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 $55^{-1} \bmod 59 = 44$.

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, $5 \cdot 54461 \bmod 136152 = 1$), so $d = 54461$. Encrypting 5 we get $5^5 \bmod 136891 = 3125$ and decrypting 3125 we get $3125^{54461} \bmod 136891 = 5$.

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)`.

5) *GCD can be computed in Gallois fields too. The algorithm is the same: repeatedly rewrite gcd(x,y) as gcd(y, x mod y) until you get a remainder of 0. (The "mod" here is remainder after dividing polynomial y into polynomial x, so do long division to find the remainder.) It does require greater attention to avoid mistakes though. Compute* $(x^3 + x^2 + x + 1)^{-1}$ *in GF(*2^4*) using the egcd algorithm learned last week. Do all your additions and multiplications using* $x^4 + x + 1$ *as the modulus you use whenever you multiply and the result becomes degree 4 or more.*

```
egcd(x4+x+1, x3+x2+x+1)
                            x4+x+1 = (x+1)(x3+x2+x+1) + (x)
                            ==> x = (1)(x4+x+1) + (x+1)(x3+x2+x+1)
egcd(x3+x2+x+1, x)
                           x3+x2+x+1 = (x2+x+1)(x) + 1
                           ==> 1 = (1)(x3+x2+x+1) + (x2+x+1)(x)
                                 = (1)(x3+x2+x+1) + (x2+x+1)[(1)(x4+x+1) + (x+1)(x3+x2+x+1)]
                                 = (x2+x+1)(x4+x+1) + (x3)(x3+x2+x+1)
egcd(x, 1)
egcd(1, 0)
```

So, the GCD is 1 and it's linear combination of $x^4 + x + 1$ and $x^3 + x^2 + x + 1$ is $(x^2 + x + 1)(x^4 + x + 1) + (x^3)(x^3 + x^2 + x + 1)$. If we apply the "mod $(x^4 + x + 1)$" operation to $(x^2 + x + 1)(x^4 + x + 1)$ it becomes 0, so we know $1 = (x^3)(x^3 + x^2 + x + 1) \bmod (x^4 + x + 1)$. This means $(x^3 + x^2 + x + 1)^{-1} \bmod x^4 + x + 1 = x^3$.

6) *Find a random prime number in the range 1000 - 9999 by picking a random four-digit odd number and performing the probable prime test from class enough times that you're pretty sure it's prime. If it turns out not to be prime, try a new number. Ultimately verify your number is prime by going to WolframAlpha and checking there (for example, "531 prime?" reports that 531 is not prime).*

To simulate picking a random four-digit prime integer, I'll choose a random odd four digit number p and then test it with up to four random bases x in $0 < x < p$. If $x^{(p-1)/2} \bmod p$ is not 1 or $p - 1$ for any of the random bases, we know candidate p is not prime. I'll have `https://random.org` produce all of my random numbers and I'll use `https://wolframalpha` as my calculator.

```
Try 1: 5633.

Random base 1: 2433. Wolfram query: "2433^((5633-1)/2) mod 5633" results in 2947.
```

```
Try 2: 2859

Random base 1: 693. Wolfram query: "693^((2859-1)/2) mod 2859" results in 2166.

Try 3: 2513

Random base 1: 1119. Wolfram query: "1119^((2513-1)/2) mod 2513" results in 225.

Try 4: 5887

Random base 1: 1331. Wolfram query: "1331^((5887-1)/2) mod 5887" results in 379.

Try 5: 8519

Random base 1: 382. Wolfram query: "382^((8519-1)/2) mod 8519" results in 1717.

Try 6: 2327

Random base 1: 1769. Wolfram query: "1769^((2327-1)/2) mod 2327" results in 1314.

Try 7: 5347

Random base 1: 3772. Wolfram query: "3772^((5347-1)/2) mod 5347" results in 5346.
Random base 2: 492. Wolfram query: "492^((5347-1)/2) mod 5347" results in 1.
Random base 3: 73. Wolfram query: "73^((5347-1)/2) mod 5347" results in 1.
Random base 4: 2440. Wolfram query: "2440^((5347-1)/2) mod 5347" results in 5346.
Wolfram query: "Is 5347 prime?" results in "5347 is a prime number".
```

That it took seven tries should not be surprising. Since four digit numbers take 10-12 bits to represent, the density of primes is such that we were lucky that it only to seven.

7) *Every element of a group generates a subgroup, and the size of the group is always a multiple of the size of the subgroup. For $\mathbb{Z}_7^*$ and $\mathbb{Z}_8^*$ determine the subgroups generated by each of its elements.*

In $\mathbb{Z}_7^*$: 1 generates $\{1\}$; 2 and 4 generate $\{1,2,4\}$; 3 and 5 generate $\{1,2,3,4,5,6\}$; and 6 generates $\{1,6\}$. In $\mathbb{Z}_8^*$ there are no even numbers: 1 generates $\{1\}$; 3 generates $\{1,3\}$; 5 generates $\{1,5\}$; 7 generates $\{1,7\}$. Note that because there is no value that generates all of $\mathbb{Z}_8^*$, it is not "cyclic" and therefore would not be useful in cryptography.

8) *Let's say Diffie-Hellman key-exchange is being done with generator $g = 4$ and prime $p = 467$. Note that g generates a subgroup of size 233. What is the key produced when the exponents chosen by the two parties are* 400 *and* 134*? What is the key produced when the exponents chosen by the two parties are* 167 *and* 134*? Why are the keys identical?*

The first key is $4^{400 \cdot 134} \bmod 467 = 161$. The second key is $4^{167 \cdot 134} \bmod 467 = 161$. Because 4 generates a subgroup of size 233, $4^{233} = 1$, so $4^{400 \cdot 134} = 4^{400 \cdot 134 \bmod 233} = 4^{10}$ and $4^{167 \cdot 134} = 4^{167 \cdot 134 \bmod 233} = 4^{10}$.

9) *A small elliptic curve group has elements from $\{(x,y) \in \mathbb{Z}_p \times \mathbb{Z}_p \mid y^2 = x^3 + ax + b \bmod p\} \cup \{0\}$ where $a = 1$, $b = 6$ and $p = 11$. Let's say you choose 6 as your multiplier in a Diffie-Hellman key exchange and you receive $(5,9)$ as your communication partner's contribution. What is the shared key generated?*

We need to compute aB where $a = 6$ and $B = (5,9)$. This is easiest done with the double-and-add multiplication algorithm. Since $a = 6_{10} = 110_2$, this means the answer is $2(2(2\mathcal{O} + B) + B)$ or simply

$2(2B + B)$. I wrote a small program to do point additions for me, from it I get $2B = (10, 9)$, $2B + B = (7, 2)$, and $2(2B + B) = (2, 7)$.