If you want to click on any of the links, you can find this at garron.net/spcs

Today's homework is less math and a bit more exploring. You don't have to do everything. Make sure to do the math, but feel free to try the rest in any order.

1 Extended GCD

Calculate the extended GCD of the following:

- $GCD(4, 30)$
- $GCD(85, 136)$
- $GCD(4, 7)$
- $GCD(104, 144)$
- $GCD(34, 55)$

2 Inverses

Calculate the following:

- $5^{-1} \mod 17$
- $23^{-1} \mod 100$

Recall that $x^{-1}(modn)$ is the number y that makes $1 = x \cdot y(modn)$.

3 GCD Order

If $x, y, z \in \mathbb{Z}^+$, prove that

$$GCD\Big(GCD(x, y), z\Big) = GCD\Big(x, GCD(y, z)\Big)$$

(Hint: Try to extend the idea we used in class. Define c as the "the GCD of all three numbers": the largest number in $\mathbb{Z}^+$ that divides all of x, y, and z. Then show that both sides must have the value c.)

4 Your Friend, the Golden Ratio

Do this in a large group:

Create a 25x25 grid and labels the rows and columns from 1 to 25 each. In the cell at row x and column y, write down *how many steps it takes for the Euclidean algorithm to finish* when calculating $GCD(x, y)$ (use the faster version, and don't count the first step if the numbers don't change). You should be able to find tricks for speeding this up because you're calculating "in bulk".

Circle the cells that have a larger value than anything "before" them. (i.e.where the value at (x, y) is the largest for any (x', y') with $x' \leq x, y \ \leq y$). Do you see a pattern? Can you explain it?

5 Identity

Prove that if $a, b \in \mathbb{Z}^+$, $a > b$, $GCD(a, b) = 1$, and $0 \leq m < n$, then:

$$gcd(a^m - b^m, a^n - b^n) = a^{GCD(m,n)} - b^{GCD(m,n)}$$

6 Thought Experiment

Suppose Alice and Bob are trying to start a conversation that has confidentiality, authentication, and (mutual) identification. Assuming they take the following two steps (in either order), which of these do they need to do first, and why?

- Prove their identities to each other (Identification)
- Agree on a shared secret key and use it to start an encrypted conversation (Confidentiality).

For now, assume they have a way to do both parts in an authenticated way (i.e. no one can tamper with what they send – the receiver gets the "authentic" message that was sent from the other person, regardless of whether they trust the person or not).

7 Repeated Squaring

Calculate the following by repeated squaring:

- $4^{13} \mod 19$
- $3^{20} \mod 17$

8 Diffie-Hellman

Pick a partner and perform Diffie-Hellman with:

- $G = \mathbb{Z}_{31}^*$
- $g = 3$

That is, pick a random number $a \in \{1, ..., 30\}$ and send your partner 3^a.

When you get a number from them (call it h), compute h^a. Compare your secrets.

(You'll probably need to do more repeated squaring.)

9 Discrete Log

Find y such that $3^y \mod 17 = 12$

10 Multi-Party Key Agreement

Use Diffie-Hellman to design a protocol that allows 3 people to agree on a secret key.

Assume that all three can communicate to each other. Anyone can eavesdrop on the communication, but not modify it.

- Easy version: Once you have a secret key in common with anyone, you can communicate securely with them.
- Easy version: You have to set up all the keys before you can communicate securely.

Try to demonstrate that breaking your system would break discrete log or Diffie-Hellman.