Homework 3

RT Hatfield

12 September 2016

1.
$$210 = 2 \bullet 105 = 2 \bullet 5 \bullet 21 = 2 \bullet 3 \bullet 5 \bullet 7$$
$$588 = 2 \bullet 294 = 2 \bullet 2 \bullet 147 = 2 \bullet 2 \bullet 7 \bullet 21 = 2 \bullet 2 \bullet 7 \bullet 7 \bullet 3$$

   The GCD of 210 and 588 is therefore $2 \bullet 3 \bullet 7 = 42$. Or, using Euclid's algorithm,

   - Euclid$(588, 210)$
     - Euclid$(210, 168)$
       * Euclid$(168, 42)$
         · Euclid$(42, 0)$
         · return 42;
       * return 42;
     - return 42;
   - return 42;

2. Find the inverse of: 20 mod 79, 3 mod 62, 21 mod 91, 5 mod 23.

   - $20 \bullet 20^{-1} \equiv 1 \bmod 79$
   - $3 \bullet 3^{-1} \equiv 1 \bmod 62$ (Honestly, I wasn't sure what to make of this one, as 62 isn't prime and 3 and 62 aren't relatively prime)
   - $21 \bullet 21^{-1} \equiv 1 \bmod 91$ (Same as above)
   - $5 \bullet 5^{-1} \equiv 1 \bmod 91$

3. Consider an RSA key set with $p = 17, q = 23, N = 391$, and $e = 3$. What value of d should be used for the secret key? What is the encryption of the message $M = 41$?

   First, we compute $3d^{-1} \equiv 1 \bmod 352$

   - eEuclid$(352, 3)$
     - eEuclid$(3, 1)$
       * eEuclid$(1, 1)$
         · eEuclid$(1, 0)$

      · $(1, 0, 1)$
    * $(0, 1, 1)$
  - $(1, -3, 1)$
- $(-3, 353, 1)$

Therefore, $d = 3$. To encrypt, we perform $M^3 \bmod 391$. (LaTeX doesn't like such deeply nested lists, so this is ugly)

- $\text{modexp}(3, 41, 391)$
  - $\text{modexp}(3, 20, 391)$
    * $\text{modexp}(3, 10, 391)$
      · $\text{modexp}(3, 5, 391)$
      · $\text{modexp}(3, 2, 391)$
      · $\text{modexp}(3, 1, 391)$
      · $\text{modexp}(3, 0, 391)$
      · 1
      · 3
      · 9
      · 243
    * 8
  - 64
- 167

The encrypted message is 167.