Lesson 9: Public Key Cryptography

Adapted from Code.org curriculum

Objectives: You will be able too…

- Explain what the modulo operation does and how it operates as a "one-way" function
- Follow an asymmetric encryption algorithm to encrypt a numerical message using the Public Key Crypto widget.
- Explain the difference between symmetric and asymmetric encryption.
- Describe characteristics of the mathematical properties that make public key encryption possible
- Explain the benefits of public key cryptography

Getting Started: Asymmetric Keys and Computationally Hard Problems

- Video:https://www.youtube.com/watch?v=ZghMPWGXexs
- Can someone in their own words explain what the video refers to as “asymmetric encryption”?
- “Can someone summarize what we learned from previous lessons about desirable properties of encryption? When designing an encryption algorithm what are the main goals?”

Getting Started: Asymmetric Keys and Computationally Hard Problems

- Video:https://www.youtube.com/watch?v=ZghMPWGXexs
- Can someone in their own words explain what the video refers to as "asymmetric encryption"?
  - the idea that you can use one key to encrypt a message and different key to decrypt it.
- "Can someone summarize what we learned from previous lessons about desirable properties of encryption? When designing an encryption algorithm what are the main goals?"
  - The goal of any encryption algorithm or function is to be something that easy to compute, but computationally hard to reverse.

What does that mean?

- By computationally hard we mean that the only known way to find an answer would simply take a computer an unreasonable amount of time to compute.
- Typically, this amounts to randomly guessing numbers over an extraordinarily large range of possibilities.*

Think about…

- Take a moment and think about this problem: assuming two people can only communicate over insecure channels, how can they send encrypted messages to each other, if they haven't met ahead of time to agree on anything?
- One answer is to use different keys: a key to "lock" the message that is public, and a key to "unlock" it that is private.
- This idea of different keys is easy to say, but how does it actually work?
- The video says "the way this works is with some mathematics that we won't explain".
- But the way that asymmetric encryption works though is super interesting and the properties and reasons why the math works are possible to understand.

Today…

- In this lesson we're going to take a walk through how public key encryption works because it's fascinating, and also crucial to every modern method of keep data safe and secure on the web.

Cups and Beans…

- The problem of how to send encrypted messages without establishing keys in private ahead of time baffled cryptographers and computer scientists for years, but there is a way to do it!
- In this story we will act out a way to send secret messages that does NOT rely on a shared secret key.
- This method is called public key cryptography because the "key" needed to encrypt something is actually public, and can be used by anyone! But that key cannot be used to decrypt.

Cups and Beans

- The goal for this story is to understand the basic mechanics of how public key cryptography works which requires the exchange of a few messages across insecure channels.
- For the story we'll imagine a cup of beans to stand in for data and information… Afterward we'll take another step toward understanding how this works with math.

Alice, Bob, and Eve

- In cryptography scenarios computer scientists use stock characters:
  - Alice and Bob ("A" and "B") who are trying to send messages to each other
  - Eve the 'eavesdropper' is listening in.
- You should always assume that Eve can see everything that Alice sends to Bob and vice versa.

Cups and Beans

- Recall the carnival game: how many jelly beans in a jar? (easy to count before, but hard to figure out once it is in the jar)
- Imagine that these beans in the cup represent an encryption function
- Only the person who put the lid on is able to remove it
- Everyone else can try to count the beans, but they can't take the lid off (computationally hard)
- There is one wrinkle: a person can add beans to the cup after the lid has been put on by pushing them through the slot in the top of the lid
- The result is that there will be more beans in the cup, but it's still hard to count them by looking in from the outside.

More Cups and Beans

- Story…

- Asymmetric Encryption - Using different procedures (keys) for encrypting or decrypting
- Private Key - Alice's secret number
- Public Key - A thing related to the private key, that can be safely shared in public, that another person can use to encrypt a message. In this case, the cup with the lid on top.
- Encrypted message - Bob adding beans to the public cup is him using Alice's public key to encrypt.

Recap:

- Alice and Bob did not have to agree on anything, or communicate ahead of time
- Alice and Bob only exchanged information in public, right in front of Eve
- Even would have to be able to count the beans in the cup without opening it, both on the way over to Bob and on the way back to Alice, in order to determine what Bob was trying to send Alice
- The real math is actually not that complicated. It essentially uses multiplication and division instead of addition and subtraction. We'll see this in the next lesson

Activity: Part 1

- http://www.visnos.com/demos/clock
- Imagine that you are a person who, when you close your eyes, loses complete track of time. When you open your eyes, a minute could have passed or an hour…or a day…or a week…or a year…you don't know.
- Now imagine a clock reads 4:00. Close your eyes and I'm going to add some time to the clock - I'm going to simulate that some amount of time is passing. Remember, with your eyes closed, any amount of time could be going by.

Activity: Part 1

- How much time passed? What are the possibilities?

Activity: Part 1

- So a clock represents what we call a one-way function! There is no way to know the original input just from looking at the face of the clock. No matter what number you put into it, only numbers 1-12 can show afterward.
- Even if the number is 2,023,789 hours, if you wind the clock around, it will still come out as a number 1-12. We say that any number "wraps around the clock."
- This means that from the clock face alone, we cannot work backwards; we cannot know what the original number was that went into the clock.

Activity: Part 2

- Real cryptography uses this technique, but with clocks that can have a wide range of possible values on their faces
- The operation is called modulo (remainder after division)
- So first, we're going to experiment a little bit with this kind of "clock arithmetic" using a widget
- Go ahead and log in to Code Studio – be sure to READ the description of the terminology

Activity: Part 2

- “modulus” = “clock size”
- “modulo” = “mod” = the official name for the operation of wrapping a number around the clock

Activity: Part 3

- We can use modulo in an encryption function, too. A weakness of the cups and beans was that we were actually sending the real numbers we intended to use over public channels, and we had to pretend that Eve couldn't count them
- No we're going to re-enact the public key encryption procedure we talked about the cups and beans, but we're going to use multiplication and modulo to create our keys and secret messages

Activity: Part 3

- We are going to use the "Public Key Cryptography – Activity Guide"
- We will work in groups of three (Alice, Bob, and Eve)
- First, follow just your character's instructions

Wrap-up: Properties of Public Key Cryptography

- What did Bob need to know to send a secret message to Alice?

- Do Bob and Alice need to share any secrets – like a secret key – in order to send a private message?

Wrap-up: Properties of Public Key Cryptography

- What did Bob need to know to send a secret message to Alice?
  - Bob needs Alice's "public key" (sealed cup)
- Do Bob and Alice need to share any secrets – like a secret key – in order to send a private message?
  - No. That's what is most amazing
  - PKC uses asymmetric encryption – one key for encrypting (public), one for decrypting (private)

Wrap-up: Properties of Public Key Cryptography

- The thing to wrap your head around is that the way you send a secret message using public key cryptography is not intuitive at first.
- Typically, you might think for Bob to send a secret message that he'd encrypt it and send to Alice and she would have to decrypt it with a secret key
- INSTEAD: for Bob to send a secret message he has to first acquire Alice's public key – and a public key only works one way, you can only use it encrypt
- Once Bob encrypts a message with Alice's public key not even he can decrypt it… BIG DEAL

Wrap-up:

- Public Key Encryption was (and is) considered a major breakthrough in computer science.
- Why do you think it's so important?
- What does public key encryption allow us to do that other encryption schemes do not?

Wrap-up:

- Public Key Cryptography is what makes secure transactions on the Internet possible
- In the history of the Internet, the creation of public key cryptography is one of the most significant innovations; without it we could not do much of what we take for granted today – we couldn't buy things, communicate without being spied on, use banks, etc. on the Internet
- Until asymmetric encryption was invented, the only way to ensure secure transactions on the Internet was to establish a shared private key, or to use a third party to guarantee security.

Major Points: Asymmetric encryption and public key cryptography

- Public key cryptography uses asymmetric encryption
- Bob is able to encrypt a secret message for Alice without needing to know her private key, but instead her "public key"
- The only "information" exchanged in public, where Even could see it, was the result of one-way functions that produced data that would be "computationally hard" to crack

Major Points: Asymmetric encryption and public key cryptography

- Anyone, not just Alice, could make a public key (a sealed cup of beans) and put it out in the public with their name on it, allowing anyone else to encrypt a message just for them!
- Because the method is publicly known it actually makes the encryption MORE secure since both good and bad guys know how hard it is to crack

Major Points: Asymmetric encryption and public key cryptography

- Asymmetric encryption in a nutshell:
  - One key can only be used to encrypt data, and a different (but related) key can only be used to decrypt
  - The "related key" relies on mathematical properties that make it easy to produce a public/private key pair, but hard to figure out the private one if you can only see the public one
  - The fact that modulo acts as a one way function is critical in this process

Big Ideas:

- asymmetric encryption is a big deal because without it modern ideas about security on the web would not be possible
- Computationally hard problems are problems for which the only known algorithm to solve them would take an unreasonable amount of time to run to completion. In cryptography this typically means have no avenue to crack a code besides exhaustively guessing every possible key.

Vocabulary:

- **asymmetric encryption** - used in public key encryption, it is scheme in which the key to encrypt data is different from the key to decrypt.
- **modulo** - a mathematical operation that returns the remainder after integer division. Example: 7 MOD 4 = 3
- **Public Key Encryption** - Used prevalently on the web, it allows for secure messages to be sent between parties without having to agree on, or share, a secret key. It uses an asymmetric encryption scheme in which the encryption key is made public, but the decryption key is kept private.