Ungraded Homework Solutions

CSC 152 – Cryptography

Please notify me of any errors you find. If you need help, ask.

1) *Find egcd(59,55) and format your intermediate results as seen in class.*

```
egcd(59,55)
              59 = (1)(55) + 4
              ==> 4 = (1)(59) + (-1)(55)
egcd(55,4)
              55 = (13)(4) + 3
              ==> 3 = (1)(55) + (-13)(4)
                    = (1)(55) + (-13)[(1)(59) + (-1)(55)]
                    = (-13)(59) + (14)(55)
egcd(4,3)
              4 = (1)(3) + 1
              ==> 1 = (1)(4) + (-1)(3)
                    = (1)[(1)(59) + (-1)(55)] + (-1)[(-13)(59) + (14)(55)]
                    = (14)(59) + (-15)(55)
egcd(3,1)
              3 = (3)(1) + 0
              ==> 0 = (1)(3) + (-3)(1)
                    = (1)[(-13)(59) + (14)(55)] + (-3)[(14)(59) + (-15)(55)]
                    = (-55)(59) + (59)(55)
egcd(1,0)
```

So, the GCD is 1 and its linear combination of 55 and 59 is (14)(59) + (-15)(55).

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

From Problem 1 we know 1 = (14)(59) + (-15)(55). If we apply the "mod 59" operation to each part of this, it turns into 1 = (14)(0) + (44)(55), so we know 1 = (44)(55) mod 59. This means 55^{-1} mod 59 $= 44$.

3) *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.*

The RSA modulus is $n = pq = (367)(373) = 136891$. The exponents must have no common factors with $\Phi(n) = (p-1)(q-1) = 136152$. The GCDs with 136152 of 2, 3, and 4 are all not 1, so none of them are suitable for e, but GCD(5,136152) is 1, so $e = 5$ is the smallest suitable RSA exponent. The multiplicative inverse of 5 modulo 136152 is 54461 (ie, $5 \cdot 54461$ mod $136152 = 1$), so $d = 54461$. Encrypting 5 we get 5^5 mod $136891 = 3125$ and decrypting 3125 we get 3125^{54461} mod $136891 = 5$.

4) *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.*

$$\begin{aligned}
1 &= 12^{0} \\
1^2 \cdot 12 \bmod 13 = 12 &= 12^{1} \\
12^2 \cdot 12 \bmod 13 = 12 &= 12^{11} \\
12^2 \bmod 13 = 1 &= 12^{110} \\
1^2 \cdot 12 \bmod 13 = 12 &= 12^{1101}
\end{aligned}$$

So $12^{13} \bmod 13 = 12$, and we solved it in $\log_2 13$ (rounded up) steps. The same sequence of squares and multiplies can be expressed as $(((1^2 \cdot 12)^2 \cdot 12)^2)^2 \cdot 12$. On a quiz, you may be asked to express the SQ/SQ-MULT sequence in text without spaces, placing a close parentheses after each SQ or SQ-MULT step. For this problem the answer would be `((((1^2*12)^2*12)^2)^2*12)`.