Forensic and Information Assurance I

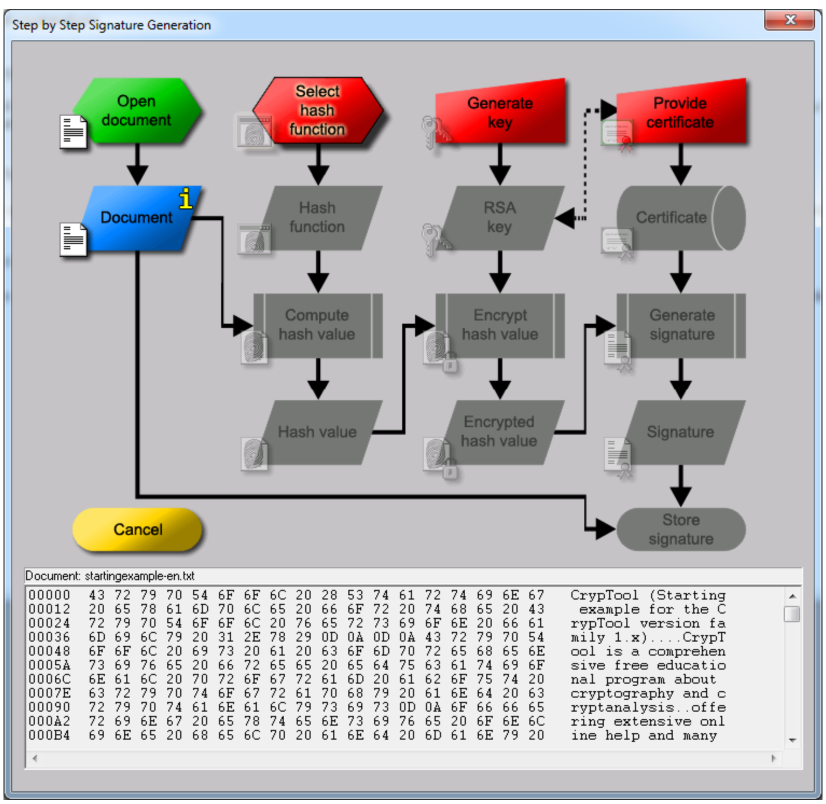
Lab 4 Digital Signature

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.

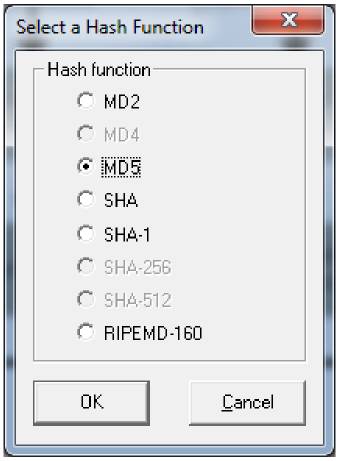
Similar to signature in the real world, digital signature is used to digitally “sign” a document. The signed document provides authenticity – no one can forge the signature except the private key owner, and non-repudiation – signer cannot deny that he/she has signed the document.

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

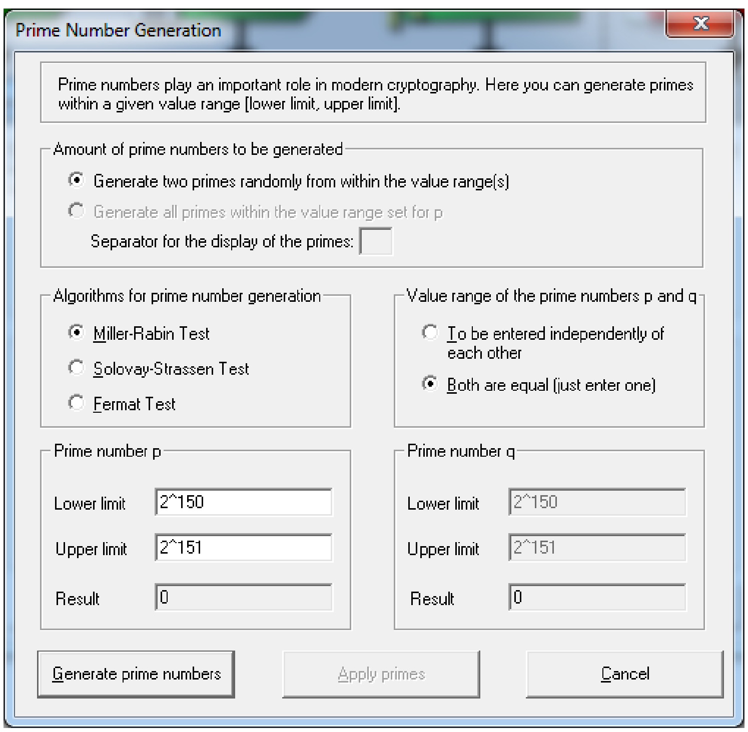
1. Select from menu of CrypTool “**Digital Signatures/PKI” \ “Signature Demonstration (Signature Generation)**”



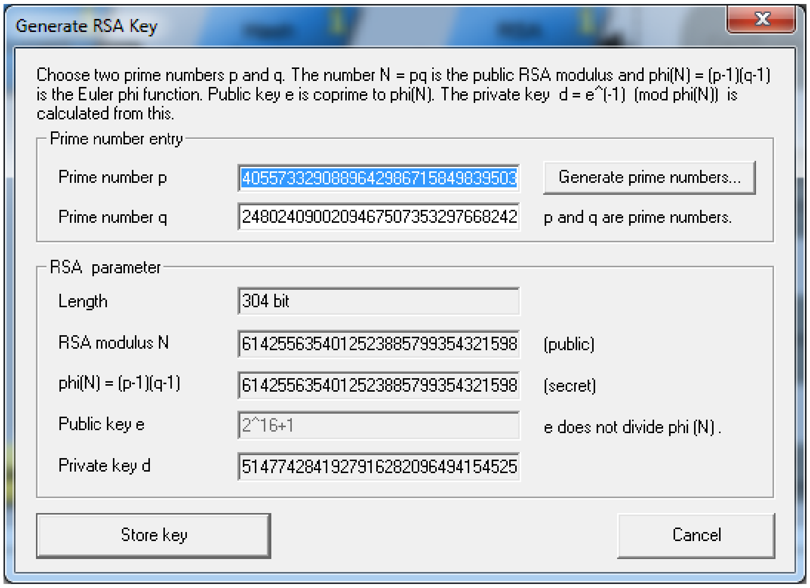
2. Click on “**Select hash function**”. Choose **MD5** (or others) and click **OK**.



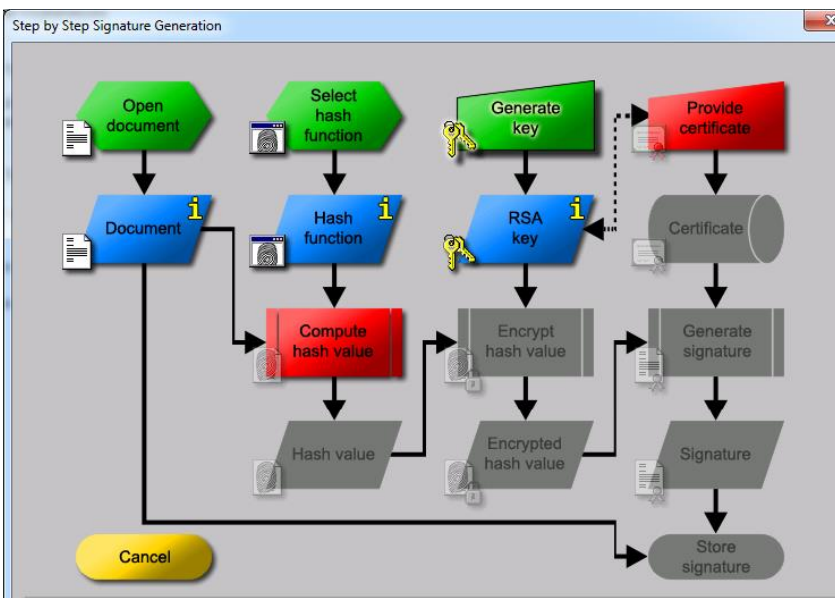
3. Click “**Generate Key**” and “**Generate prime numbers**” in **step by step Signature Generation** dialog. (Note: we did not explain the details of public cryptography algorithm in class. The whole system is based on, or start with, two very large prime numbers. And here this program is to generate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



4. Enter **2^150** as the <u>lower limit</u> and **2^151** as <u>upper limit</u>. And click **Generate prime numbers** and **apply primes**.



5. Click **Store key** button.



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

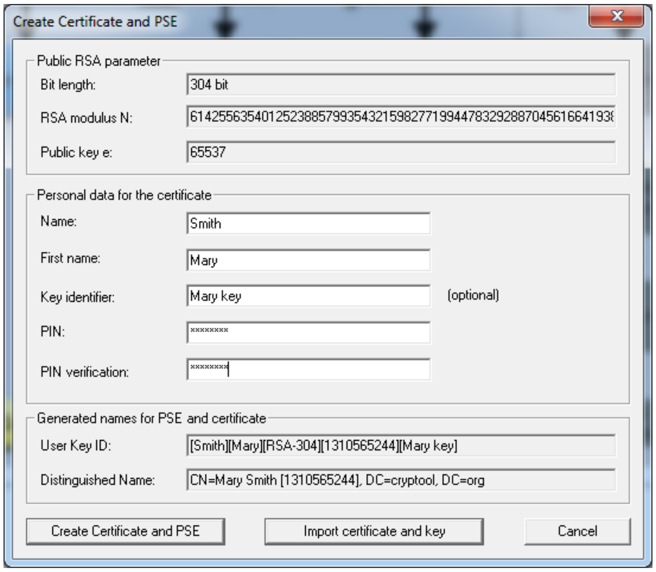
Name: **Smith**

First name: **Mary**

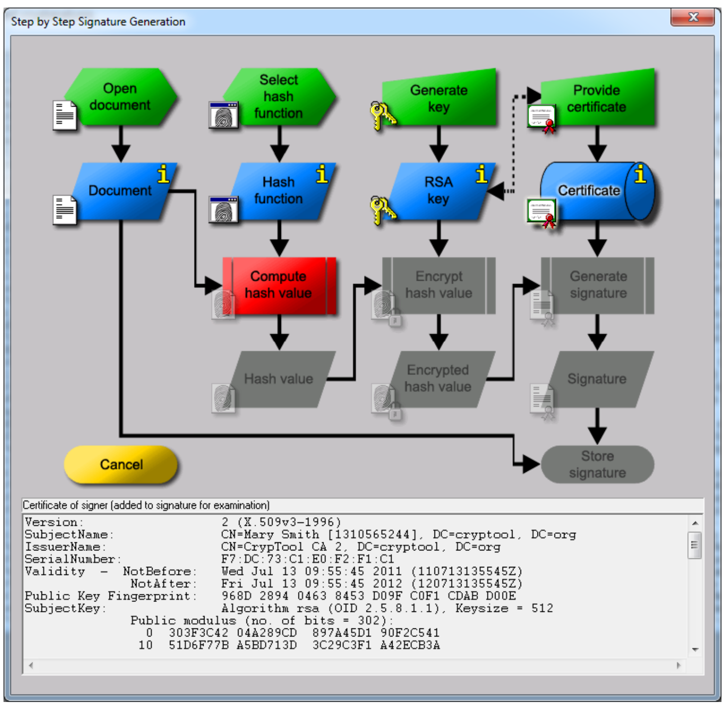
Key identifier: **Mary key**

PIN: **cryptool**

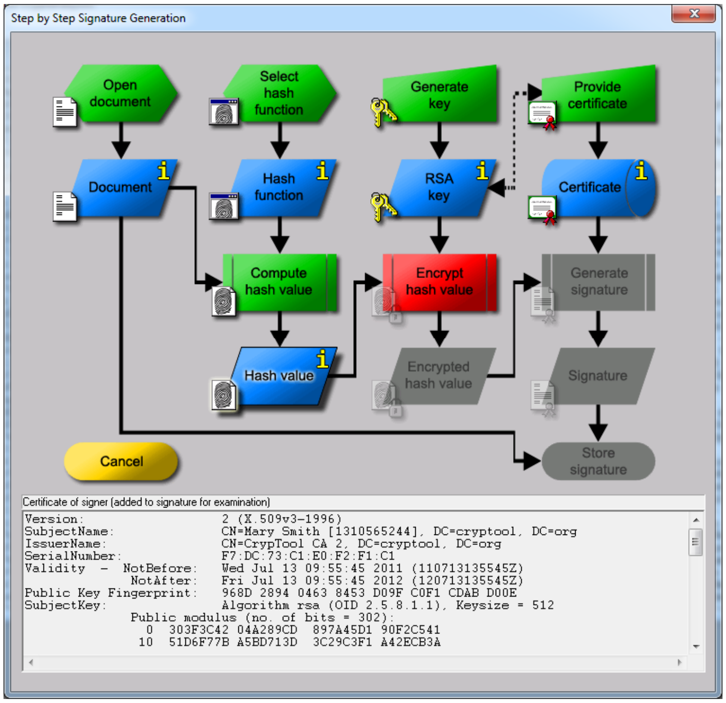
PIN verification: **cryptool**



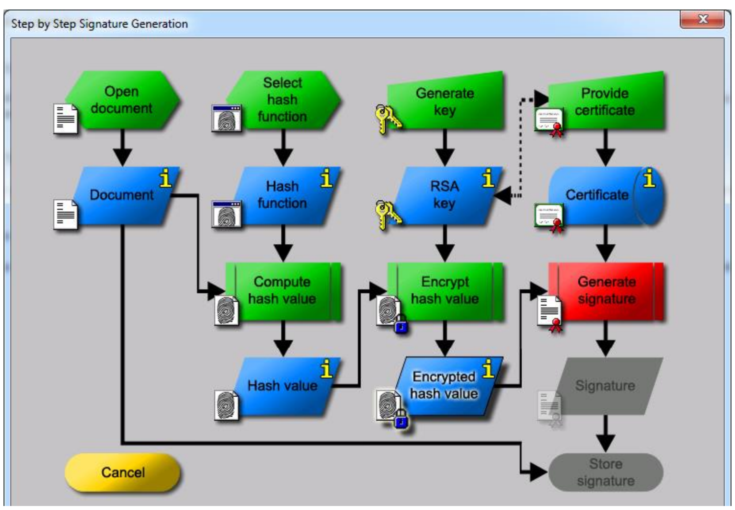
7. And click “**Create Certificate and PSE**”.



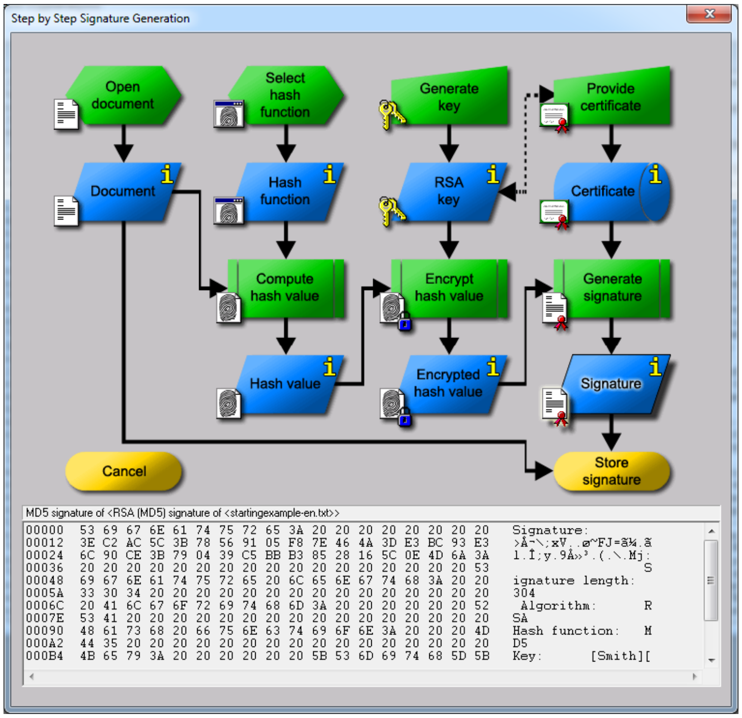
8. click “**Compute hash value**”.



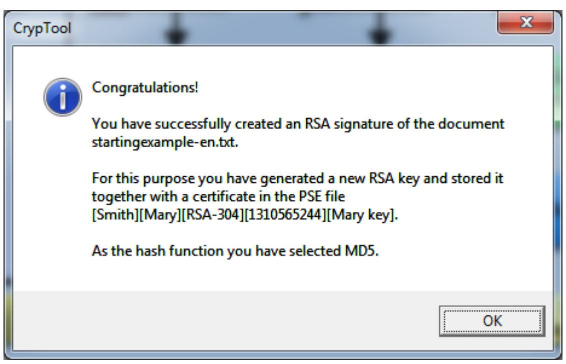
9. Click “**Encrypt hash value**”.



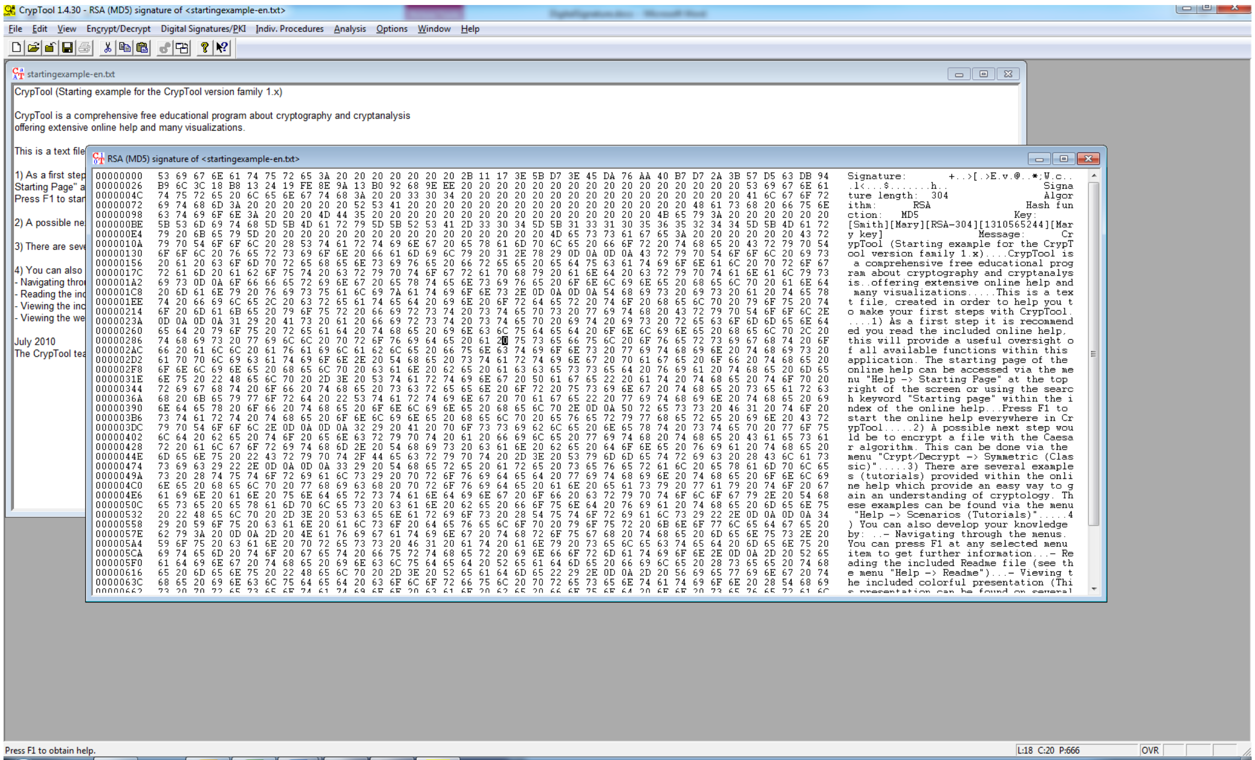
10. Click “**Generate signature**”.



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.)