1. In the process of implementing RSA, you need to verify whether two integers are coprime via implementing the Euclidean Algorithm based on the following equation.

Use your code to compute the gcd(12543, 1682), and print out the final result :

gcd(12543, 1682) = 1
Code for gcd method location RSA/Src/gcd
Gcd
Proof:
By definition of mod,
A = 55
B = 22
R = 11
gcd(55, 22) = gcd(22, 55 mod 22) = gcd(22, 11) = 11
Since gcd(22, 55 mod 22) = gcd(22, 11) = 11
Can calculate the proof by Proof a = kb + r == a mod b = r

A = kb + r	11 = 11 mod 22
r = r(mod b)	55 = 2(22) + 11
A mod b = r;	55%mod22 = 11

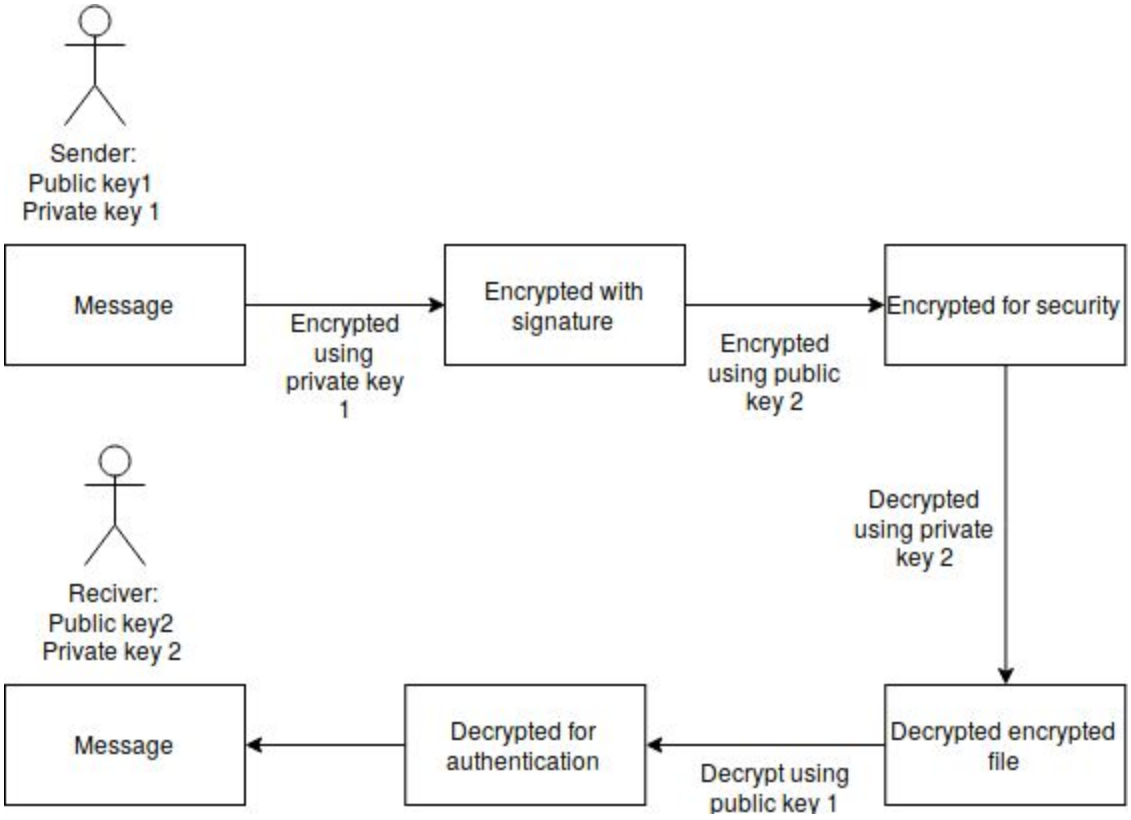
Rearrange:

A = kb + r	r = a - kb
(a mod b) = a - kb	55%mod22 = 55 -2(22) = 11

This proves that both equations have the same set on common divisors, and the same gcd e.g 11 for this example.

Assuming that Alice signed a document m using RSA signature scheme. (You should describe RSA signature structure first with a diagram and explain the authentication principle).

The rsa signature scheme involves, before encrypting the file the sender first encrypts the file with their private key, this allows the receiver of the file to decrypt the file using the sender's public key, if the file is readable it means that Person 1 did send that message, because there should only be one matching set of public and private key and no-one knows Persons 1 private key - meaning it must of been sent by person 1 thisi creates authentication of the file.



The signature is sent to Bob. Accidentally Bob found one message m' (mm ≠ mm') such that H(m)=H(m'), where H() is the hash function used in the signature scheme. Describe clearly how Bob can forge a signature of Alice's with such m'. Justify your forgery with the knowledge you learned from this Unit.

If Alice is sending more of this documents to other people transmits a data block and attach her hash value. Bob could intercept her message and replace it with his and when the hash function is checked to confirm authentication it will pass both messages match.

Also Bob would be able to say that his document was signed by Alice

Bob can say that Alice signed the matching document that she did not really sign, it could be something important like a bank deposit that is normally forward to Bob before sending to the Bank. If Bob noticed his matching document was a payment to his own account rather than the companies Bob can forward this message to the bank like usual but with his own message, the bank will authenticate with Alices public key and think the document is unedited from Alice.

5. In a group of 23 randomly selected people, the probability that two of them share the same birthday is larger than 50%.

The more people in the room the more comparisons are made and so the higher the probability of a shared birthday. For 23 people there are 253 comparisons
23*22/ 2
Compare everyone to everyone nPeople*npeople-1 /2 - divide two to remove repeated comparisons

The chance of one group of two people having different birthdays in a year is
1- (1/365) = 0.997260

Reverse to get the change the one group of two people having the same birthday:
1 - 0.997260 = 0.00274

To find the probability of different birthdays for 253 comparisons(23 people in the room) we can use:
1- (364/365)^253 = 0.4995

Reverse to get the chance of a birthday collison: 1- 0.4995 = 0.5005