4.1 Lab on Digital Signature Visualization

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.
4. Enter $2^{150}$ as the lower limit and $2^{151}$ as upper limit. 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>. 