ECE4893/8893 **Fall Semester, 2013**

RSA Encryption

Assigned: Oct 30, 2013 *Due: Nov 8, 2012, 11:59pm*

Introduction. In this assignment we will use the GNU multi-precision arithmetic library to implement the well-known public-key encryption algorithm known as *Rivest-Shamir-Adelman* (*RSA*). Our program will choose appropriate public/private key pairs, choose random messages, encrypt the random message with the public key, decrypt the random messagse with the private key, and verify that the decrypted message matches the original messages.

Choosing the RSA public/private key pair. To select the public key (n, d) and private key (n, e), do the following.

1. Create a variable of type `gmp_randclass` to generate randomd numbers.
2. Select two random prime numbers p and q of size *sz* bits. (Note we will vary *sz* as described below). The gmp_randclass object has a method called `get_z_bits` which returns a random value of the specified size. The GNU multi-precision library has a function `mpz_probab_prime_p` to determine if a given number is "likely" to be prime. For this assignment, use 100 iterations of the primality testing algorithm (the second parameter on the `mpz_probab_prime_p` function).
3. Compute $n = p * q$.
4. Compute $\phi(n) = (p - 1) * (q - 1)$
5. Choose a random d of size *sz * 2* and with $d < \phi(n)$. Note that d does not have to be prime.
6. Insure that the greatest common divisor of d and $\phi(n)$ is exactly 1. If not, choose another d. The GMP library has a function `mpz_gcd` to compute the greatest common divisor.
7. Finally, compute e as the multiplicative inverse of d modulo $\phi(n)$. Use the GMP function `mpz_invert` for this.

At this point the pair (n, d) is the public key, and (n, e) is the private key (although this is arbitrary, we could use (n, d) as the private key and (n, e) as the public).

Performing the Encryption and Decryption. Given a key (either public or private) (n, d), and a plaintext message m, the RSA encryption algorithm is simple. Just compute the ciphertext message c as $c = m^d \bmod n$. The GMP function `mpz_powm` does this for us.

Specific program details.

1. Start with sz as 32 bits, and double the size for each iteration up to and including 1024 bits. Recall that sz is the size of p and q, and n is $p * q$, so n has twice as many bits.
2. For each value of sz, compute 100 different public/private key pairs as described above.
3. For each public/private key pair compute 100 random messages of size less than n bits. Again, you can use the `get_z_bits` function of the GMP random nubmer generator to do this.
4. For each random message, compute the ciphertext (using the RSA algorithm), and then decrypt the ciphertext message (again using the RSA algorithm) and verify the decrypted message is identical to the original plaintext message.
5. **Grad Students Only**. Attempt to "break" the RSA algorithm for the 64 bit n values using a factoring algorithm of your choice.
6. **IMPORTANT.** Since these jobs will take several minutes of CPU time, we must use the `qsub` procedure we used in the MPI lab. Of course, we only need one CPU, rather then the multiple CPU's we used in MPI.

Copying the Project Skeletons

1. Log into `jinx-login.cc` using `ssh` and your prism log-in name.
2. Copy the files from the ECE8893 user account using the following command:

   ```
   /usr/bin/rsync -avu /nethome/ECE8893/RSA .
   ```

   Be sure to notice the period at the end of the above command.
3. Change your working directory to `RSA`

   ```
   cd RSA
   ```

4. Copy the provided `RSA-skeleton.cc` to `RSA.cc` as follows:

   ```
   cp RSA-skeleton.cc RSA.cc
   ```

5. Then edit `RSA.cc` to create your code for the project

Turning in your Project. The system administrator for the jinx cluster has created a script that you are to use to turn in your project. The script is called `riley-turnin` and is found in `/usr/local/bin`, which should be in the search path for everyone. From your **home directory** (not the RSA subdirectory), enter:

`riley-turnin RSA`.

This automatically copies everything in your `Vector` directory to a place that I can access (and grade) it.