1 GCD

Recall Euclid's Algorithm for computing $GCD(A, B)$:

- Subtract the larger number from the smaller number as many times as possible and replace the larger one with it.
- Continue until $A = B$

Compute the GCD of the following and show your work.

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

Now, do the same for the Extended Euclidean Algorithm, i.e. write each of these as:

$$A \cdot X + B \cdot Y = GDC(A, B)$$

2 Caesar Cipher

Sometimes the Caesar Cipher encryption of one English word becomes another word.

For example, the world COLD becomes FROG with a shift key of $k = 3$.

Figure out which word each of these can be encrypted to. Write down the encrypted word and the shift key:

- FOLK [SOLUTION: IRON, 3]
- SLEEP [SOLUTION: BUNNY, 9]
- WITS [SOLUTION: COZY, 10]
- DAZED [SOLUTION: SPOTS, 11]

Do the same for at least 3 of these next ones. Try working with partners, and pick words that other teams aren't working on:

- ALOHAS [SOLUTION: GRUNGY, 6]
- ARENA [SOLUTION: RIVER, 17]
- CUBED [SOLUTION: MELON, 16]
- FAKE [SOLUTION: TOYS, 14]
- FERNS [SOLUTION: BANJO, 22]
- INGOT [SOLUTION: CHAIN, 20]
- JEDI [SOLUTION: TONS, 10]
- LATTE [SOLUTION: FUNNY, 20]
- LAYOUT [SOLUTION: FUSION, 20]
- MEET [SOLUTION: WOOD, 10]
- OVALS [SOLUTION: HOTEL, 19]

3 Other Kinds of Crypto

In class, we discussed, confidentiality, authentication, and integrity. There are many ways to trade these off. Here is an example:

- There is a central server that shares with everyone. In order to send a message to anyone, you send a key to the server, and the server encrypts it to that person.
- This can preserve confidentiality, authentication, and integrity between you and the receiver, except that the server also sees the message.
- Advantage: You only need to know one key to communicate with anyone.
- Disadvantage: If the server doesn't work, you can't send messages.

- Disadvantage: If someone hacks the server, they can see your messages (breaks confidentiality).

You don't have to be as detailed, but try to come up with something as creative and different from the systems we discussed as possible. Describe how it works, what kind of confidentiality/authentication/integrity is has It doesn't have to be realistic, but try to make it useful.

Some ideas that you can use:

- You don't have to know whom you're sending a message.
- Anything that usually requires one person requires multiple people.
- The encrypted message can be modified in some useful way.

4 Alphabetic Shift Tool

Come up with a tool that allows you to shift the alphabet by a given key easily.

For example, you could use rotating disks or sliding rulers.

5 Solitaire Cipher

Write down your own message and encrypt it using the Solitaire Cipher.

You can use either Bruce Schneier's description at

- https://www.schneier.com/solitaire.html

or the 26-card Wikipedia version at

- https://en.wikipedia.org/wiki/Solitaire_(cipher)

Also write down enough information so that I can decode it, like the key (including jokers). If you want to keep it simple, you can start with the deck in order as your "key".

Computer Things

If you have a smartphone or can get access to the computers, try these. Try to do this together with someone else if they don't have a smartphone.

Smartphone Apps / Encrypted Email

Look for crypto apps on you can use on your phone or the internet, and try out anything that seems interesting. (But don't buy anything unless you have permission from your parents!)

Write down a brief review of your experience. Some questions to answer:

- How does the cryptography affect how you use it?
- How easy is it to use? Can you send messages to each other?
- Would you trust it if you needed to keep a secret? Why/why not?
- Can you explain some details of the cryptography behind it? (Other than "it encrypts my messages"?)

Here are some apps you could try:

- TextSecure and RedPhone (Android)
- iMessage (iOS)
  - Apple has a cool paper about how iMessage works: https://ssl.apple.com/iphone/business/docs/iOS_Security_Feb14.pdf
- Anything on an app store that doesn't sound like a scam (be careful!).
- protonmail.ch
- scramble.io

keybase.io

In particular, I have invites to keybase.io I encourage you to try it; send me an email for an invite.

PGP

This on's a bit of a challenge. Try to make yourself a PGP key, and send an encrypted message to:

- lucas@garron.net
- My PGP key is at: https://garron.net/
  (click on `E3EE C254 3880 CAE7` next to the lock).

Here are two useful tutorials on how to do it on a computer. They're fairly detailed, and you might need to try different things to make it work:

- https://emailselfdefense.fsf.org/
- http://futureboy.us/pgp.html

Programming

If you know how to program, implement the Caesar Cipher, the Solitaire Cipher, or some of the math we learned in class.

Try to make something you can show to other students, but don't spend too much time on it.