ISEC 2000 Assignment 2: RSA encryption

1.) **The euclidean algorithm**

Two integers a and b are coprime when their greatest common divisor (the greatest integer that divides both a and b) is 1. Where a is greater than b or:

gcd(a, b) = 1

also:

gcd(a, b) = gcd(b, a mod b)

The underlying principle of algorithm is that the greatest common divisor of two numbers doesn't change when the larger number is replaced by its difference With the smaller number.

If r1 = 0 then b|a and d = gcd(a,b) = b. If r1 != 0 then d|r1. This is due to the basic properties of divisibility. d|a and d|b imply that d|(a - q1b) which is the same as d|r1

The algorithm is applied repeatedly as:

ri-2 = qi ri-1 + ri

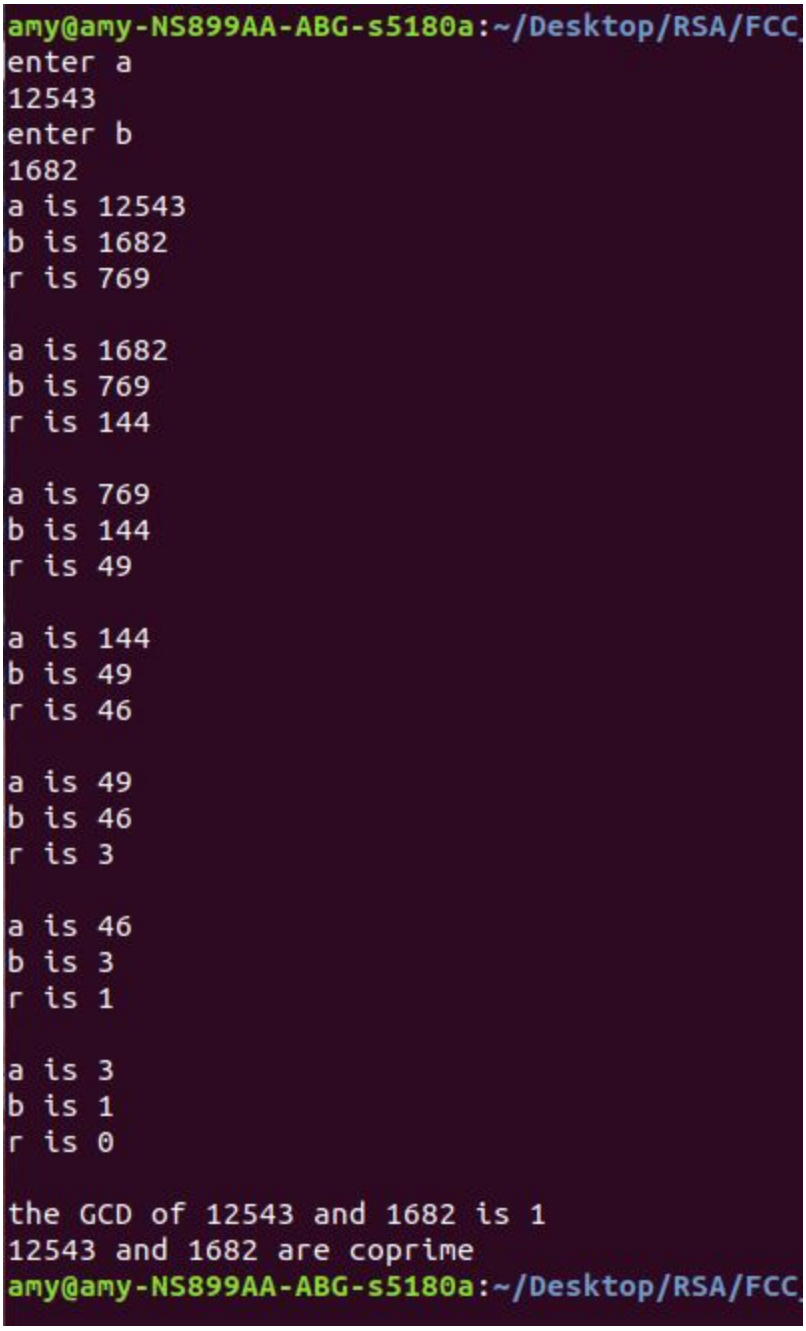
ri-2 is the dividend, ri-1 is the divisor, qi is quotient and ri is the remainder. For example The algorithm starts as

a = q1 b + r1
b = q2 r1 + r 2
r1 = q3 r2 + r3

and so on. Each iteration results in d where d = gcd(ri , ri + 1) until we get

d = gcd(rn , 0) = rn

using an implementation of the algorithm in java for gcd(12543, 1682) results in:



As shown gcd(12543, 1682) = 1. Therefore these two numbers are coprime. r is the remainder or a mod b which shows that gcd(a, b) = gcd(b, a mod b).

2.) RSA encryption

The implementation of RSA encryption resulted in the following:

A sample of the provided test file (testfile-SDES.txt):

```
For example as pointed out by researcher. For each set of fuzzy terms, $A \subseteq M$,
$\prod_{m\in
A}m$ represents a conjunction of the fuzzy terms in $A$. For
instance,
 let $A=\{m_{1,2},m_{2,1},m_{4,2}\}\subseteq M$, a new
fuzzy concept ``$m_{1,2}$ and $m_{2,1}$ and $m_{4,2}$" with the linguist
interpretation ``\emph{short sepal and wide sepal and narrow petal}"
can be represented as $\prod_{m\in
 A}m=m_{1,2}m_{2,1}m_{4,2}$. Then the fuzzy rules can be represented as follows:

\bigskip

 \textbf{Rule} $R_1$ : If $x$ is
$m_{1,2}m_{2,1}m_{4,2}$, then $x$ belongs to Class 1;

\textbf{Rule} $R_2$ : If $x$ is $m_{2,1}m_{3,2}$, then $x$ belongs
to Class 1;

\textbf{Rule} $R_3$ : If $x$ is $m_{1,2}m_{4,2}$, then $x$ belongs
to Class 1.
\bigskip

\noindent Then, the antecedent of three fuzzy rules $R_1, R_2, R_3$ for Class
1 can be represented by ``or" as follows:
\bigskip

\textbf{Rule} $R$ : If $x$ is ``$m_{1,2}m_{2,1}m_{4,2}$ or
$m_{2,1}m_{3,2}$ or $m_{1,2}m_{4,2}$", then $x$ belongs to Class 1.

\bigskip

$\sum^{r}_{u=1}(\prod_{m\in A_u}m)$, which is a formal sum of the
fuzzy concepts $\prod_{m\in A_u}m$, $A_u \subseteq M$, is the disjunction of
the conjunctions represented by $\prod_{m\in A_u}m, u=1,\ldots,r$.
For example, let $A_1=\{m_{1,2},m_{2,1},m_{4,2}\},
A_2=\{m_{2,1},m_{3,2}\}, A_3=\{m_{1,2},m_{4,2}\} \subseteq M$, then
 a new
fuzzy set (i.e., fuzzy concept) as the disjunction of $\prod_{m\in A_1}m$,  $\prod_{m\in
A_2}m$,  $\prod_{m\in A_3}m$, i.e., ``$m_{1,2}m_{2,1}m_{4,2}$ or
$m_{2,1}m_{3,2}$ or $m_{1,2}m_{4,2}$'', can be represented as

\[\sum^{3}_{u=1}(\prod_{m\in A_u}m)=\prod_{m\in A_1}m + \prod_{m\in
A_2}m + \prod_{m\in A_3}m=m_{1,2}m_{2,1}m_{4,2}+m_{2,1}m_{3,2}+m_{1,2}m_{4,2}\]

\noindent Thus, the fuzzy rule $R$ can be denoted as follows:

\bigskip
\textbf{Rule} $R$ : If $x$ is $\sum^{3}_{u=1}(\prod_{m\in A_u}m)$,
then $x$ belongs to Class 1.
```

The resulting ciphertext sample (encrypted_file) each number on a line represents a corresponding encrypted char:

```
27456304
54679333
73290579
51873724
58483733
36745996
84341910
4205285
67945802
4927104
58483733
51873724
84341910
21089663
51873724
67945802
54679333
32253870
27494271
77298060
58483733
41829179
51873724
54679333
82159954
77298060
51873724
47879689
55614883
51873724
73290579
58483733
21089663
58483733
84341910
73290579
11275279
59982646
```

Finally a sample of the decrypted ciphertext:

```
For example as pointed out by researcher. For each set of fuzzy terms, $A \subseteq M$,
$\prod_{m\in
A}m$ represents a conjunction of the fuzzy terms in $A$. For
instance,
 let $A=\{m_{1,2},m_{2,1},m_{4,2}\}\subseteq M$, a new
fuzzy concept ``$m_{1,2}$ and $m_{2,1}$ and $m_{4,2}$" with the linguist
interpretation ``\emph{short sepal and wide sepal and narrow petal}"
can be represented as $\prod_{m\in
 A}m=m_{1,2}m_{2,1}m_{4,2}$. Then the fuzzy rules can be represented as follows:

\bigskip

 \textbf{Rule} $R_1$ : If $x$ is
$m_{1,2}m_{2,1}m_{4,2}$, then $x$ belongs to Class 1;

\textbf{Rule} $R_2$ : If $x$ is $m_{2,1}m_{3,2}$, then $x$ belongs
to Class 1;

\textbf{Rule} $R_3$ : If $x$ is $m_{1,2}m_{4,2}$, then $x$ belongs
to Class 1.
\bigskip

\noindent Then, the antecedent of three fuzzy rules $R_1, R_2, R_3$ for Class
1 can be represented by ``or" as follows:
\bigskip

\textbf{Rule} $R$ : If $x$ is ``$m_{1,2}m_{2,1}m_{4,2}$ or
$m_{2,1}m_{3,2}$ or $m_{1,2}m_{4,2}$", then $x$ belongs to Class 1.

\bigskip

$\sum^{r}_{u=1}(\prod_{m\in A_u}m)$, which is a formal sum of the
fuzzy concepts $\prod_{m\in A_u}m$, $A_u \subseteq M$, is the disjunction of
the conjunctions represented by $\prod_{m\in A_u}m, u=1,\ldots,r$.
For example, let $A_1=\{m_{1,2},m_{2,1},m_{4,2}\},
A_2=\{m_{2,1},m_{3,2}\}, A_3=\{m_{1,2},m_{4,2}\} \subseteq M$, then
 a new
fuzzy set (i.e., fuzzy concept) as the disjunction of $\prod_{m\in A_1}m$,  $\prod_{m\in
A_2}m$,  $\prod_{m\in A_3}m$, i.e., ``$m_{1,2}m_{2,1}m_{4,2}$ or
$m_{2,1}m_{3,2}$ or $m_{1,2}m_{4,2}$'', can be represented as

\[\sum^{3}_{u=1}(\prod_{m\in A_u}m)=\prod_{m\in A_1}m + \prod_{m\in
A_2}m + \prod_{m\in A_3}m=m_{1,2}m_{2,1}m_{4,2}+m_{2,1}m_{3,2}+m_{1,2}m_{4,2}\]

\noindent Thus, the fuzzy rule $R$ can be denoted as follows:

\bigskip
\textbf{Rule} $R$ : If $x$ is $\sum^{3}_{u=1}(\prod_{m\in A_u}m)$,
```

The same as the original test file.

3.) Bob and Alice

A digital signature is a way to verify the integrity and authenticity of a message by identifying the sender via their signature . The sender creates a one way hash of the data to be signed. The hash itself is then encrypted using their private key. The signature is the encrypted hash as well as other information (such as the hashing algorithm). It is then attached to the message and the message is sent.

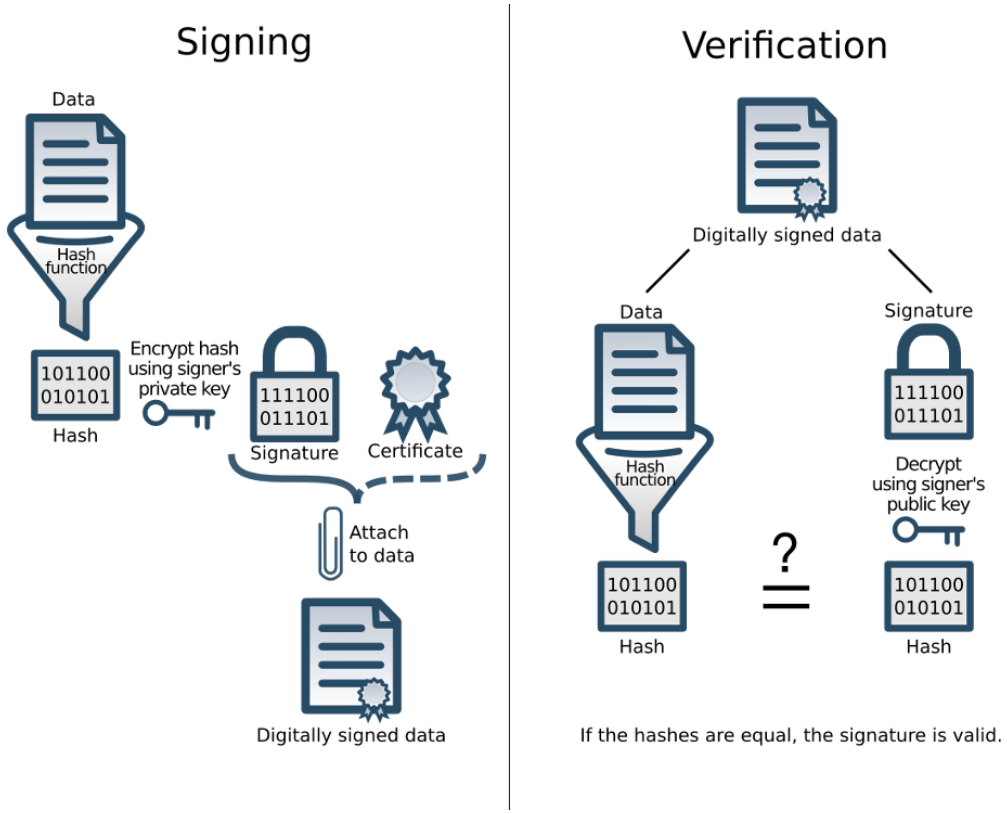


Figure 1: signature structure chart from https://www.strategyobject.com/technologies/security/

To verify the integrity of the message the receiver decrypts both the message and the signature with the sender's public key. The message and signature are then run through the same hashing function as the sender. If they match then the message is secure.

The two different messages m and m' have the same hashing function:

H(m)=H(m')

This is known as a collision (an otherwise unlikely occurrence but still possible to intentionally replicate through brute force) such a collision can be exploited.
Alice signed m and sent it to Bob. Bob can take the signature from m and attach it to m'. He can then send m' to a third party (Ray) Ray who believes that the message was sent by Alice as it has

her signature. He runs the hash functions and find them to be a match, therefore bob managed to forge Alice's signature.

5.) Birthday Problem

In a group of 23 random people there is a larger than 50% chance that they will share a birthday.

With 23 people there are 253 possible comparisons (23*22)/2 = 253. This is more than half of days in a year. The probability of **two people** having a different birthdays is

1 - 1/365 = 364/365 = .997260

The probability of **all 23 people** having different birthdays is:

1 * (1 - 1/365)(1 - 2/365)...(1 - 22/365) = 0.493

as the number of comparisons increases the probability of a different match decreases, eg: the probability of a third person having a different to the first two is

363/365

Therefore after all comparisons the probability of at least two people having the **same** birthday is:

1-0.493 = 0.507

Which is just over 50%