# Ungraded Homework

CSC 152 – Cryptography

**Due:** This work should be completed before you take your module quiz.

Ungraded work is designed to help prepare you for your module quiz. It can be completed anyway you feel helps you learn the material with the exception that you are not allowed to copy anything from anyplace. You may work closely with other people and with internet resources, but when it comes time to write your solution down, you may not copy it from anyone or anyplace.

You must do this assignment in three steps: (1) do the assignment to the best of your ability; (2) study provided solutions; (3) in a second document fix your mistakes. These steps are detailed more below.

If anything in this assignment does not make sense, please ask for help.

**Step 1: Do the following work and submit**

**0)** Read `http://proquest.safaribooksonline.com.proxy.lib.csus.edu/9781492067511` Chapters 8 and 10. Review as needed notes on RSA: `http://krovetz.net/152/rsa.txt`.

**1)** Recall that the extended GCD algorithm goes like this.

```
When calculating the GCD of a and b, repeatedly do the following:
   Rewrite egcd(x, y) as egcd(y, r) where x = qy + r for some 0 <= r < y
   Solve for r:  r = x + (-q)y
   Substitute combinations of a and b for x and y, and simplify
```

At each iteration of the algorithm, you get a new $r$ as a combination of $a$ and $b$, which can be used in later iterations for substitution. The algorithm terminates when $r = 0$, meaning that $y$ is the GCD.

Follow this process to find egcd(59,55) and format your intermediate results as seen in class.

**2)** Compute $55^{-1}$ mod 59 using the result of Problem 1. Explain.

**3)** In a prior homework you needed to compute $(x^3 + x^2 + x + 1)^{-1} \bmod x^4 + x + 1$. Use the egcd algorithm to compute it.

**4)** Let $p = 367$ and $q = 373$ be randomly chosen primes. Use them to produce a public and private RSA key. When it comes time to pick $e$, choose the smallest value greater than 1 that qualifies. When it comes time to find an inverse, use the extended GCD algorithm to find it. Use your public key to encrypt 5, and show that your private key returns 5 when decrypting the result.

**5)** In class we saw an exponentiation algorithm that runs in time proportional to the log of the exponent. Follow that algorithm to compute $12^{13}$ mod 13. Mod each of your intermediate values to keep them from getting too big. Format your computation similar to the following example which computes $3^5$ mod 10: Exponent 5 in binary is 101 indicating (from left-to-right) SQ/MULT - SQ - SQ/MULT.

$$\begin{aligned} 1 &= 3^0 \\ 1^2 \cdot 3 = 3 &= 3^1 \\ 3^2 = 9 &= 3^{10} \\ 9^2 \cdot 3 = 3 &= 3^{101} \end{aligned}$$

The first line shows the identity equal to the base raised to 0. Each subsequent line shows on the left the prior value squared or squared and multiplied by the base, as appropriate, and then the result modulo the modulus. This is followed by the base to the current exponent in binary.

Submit to Fileinbox your solutions to the problems. The file must be named exactly **hw5_ungraded.pdf** (including capitalization) and must be less than 500KB in size to receive credit.

**Step 2: Study my solutions**

Solutions to much of the work done in Step 1 will be posted on the course webpage within a week of the module start. You should examine it and critically compare it with your own work. Some problems are solvable in more than one way, so it is possible your work is correct even if it differs from mine. If you are unsure, ask.

**Step 3: Make corrections and submit**

Redo any problems from Part 1 that you did not get right the first time and submit a second file to Fileinbox showing the correct solution. The file must be named exactly **hw5_ungraded_revised.pdf** (including capitalization) and must be less than 500KB in size to receive credit.