CIPHERS

About:
The objective of this lab is to get students to understand some of the main concepts in cryptography, which are:

demonstration of **digital signature**

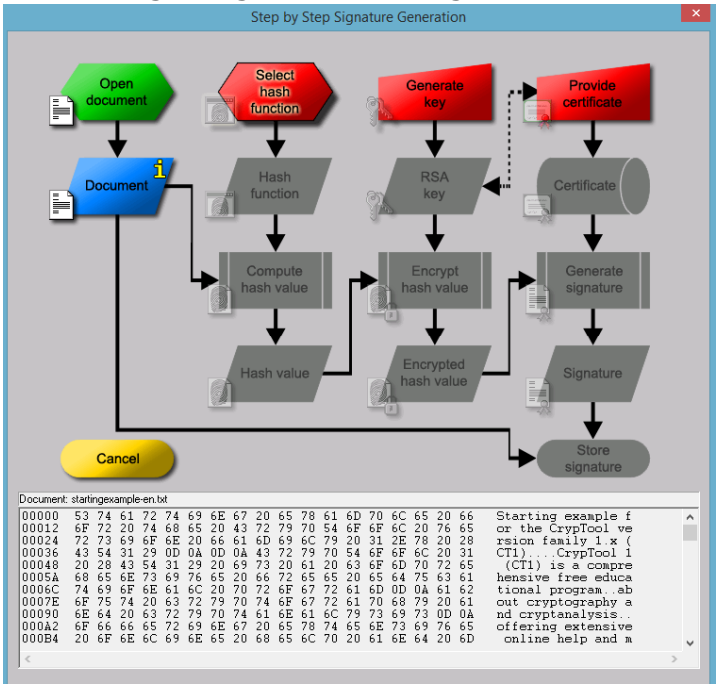
Prerequisites:
Install cryptool 1 from https://www.cryptool.org/en/ct1/

ASSIGNMENT SEVEN

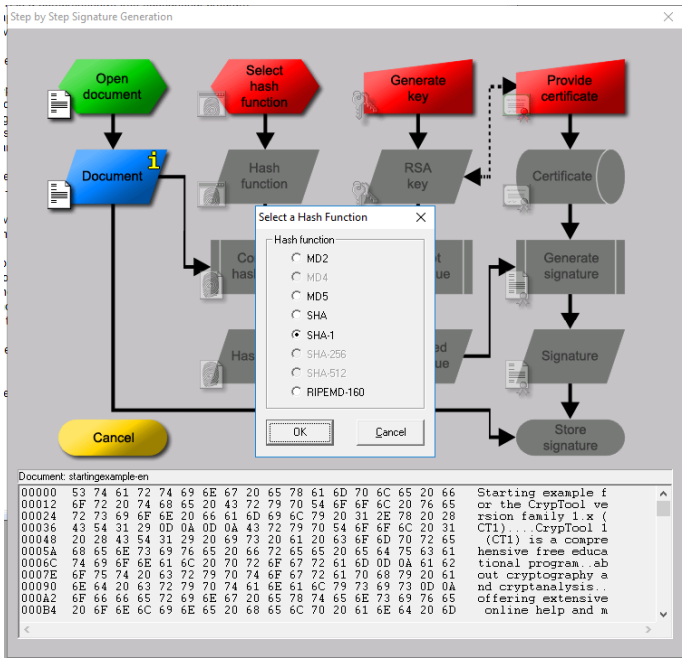
Exercise • 1: (1 POINT)

A digital signature added to a document shows the sender's identity. It can also provide non-repudiation. The sender cannot deny sending the document, only the sender has that digital signature. Digital signatures are created through multiple steps. We need to understand all the steps that must be performed before a digital signature can be generated.

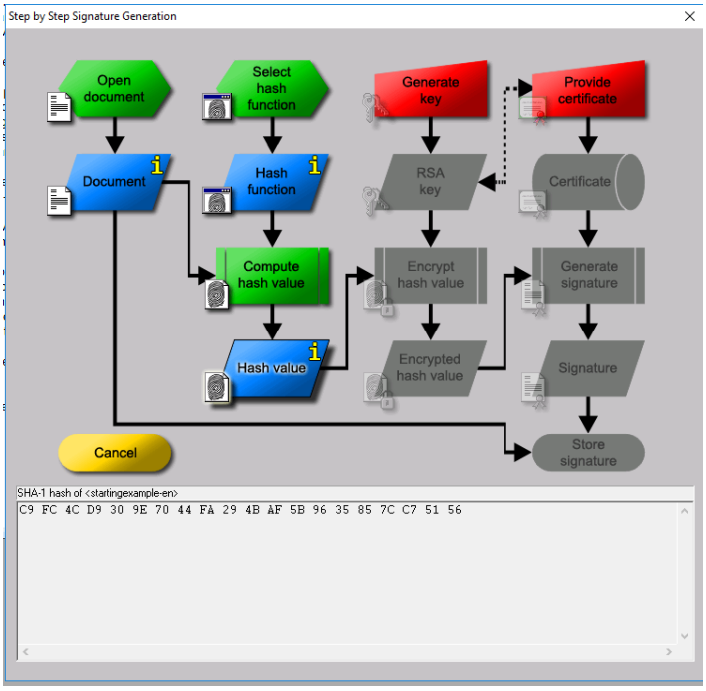
1. Click on Digital Signatures/PKI>Signature Demonstration.

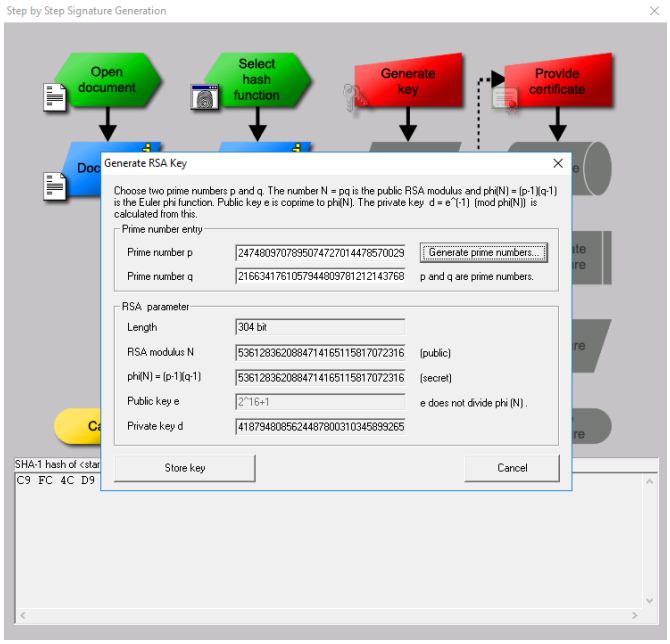


2. First we need to generate a hash value of the document. To generate it, we need to select a hashing algorithm, select SHA-1.

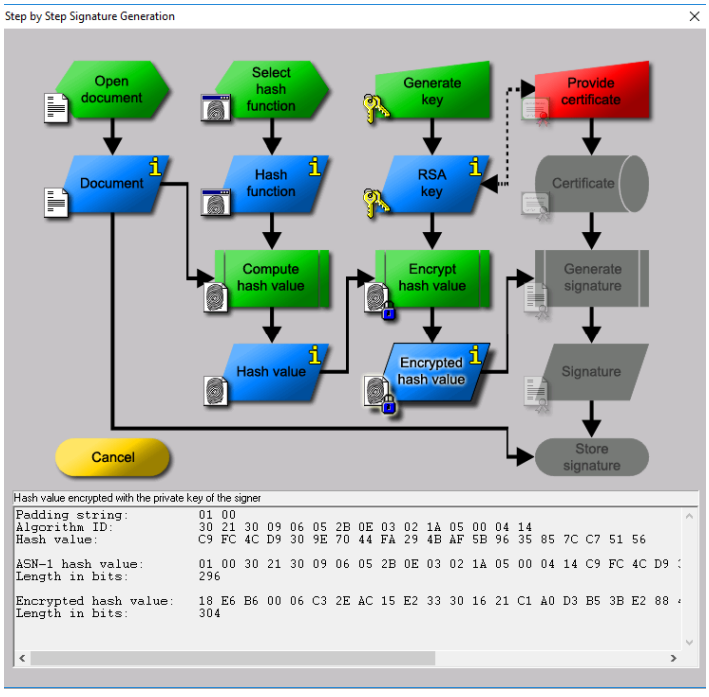


3. Next, generate a key pair. We'll generate RSA keys.

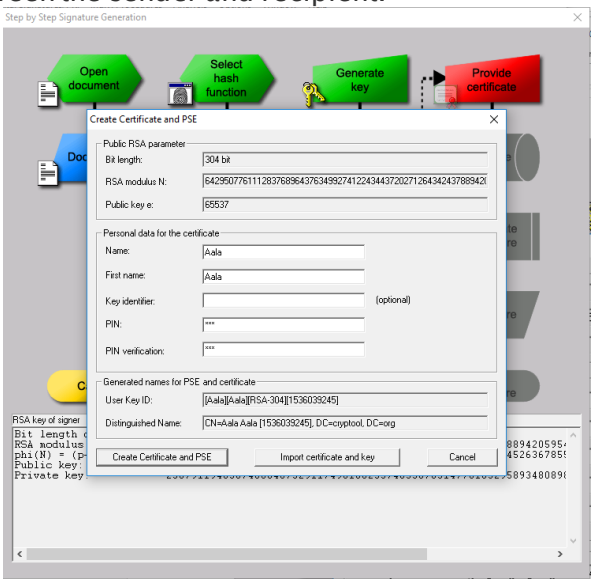




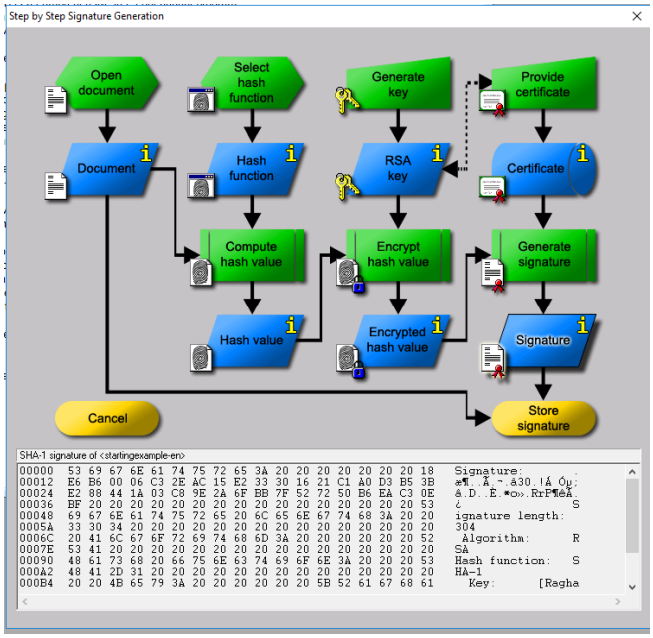
4. After successfully generating keys, encrypt the hash value generated earlier.



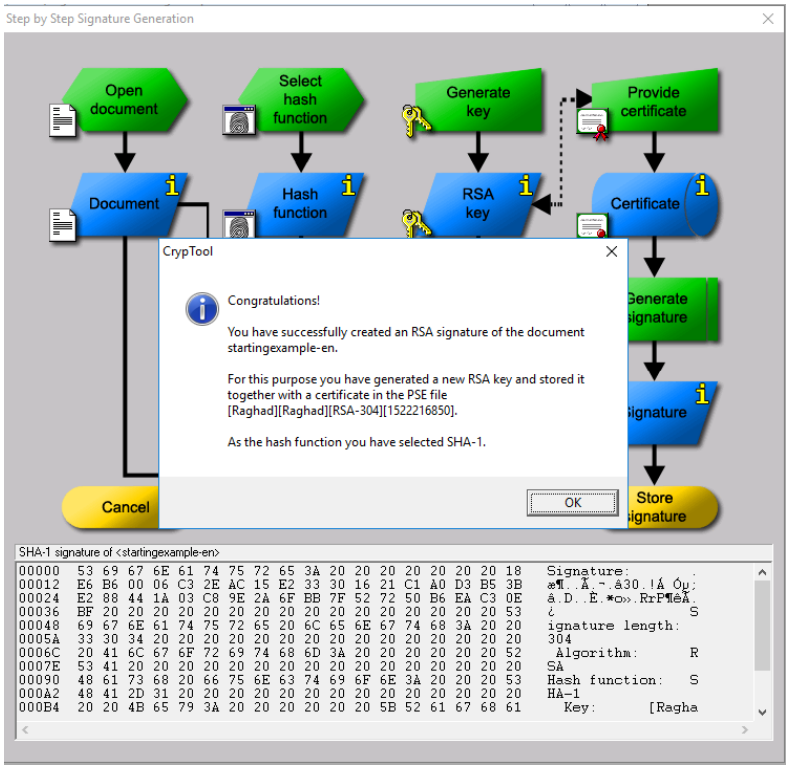
1. We need to create a certificate associated with the RSA key. Press on “Provide Certificate” and fill your information. Then click on “create certificate.” It’ll be used for communication between the sender and recipient.



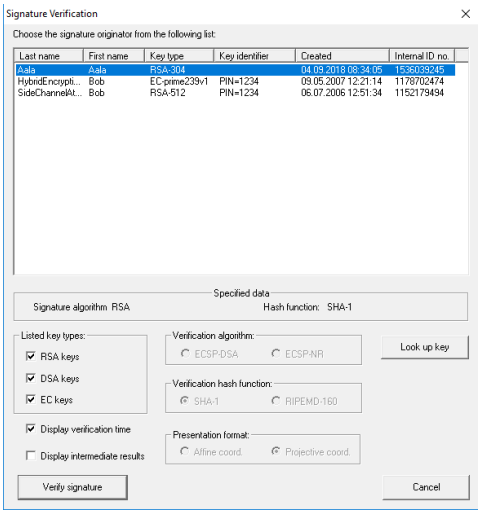
2. Click on create certificate and PSE.
3. Click on Generate Signature.

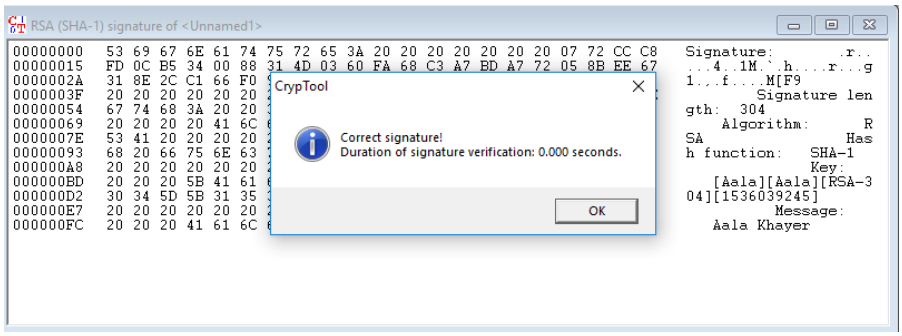


4. Click store signature.



a. Verify the signature using Cryptool.
Digital Signatures/PKI → Verify Signature.




RSA (SHA-1) signature of <Unnamed1>
00000000 53 69 67 6E 61 74 75 72 65 3A 20 20 20 20 20 20 07 72 CC C8
00000015 FD 0C B5 34 00 88 31 4D 03 60 FA 68 C3 A7 BD A7 72 05 8B EE 67
0000002A 31 8E 2C C1 66 F0
0000003F 20 20 20 20 20 20
00000054 67 74 68 3A 20 20
00000069 20 20 20 20 41 6C
0000007E 53 41 20 20 20 20
00000093 68 20 66 75 6E 63
000000A8 20 20 20 20 20 20
000000BD 20 20 20 5B 41 61
000000D2 30 34 5D 5B 31 35
000000E7 20 20 20 20 20 20
000000FC 20 20 20 41 61 6C
Signature: .r..
...4..1M.`.h...r...g
1..,f...M[F9
Signature length: 304
Algorithm: RSA
Hash function: SHA-1
Key:
[Aala][Aala][RSA-304][1536039245]
Message:
Aala Khayer
CrypTool
Correct signature!
Duration of signature verification: 0.000 seconds.
OK