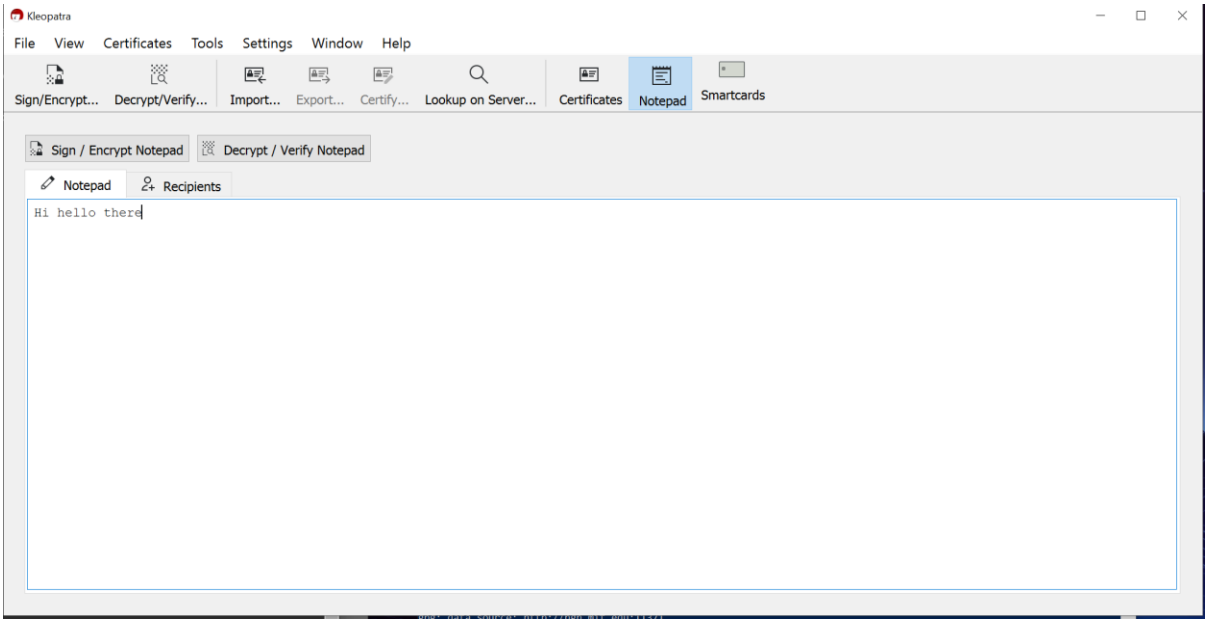
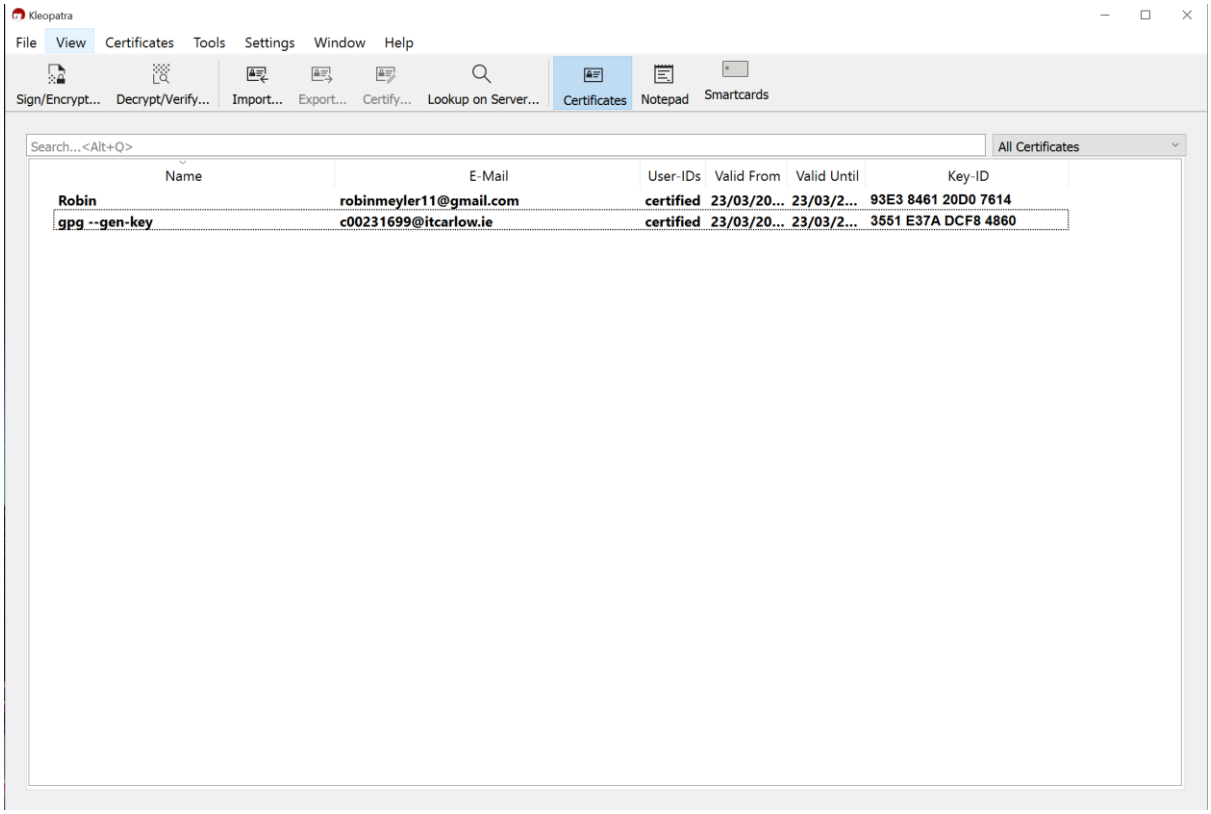
Lab 12

1. *Encrypt/Decrypt*

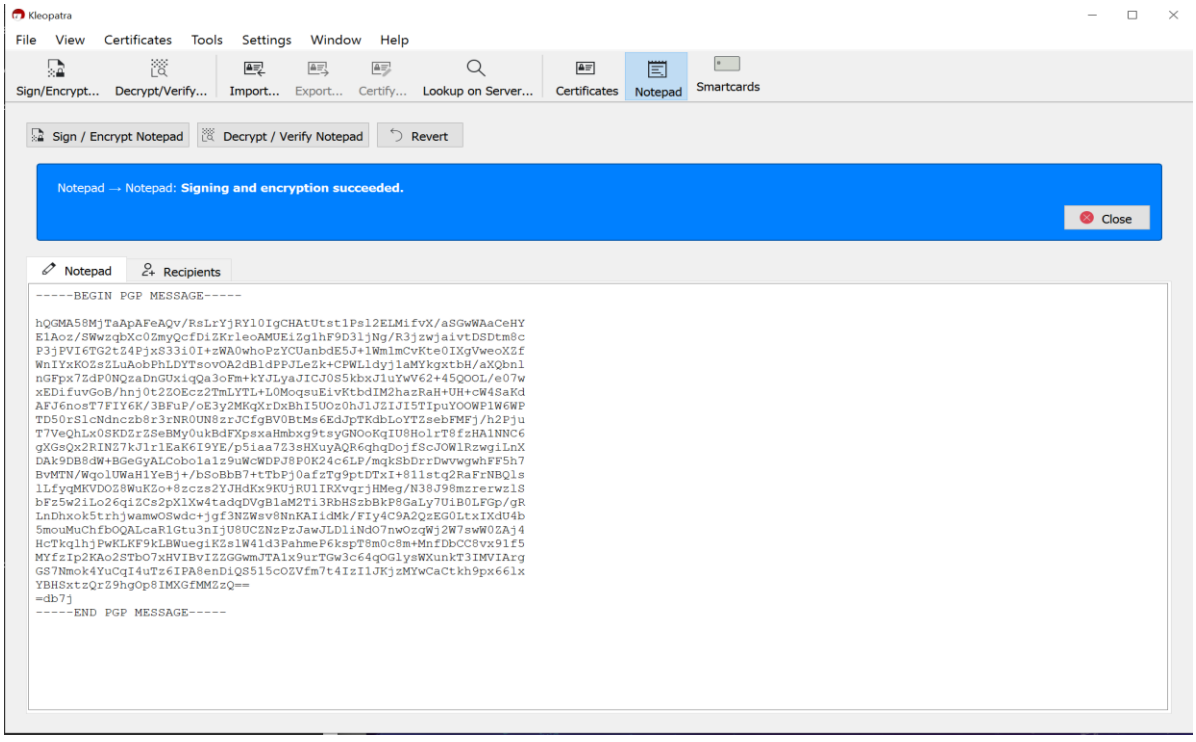
A plaintext message before encryption in Kleopatra:



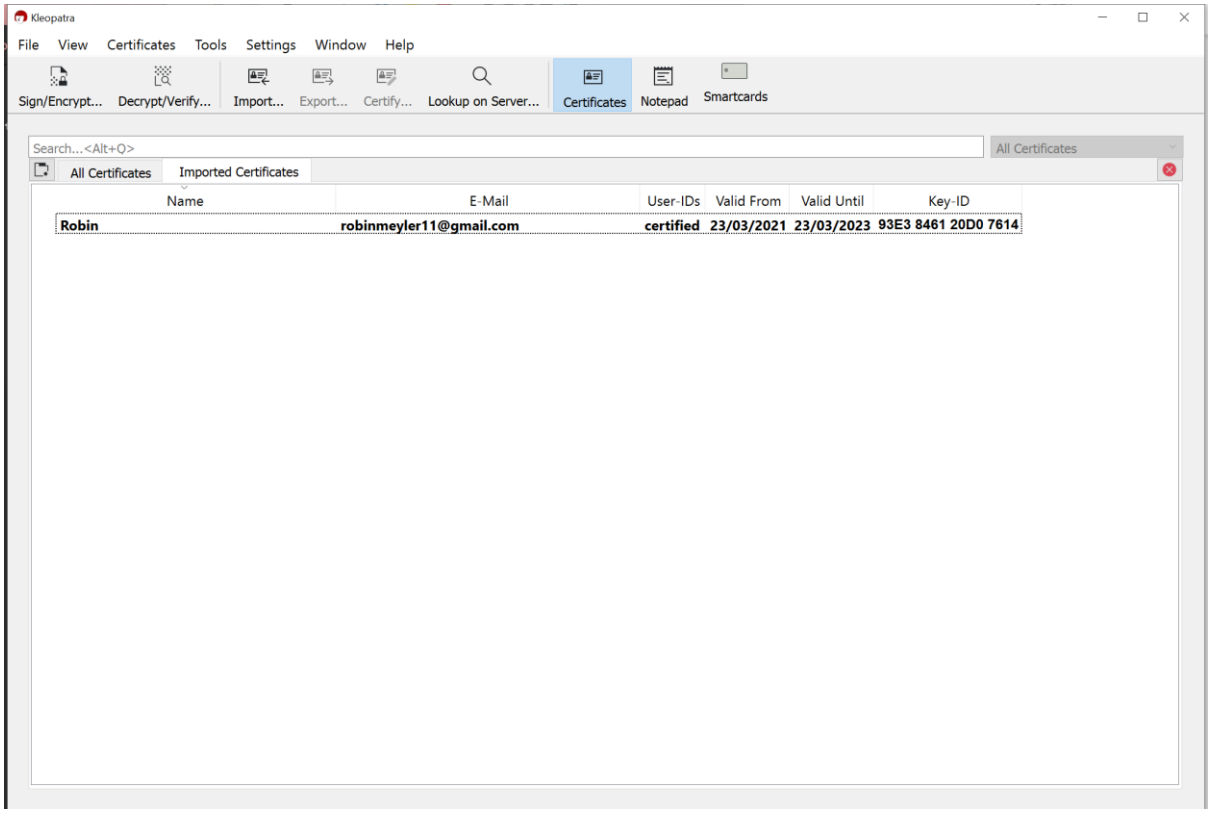
The Encryption of the message with the Key create on the command line:



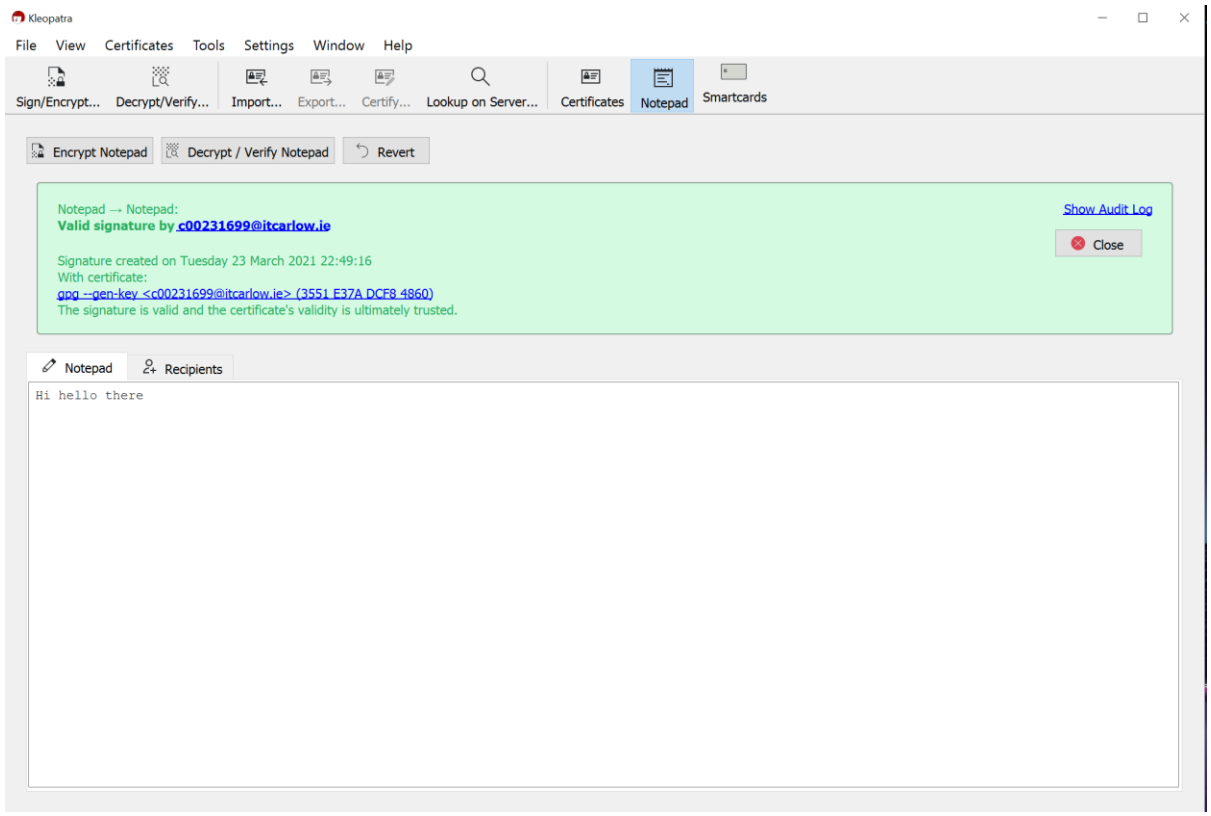
Encrypting of the message:



Importing a key:



Decrypting a key back to the message:



2. RSA example

P and Q have to be prime numbers:

P = 5, Q = 13

N = pq, Z = (p-1)(q-1)

N = 5(13) = 65

Z = (5-1)(13-1) = (4)(12) = 48

E = 5

48*3 = 144

5 *29 = 145 -1

D = 29

Public key = (n,e) = (65,5)

Private key = (n,d) = (65, 29)

For Letter D, m = 4

To Encrypt:

C = m^5 % 65,

C = 4^5 % 65 = 1024 % 65 = 49

To Decrypt:

M = c^29 % 65 = 49^29 % 65 = 4