University of Regina
Software Systems Engineering

Winter term, March 2018 ENSE-350

Lab# 02

The RSA Cryptosystem

Beforehand

The receiver creates a public key and a secret key as follows.

1. Generate two distinct primes, p and q. Since they can be used to generate the secret key, they must be kept hidden.
2. Let $n = pq$, phi(n) = ((p-1)*(q-1))
3. Select an integer e such that $\gcd(e,(p-1)(q-1)) = 1$. The *public key* is the pair (e,n). This should be distributed widely.
4. Compute d such that $de \equiv 1(\text{mod } (p-1)(q-1))$. This can be done using the Pulverizer. The *secret key* is the pair (d,n). This should be kept hidden!

Encoding:

Given a message m, the sender first checks that $\gcd(m,n) = 1$. The sender then encrypts message m to produce m' using the public key:

$$m' = rem(m^e, n)$$

Decoding:

The receiver decrypts message m' back to message m using the secret key:

$$m = rem((m')^d, n)$$

Develop an application that will implement the RSA cryptosystem.

Inputs:

1. Two prime numbers: p and q

2. The message to be encrypted (this is an integer): m

Required features:

1. An independent method that could be used to compute $\gcd$ of two numbers using the Euclidean algorithm: $\gcd(a,b) = \gcd(b, rem(a,b))$
2. Ability to find the values of two integers s and t such that $\gcd(a,b) = sa + tb$. This should be implemented as an independent method. This method is the Pulverizer or the Extended Euclidean algorithm.
3. Compute the public and private keys. You need to think about an intelligent way to utilize the routines that you have developed in Step 1 and Step 2.
4. Perform encryption and decryption.
5. The application should print the encrypted message on the output screen and should also verify that decryption actually reproduce the original message.
6. Your application should NOT be using any built in libraries.
7. Use the (%) operator to compute the remainder.
8. You may compute $rem(a^x, b)$ using successive squaring as explained in an example on page 107 of the textbook. For example, all the congruences below hold modulo 17

   $6^2 \equiv 36 \equiv 2$

   $6^4 \equiv (6^2)^2 \equiv 2^2 \equiv 4$

   $6^8 \equiv (6^4)^2 \equiv 4^2 \equiv 16$

   $6^{15} \equiv 6^8 \cdot 6^4 \cdot 6^2 \cdot 6 \equiv 16 \cdot 4 \cdot 2 \cdot 6 \equiv 3$