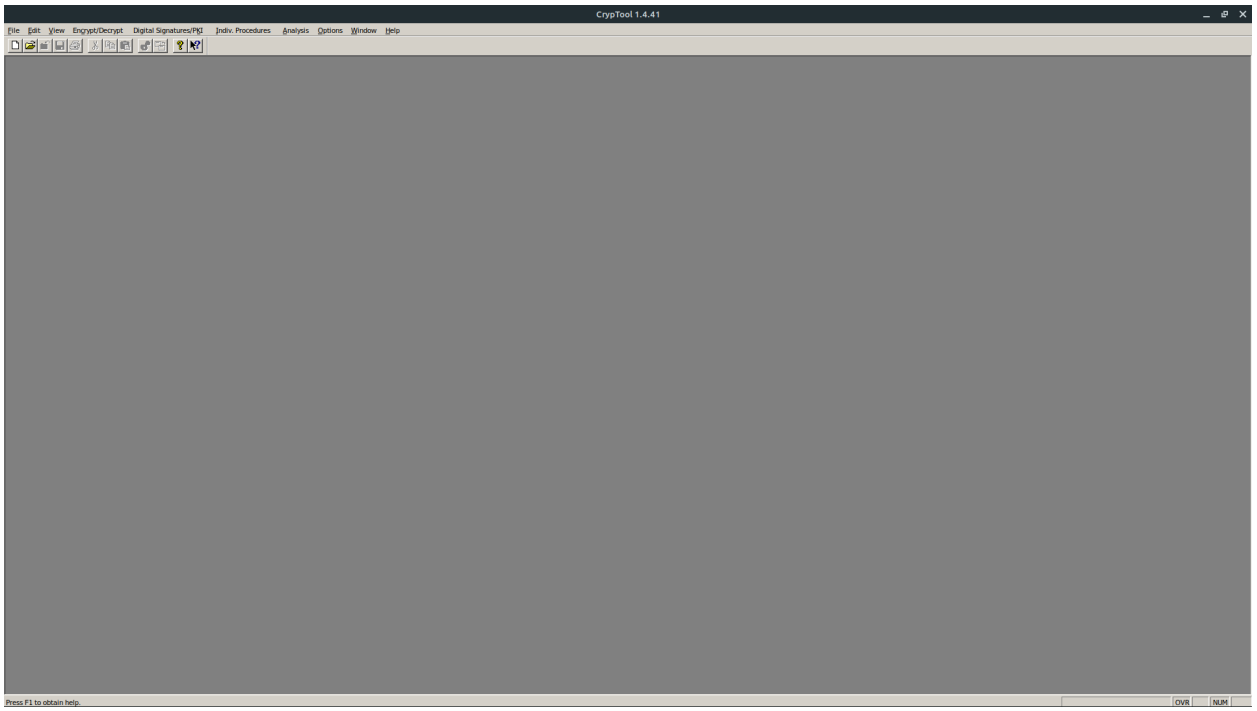
ID: 20180358
Name: Mohammad Ibrahim Abu-Amara
23112021202853

Information Systems Security
Assignment #2

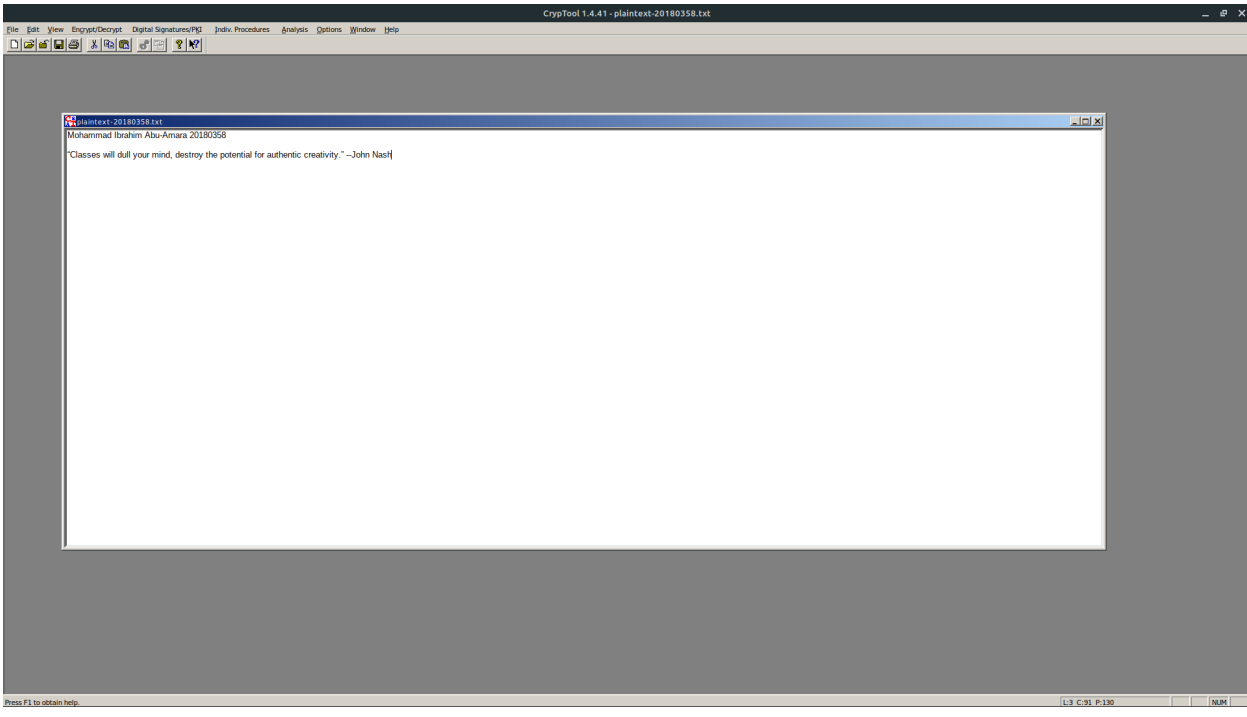
Question

a. OBJ

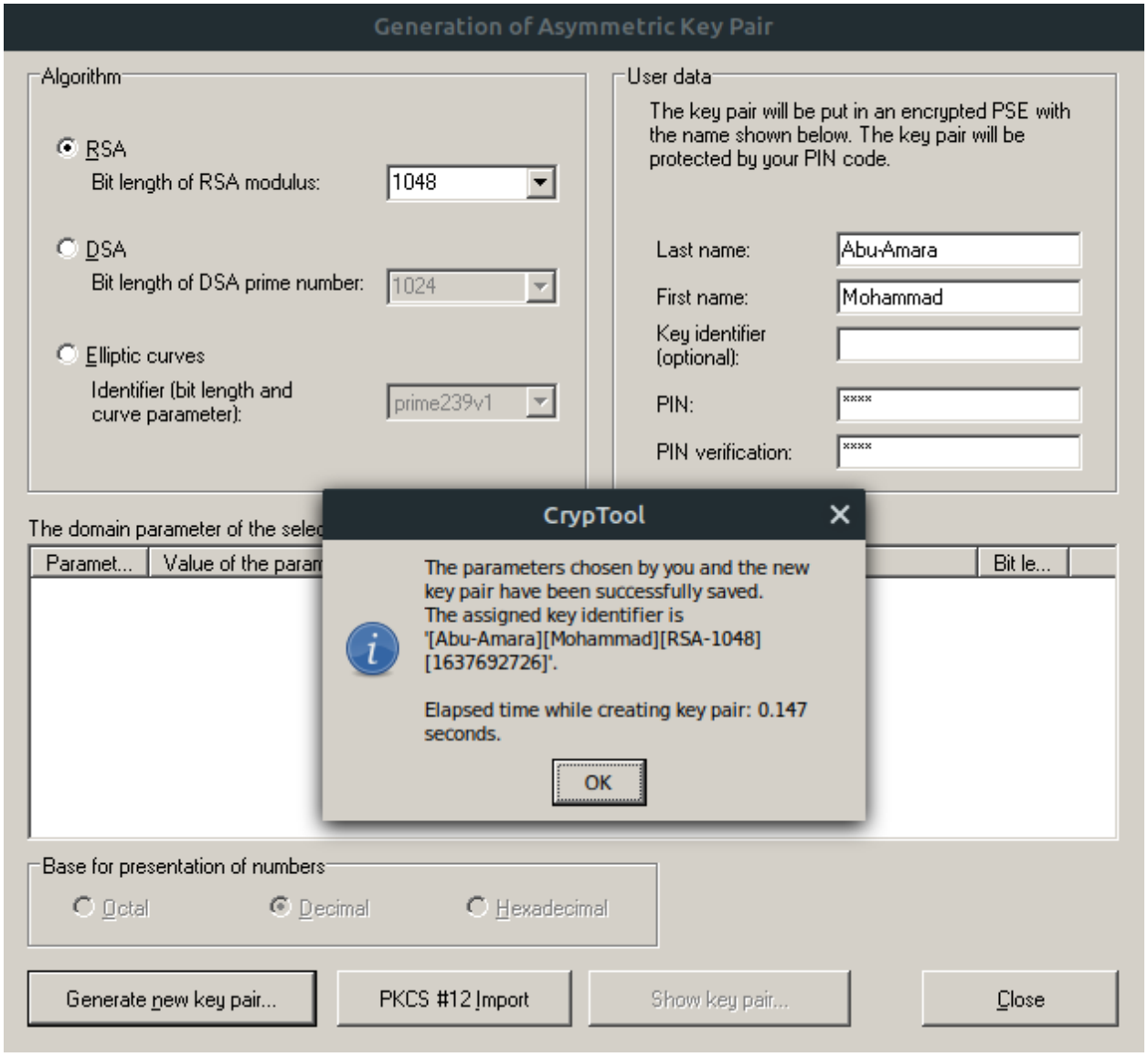
1. Run Cryptool



2. Prepare plaintext file

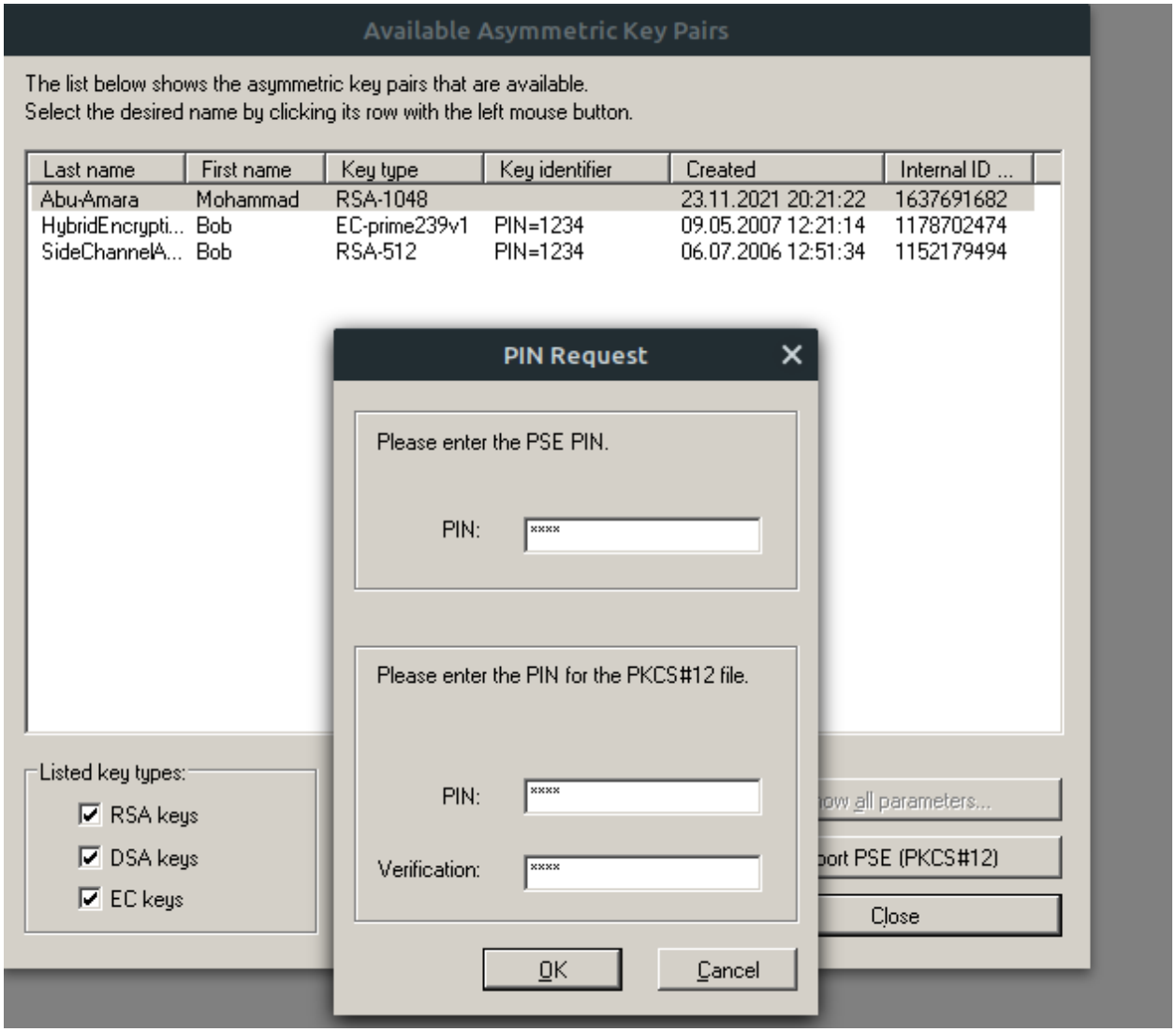


3. Generate RSA key pair



Here we put a PIN code in order **to protect** the keys, or in particular **the private key**.

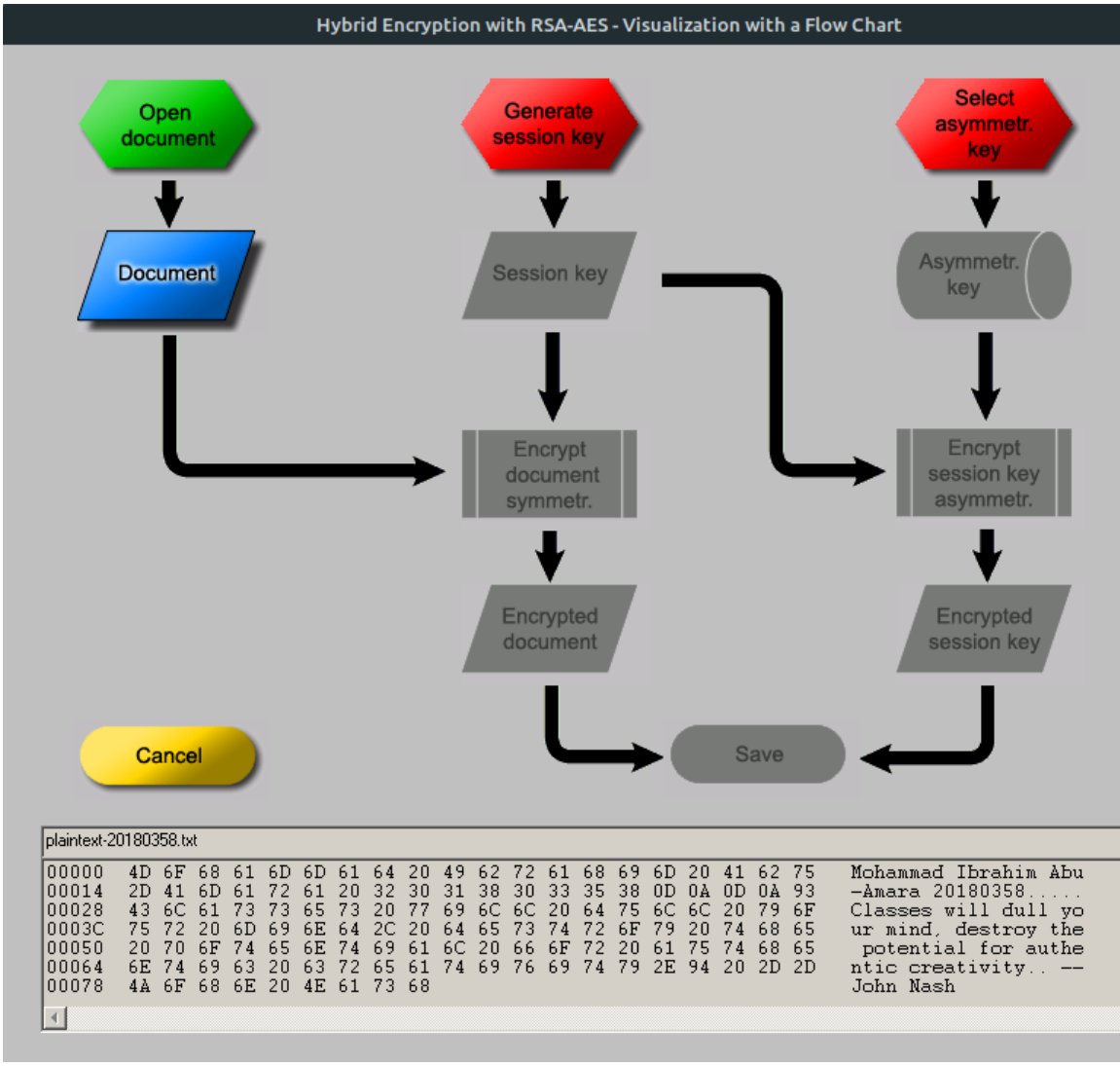
4. Export the key pair



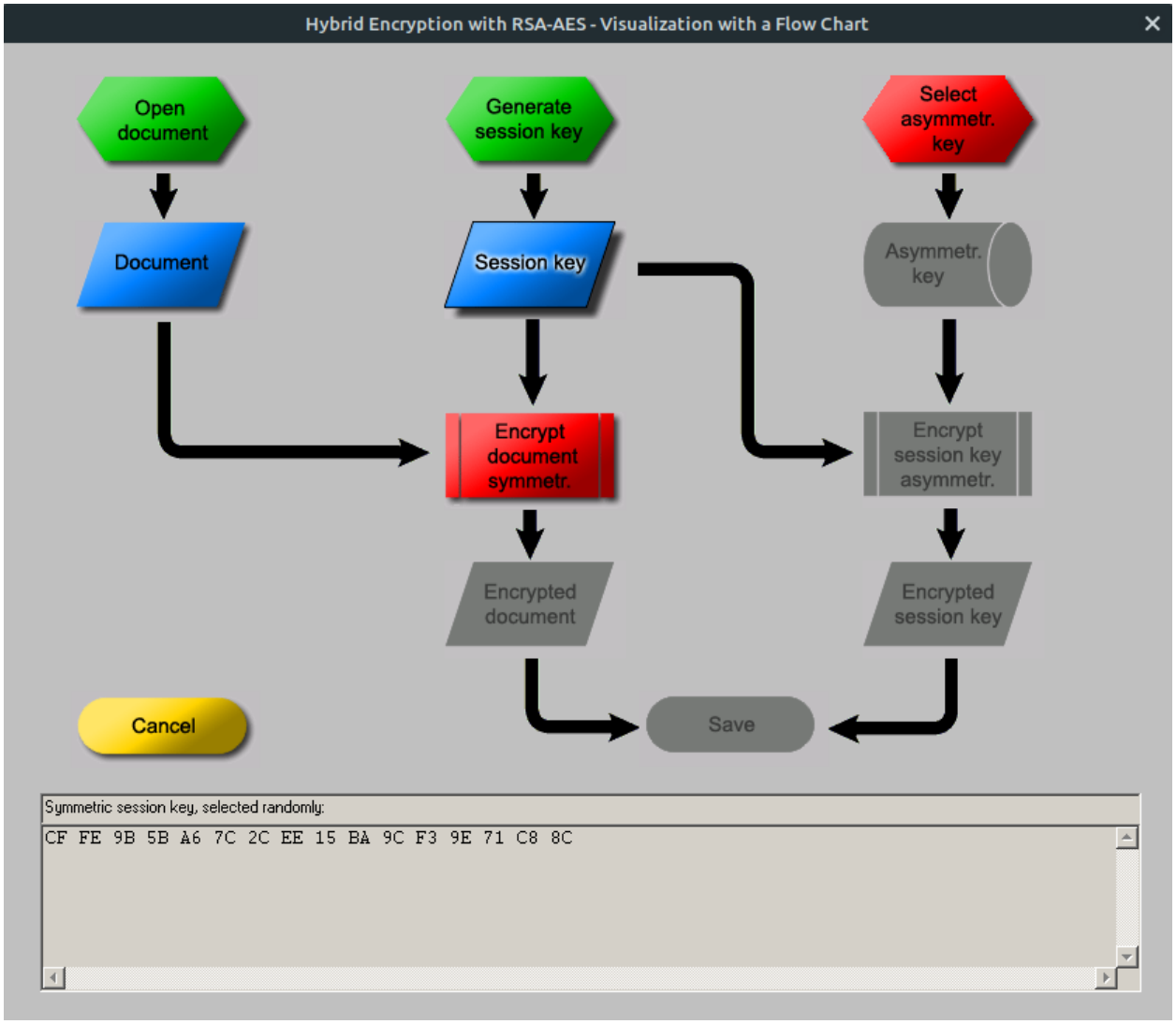
The first PIN is to access the key that we generated in the previous step, and the second PIN is for protecting the object file that the keys, the public key and the private key, will be stored in.

5.

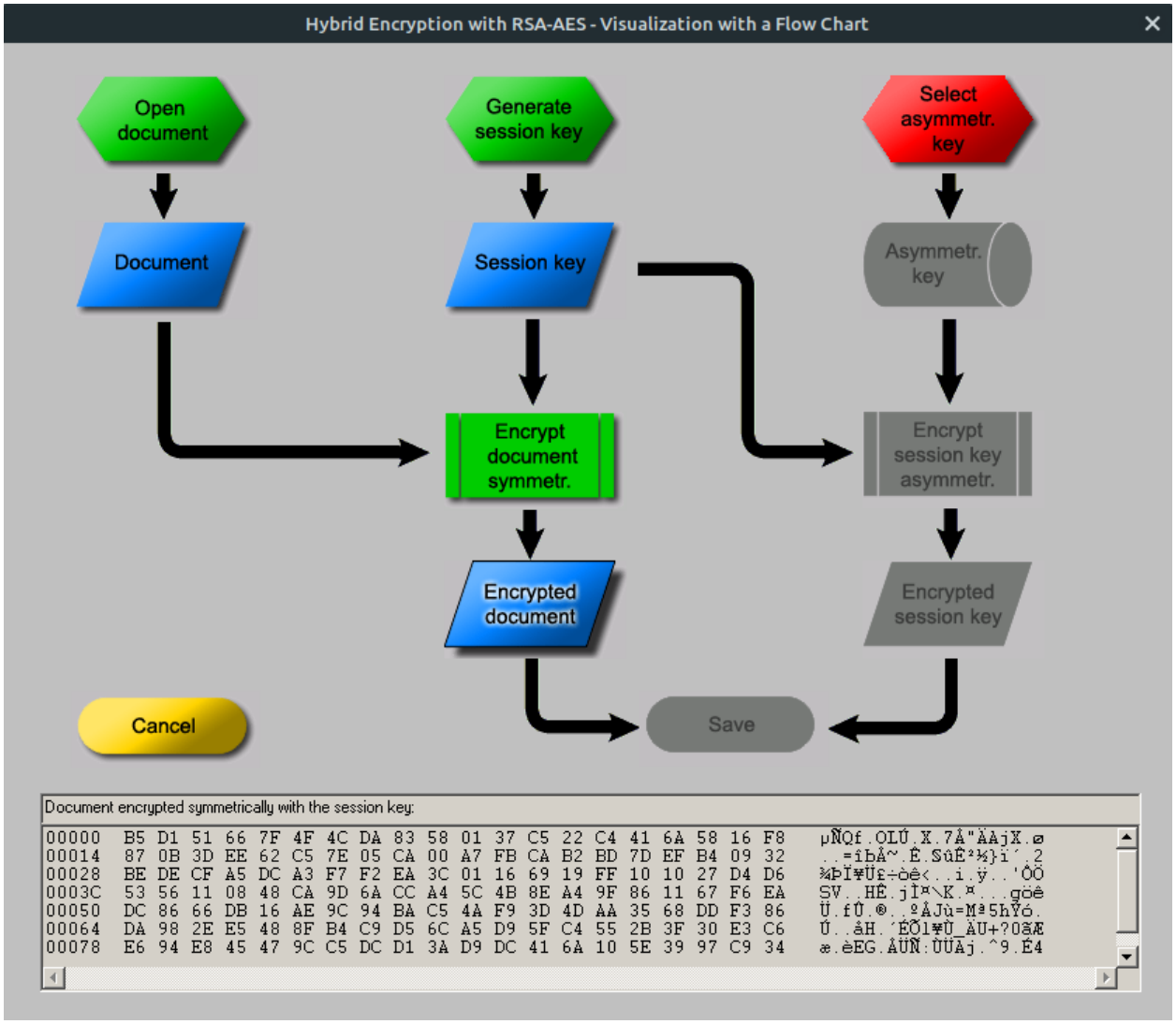
I. First we open the document for which we want to encrypt



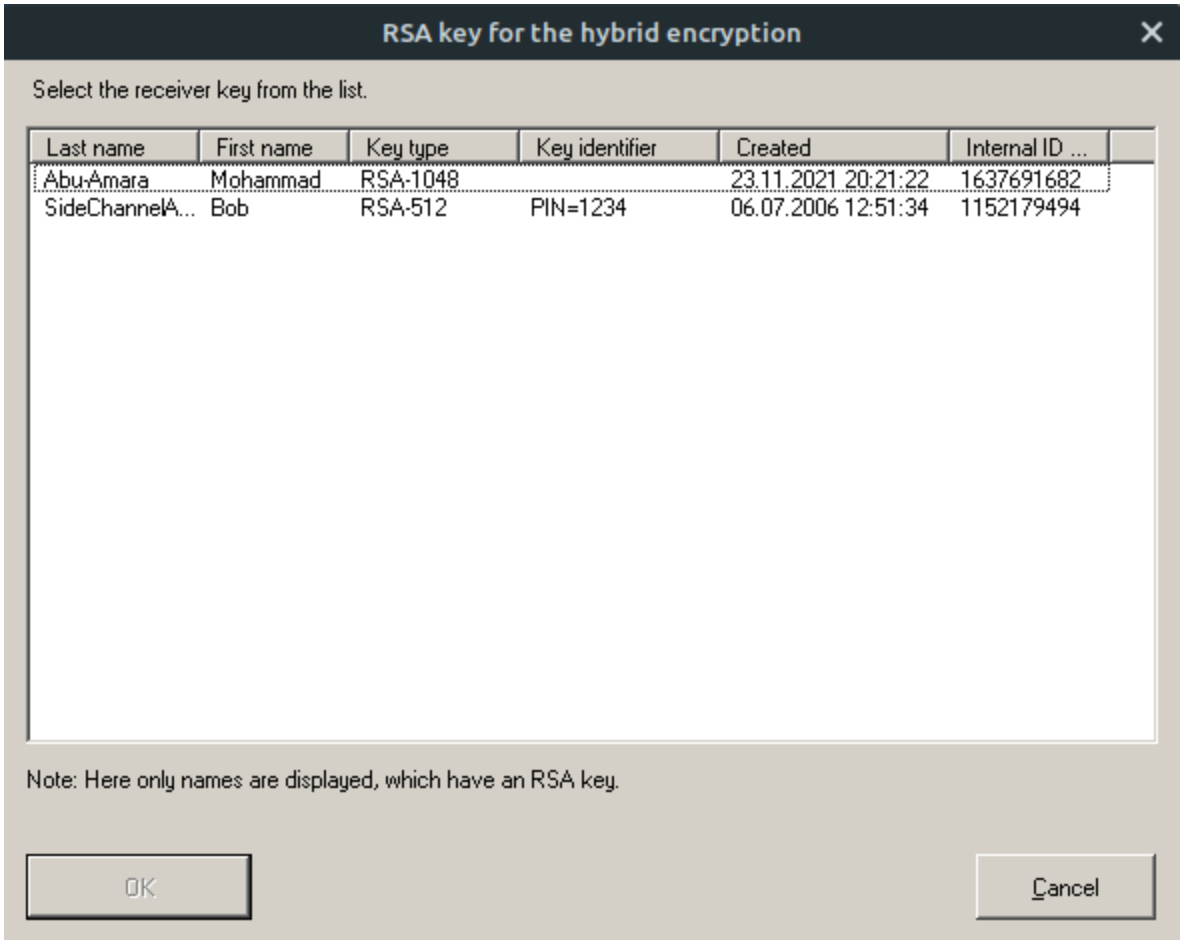
II. We generate the session key in order to secure the communication between two parties



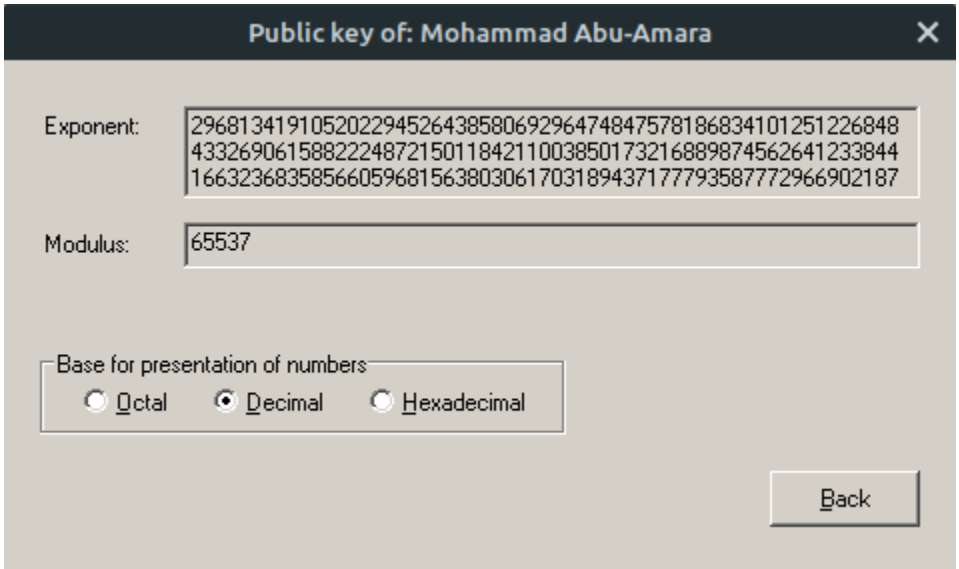
III. Then we encrypt the selected document using the generated session key (symmetric key)



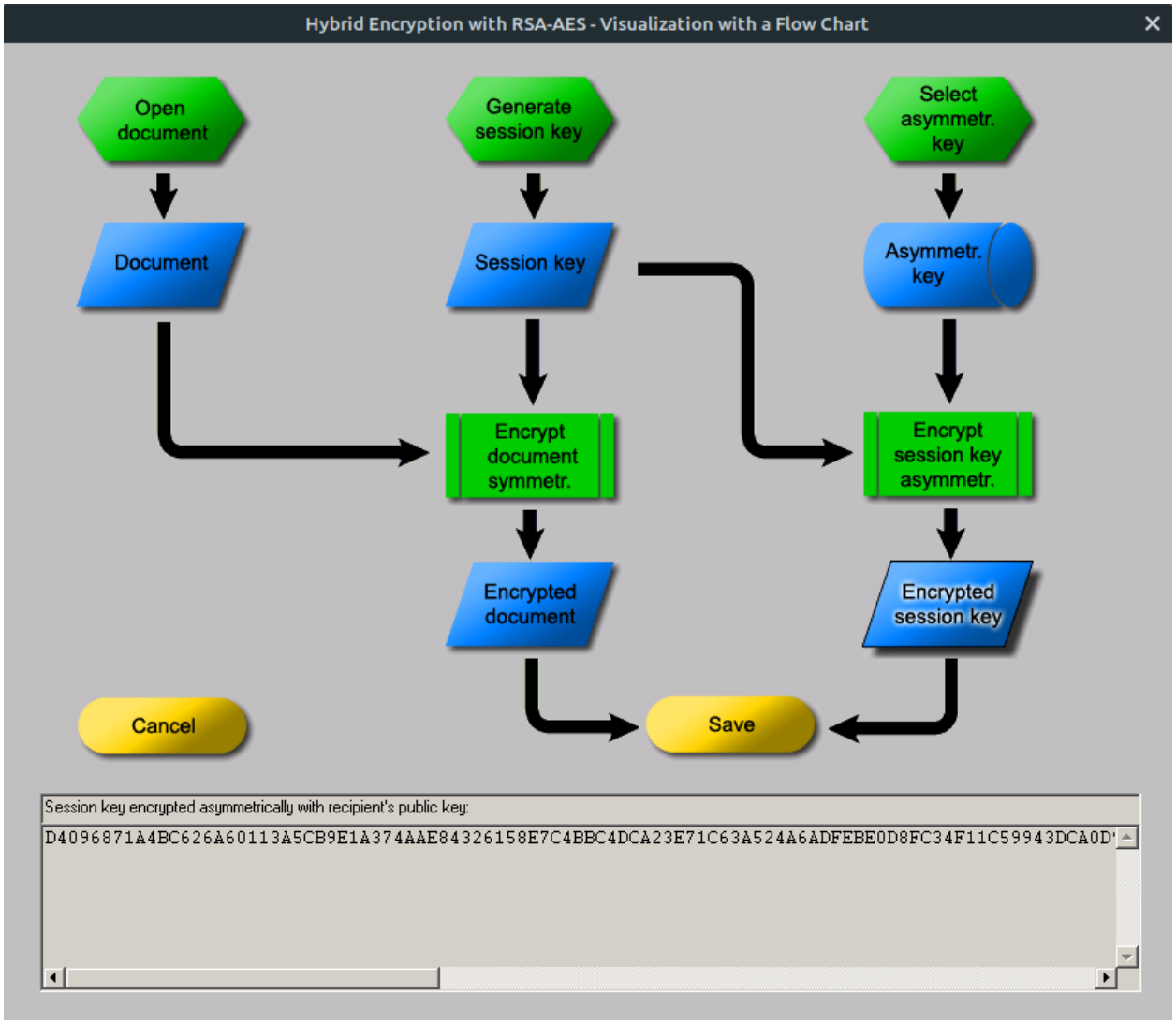
IV. Then we choose our generated private key (asymmetric key)

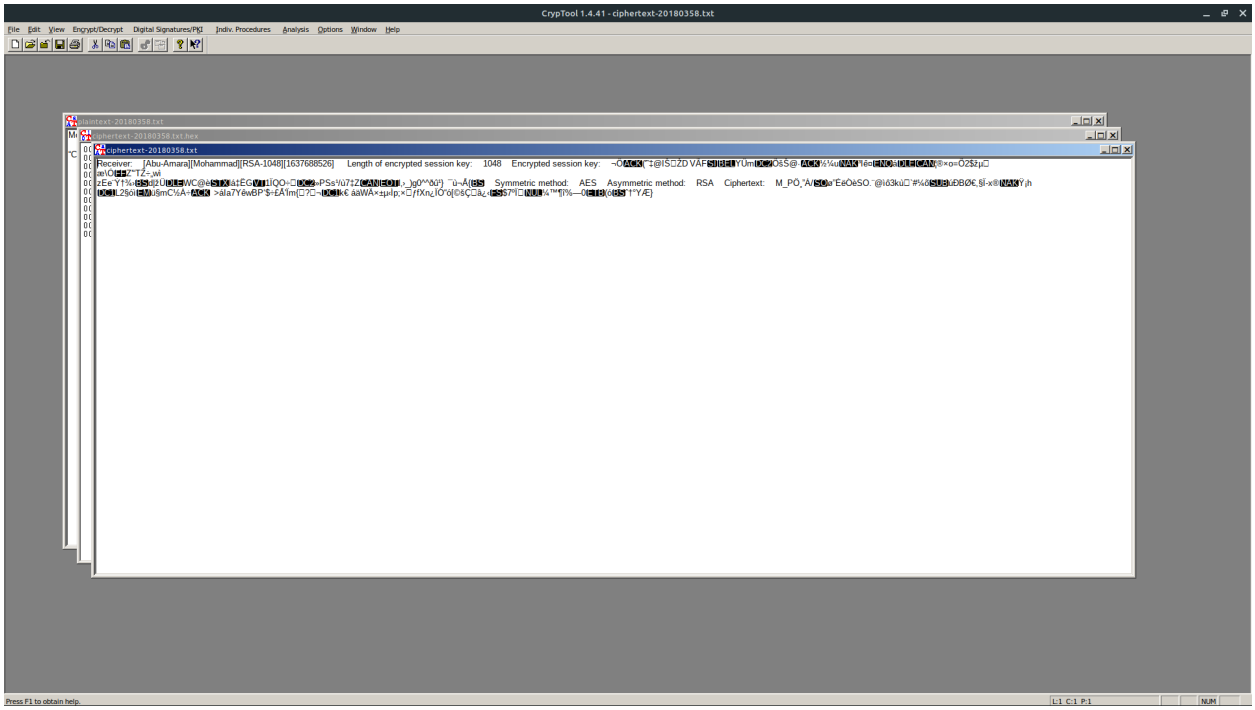


V. Using the private key, we encrypt the public key



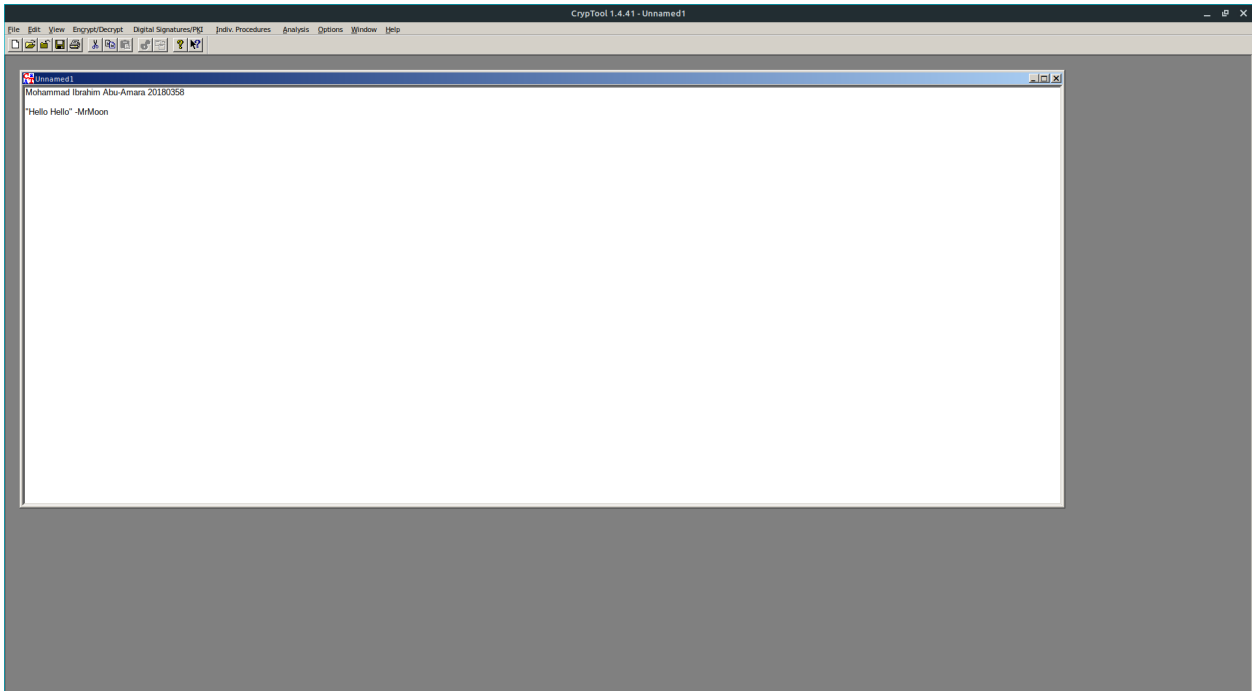
VI. Encrypt the document using the keys

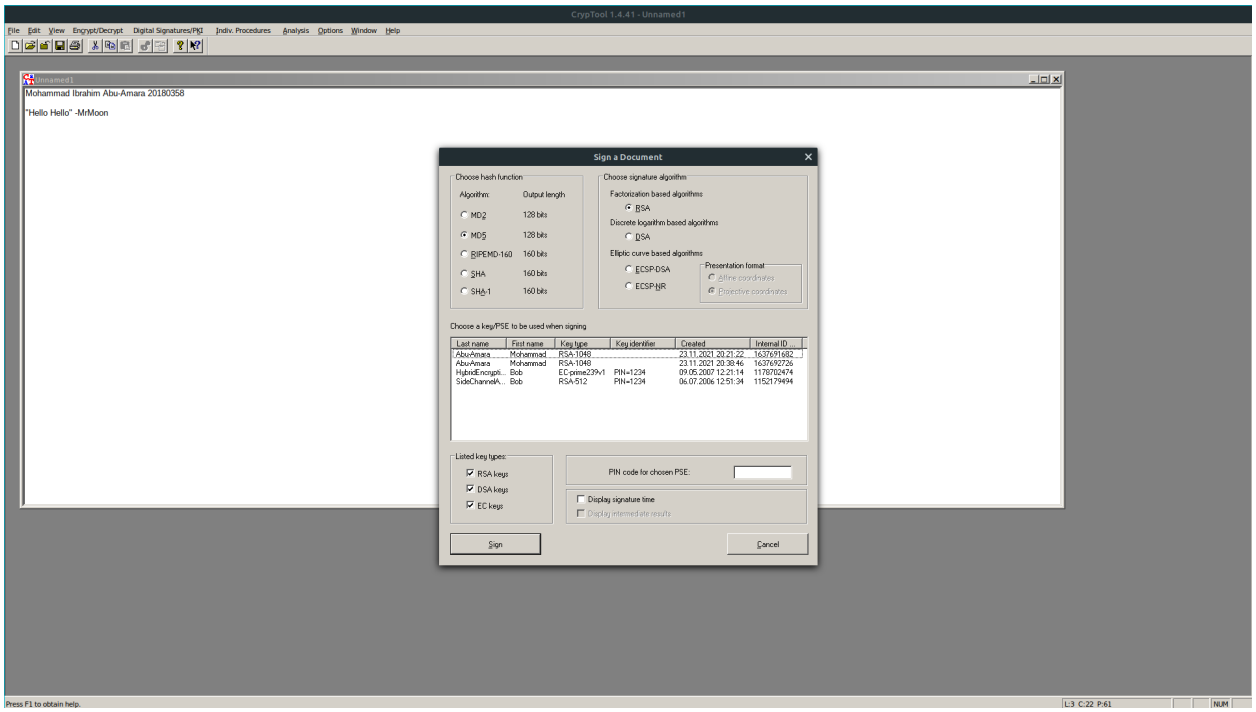

Hybrid Encryption with RSA-AES - Visualization with a Flow Chart
Open document
Generate session key
Select asymmetr. key
Document
Session key
Asymmetr. key
Encrypt document symmetr.
Encrypt session key asymmetr.
Encrypted document
Encrypted session key
Cancel
Save
Session key encrypted asymmetrically with recipient's public key:
D4096871A4BC626A60113A5CB9E1A374AAE84326158E7C4BBC4DCA23E71C63A524A6ADFEBE0D8FC34F11C59943DCA0D

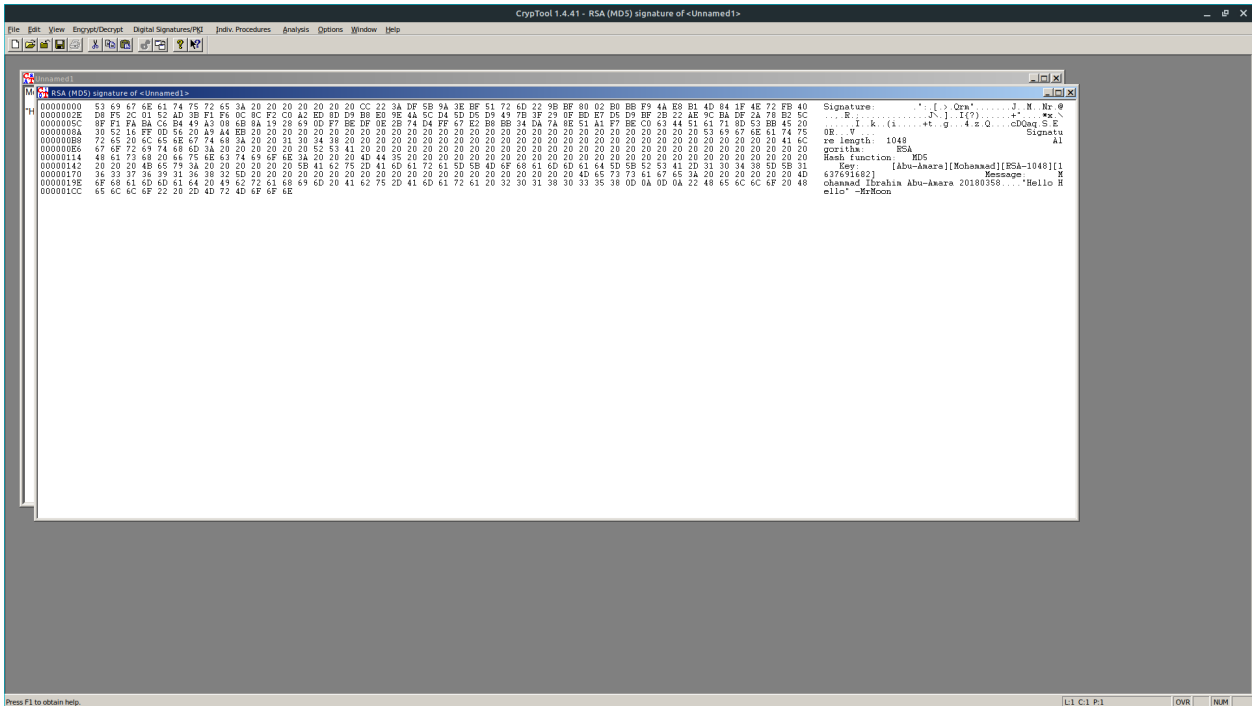

CrypTool 1.4.41 - ciphertext-20180358.txt
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
plaintext-20180358.txt
ciphertext-20180358.txt.hex
ciphertext-20180358.txt
Receiver: [Abu-Amara][Mohammad][RSA-1048][1637688526] Length of encrypted session key: 1048 Encrypted session key:
Symmetric method: AES Asymmetric method: RSA Ciphertext:
Press F1 to obtain help.
L:1 C:1 P:1
NUM

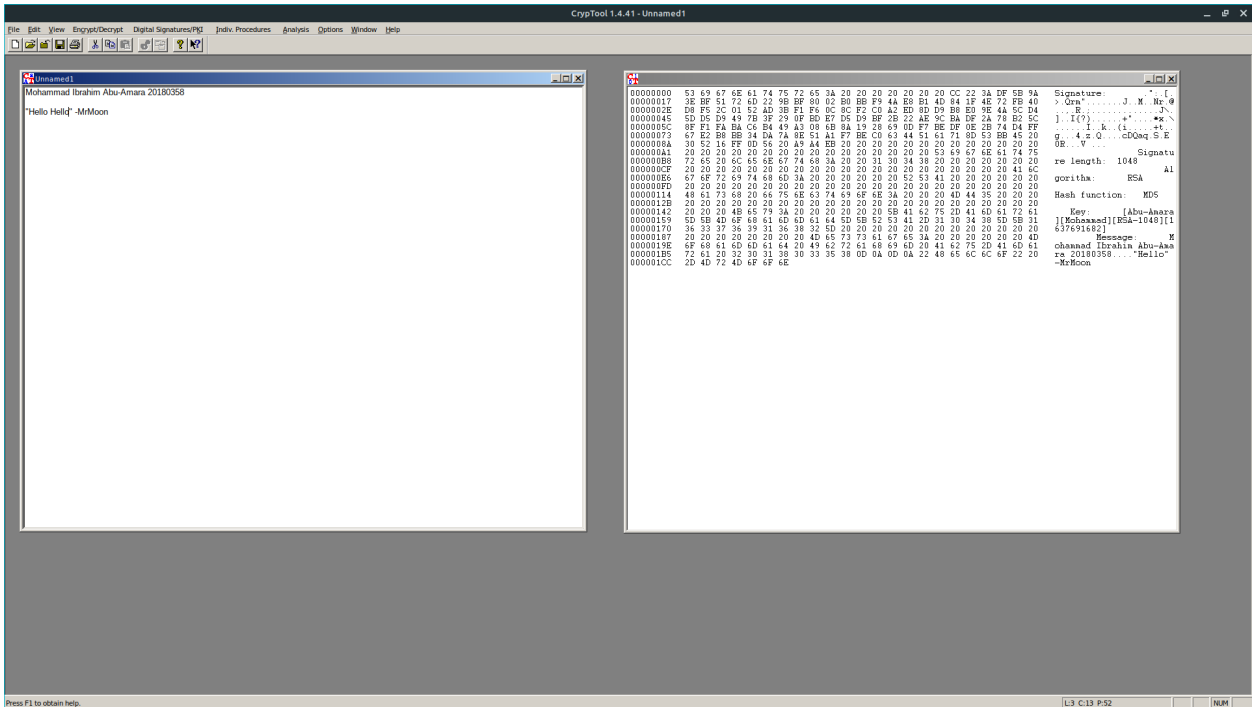
(b)

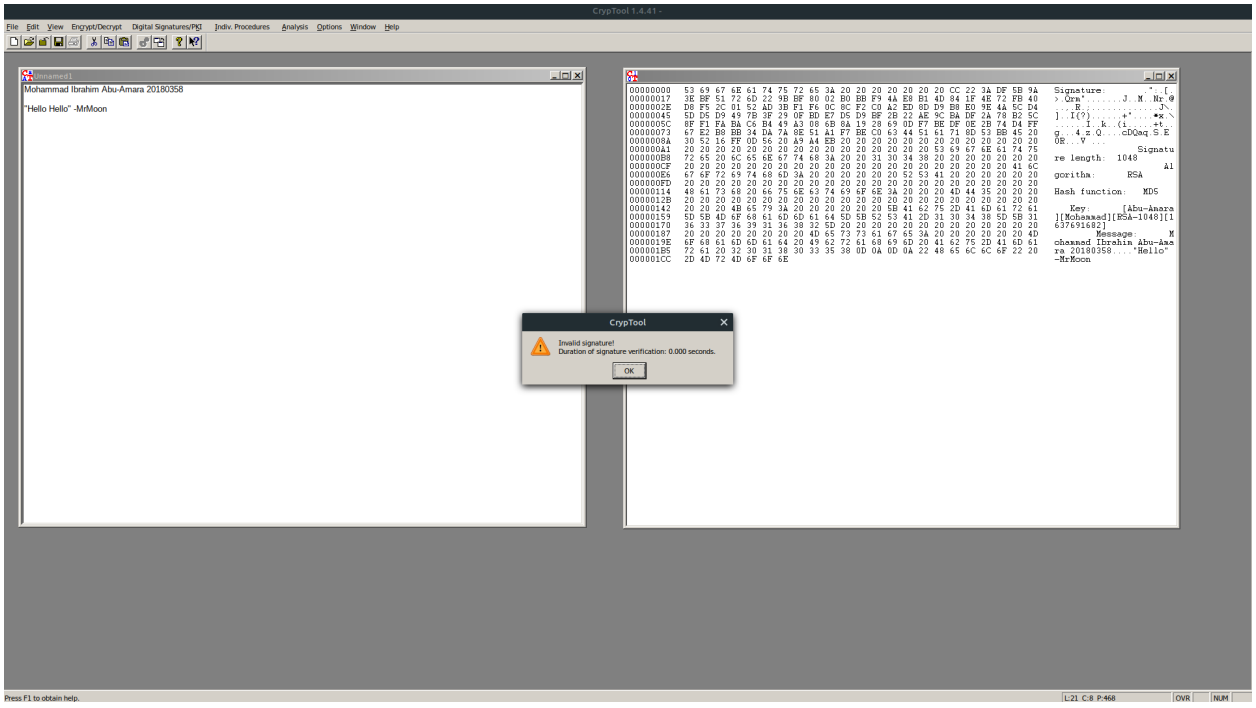
1)


CrypTool 1.4.41 - Unnamed1
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Unnamed1
Mohammad Ibrahim Abu-Amara 20180358
"Hello Hello" -MrMoon


CrypTool 1.4.41 - Unnamed1
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Unnamed1
Mohammad Ibrahim Abu-Amara 20180358
"Hello Hello" -MrMoon
Sign a Document
Choose hash function
Algorithm
Output length
MD2 128 bits
MD5 128 bits
RIPEMD-160 160 bits
SHA 160 bits
SHA-1 160 bits
Choose signature algorithm
Factorization based algorithms
RSA
Discrete logarithm based algorithms
DSA
Elliptic curve based algorithms
ECSP-DSA
ECSP-NR
Presentation format
Affine coordinates
Projective coordinates
Choose a key/PSE to be used when signing
Last name
First name
Key type
Key identifier
Created
Internal ID
Abu-Amara Mohammad RSA-1048 23.11.2021 20:21:22 1637691682
Abu-Amara Mohammad RSA-1048 23.11.2021 20:38:46 1637692726
HybridEncrypti... Bob ECprime239v1 PIN=1234 09.05.2007 12:22:14 1170702474
SideChannelA... Bob RSA-512 PIN=1234 06.07.2006 12:51:34 1152179494
Listed key types:
RSA keys
DSA keys
EC keys
PIN code for chosen PSE:
Display signature time
Display intermediate results
Sign
Cancel
Press F1 to obtain help.
L:3 C:22 P:61
NUM


CrypTool 1.4.41 - RSA (MD5) signature of <Unnamed1>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Unnamed1
RSA (MD5) signature of <Unnamed1>
Signature: Key: [Abu-Amara][Mohammad][RSA-1048][1637691682] Message: Mohammad Ibrahim Abu-Amara 20180358..."Hello Hello" -MrMoon
Hash function: MD5
Algorithm: RSA
Press F1 to obtain help.
L:1 C:1 P:1
OVR
NUM


CrypTool 1.4.41 - Unnamed1
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Unnamed1
Mohammad Ibrahim Abu-Amara 20180358
"Hello Hello" -MrMoon
Signature: Key: [Abu-Amara][Mohammad][RSA-1048][1637691682] Message: Mohammad Ibrahim Abu-Amara 20180358..."Hello Hello" -MrMoon
Hash function: MD5
Algorithm: RSA
Press F1 to obtain help.
L:3 C:13 P:52
NUM


CrypTool 1.4.41 -
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
unnamed1
Mohammad Ibrahim Abu-Amara 20180358
"Hello Hello" -MrMoon
00000000 53 69 67 6E 61 74 75 72 65 3A 20 20 20 20 20 20 CC 22 3A DF 5B 9A Signature: ... [
00000017 3E BF 51 72 6D 22 9B BF 80 02 B0 BB F9 4A E8 B1 4D 84 1F 4E 72 FB 40 > Qrm" ..... J . M . Nr @
0000002E D0 F5 2C 01 52 AD 3B F1 F6 0C 8C F2 C0 A2 ED 8D D9 B8 E0 9E 4A 5C D4 ..,.R.;..... J\.
00000045 5D D5 D9 49 7B 3F 29 0F BD E7 D5 D9 BF 2B 22 AE 9C BA DF 2A 79 B2 5C]..I{?) ..... +" ..... *y.\
0000005C 8F F1 FA BA C6 B4 49 A3 08 6B BA 19 28 69 0D F7 BE DF 0E 2B 74 D4 FF ..... I..k..(i ..... +t..
00000073 67 E2 B0 BB 34 DA 7A 9E 51 A1 F7 BE C0 63 44 51 61 71 0D 53 BB 45 20 g ... 4.z.Q ..... cDQaq.S.E
0000008A 30 52 16 FF 0D 56 20 A9 A4 EB 20 20 20 20 20 20 20 20 20 20 20 20 0R ... V ..... Signatu
000000A1 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 53 69 67 6E 61 74 75 re length: 1048
000000B8 72 65 20 6C 65 6E 67 74 68 3A 20 20 31 30 34 38 20 20 20 20 20 20 20 20 Al
000000CF 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 41 6C gorithm: RSA
000000E6 67 6F 72 69 74 68 6D 3A 20 20 20 20 20 20 20 20 52 53 41 20 20 20 20 20 Hash function: MD5
000000FD 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 Key: [Abu-Amara][Mohammad][RSA-1048][1637691682]
00000114 48 61 73 68 20 66 75 6E 63 74 69 6F 6E 3A 20 20 20 4D 44 35 20 20 20 20 Message: Mohammad Ibrahim Abu-Amara 20180358 ... "Hello" -MrMoon
0000012B 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00000142 20 20 20 4B 65 79 3A 20 20 20 20 20 5B 41 62 75 2D 41 6D 61 72 61
00000159 5D 5B 4D 6F 68 61 6D 6D 61 64 5D 5B 52 53 41 2D 31 30 34 38 5D 5B 31
00000170 36 33 37 36 39 31 36 38 32 5D 20 20 20 20 20 20 20 20 20 20 20 20
00000187 20 20 20 20 20 20 20 4D 65 73 73 61 67 65 3A 20 20 20 20 20 20 4D
0000019E 6F 68 61 6D 6D 61 64 20 49 62 72 61 68 69 6D 20 41 62 75 2D 41 6D 61
000001B5 72 61 20 32 30 31 38 30 33 35 38 0D 0A 0D 0A 22 48 65 6C 6C 6F 22 20
000001CC 2D 4D 72 4D 6F 6F 6E
CrypTool
Invalid signature!
Duration of signature verification: 0.000 seconds.
OK
Press F1 to obtain help.
L:21 C:8 P:468
OVR
NUM

2)