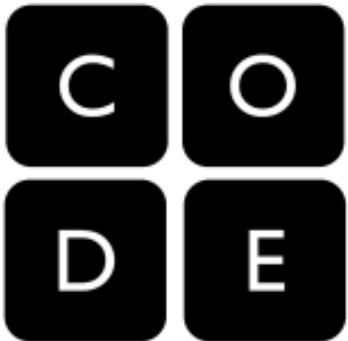
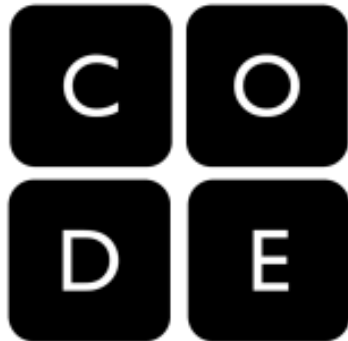


Public Key Cryptography

Unit 4 Lesson 9 (U4L9)
2 days



[\(Optional\) Public Key Bean Counting](#)
[Multiplication + Modulo](#)
[\(Optional\) Public Key Cryptography Recap](#)
[How and Why Does the Public Key Crypto Really Work?](#)



Warm-Up Discussion

Think to yourself, and then share with a neighbor, your response to the following:

Prompt: How can two people send encrypted messages to each other if they can't communicate, or agree on an encryption key ahead of time, and the only way they have to communicate is over the Internet?

Video:
**Encryption
and Public
Keys**
Start at 4:11



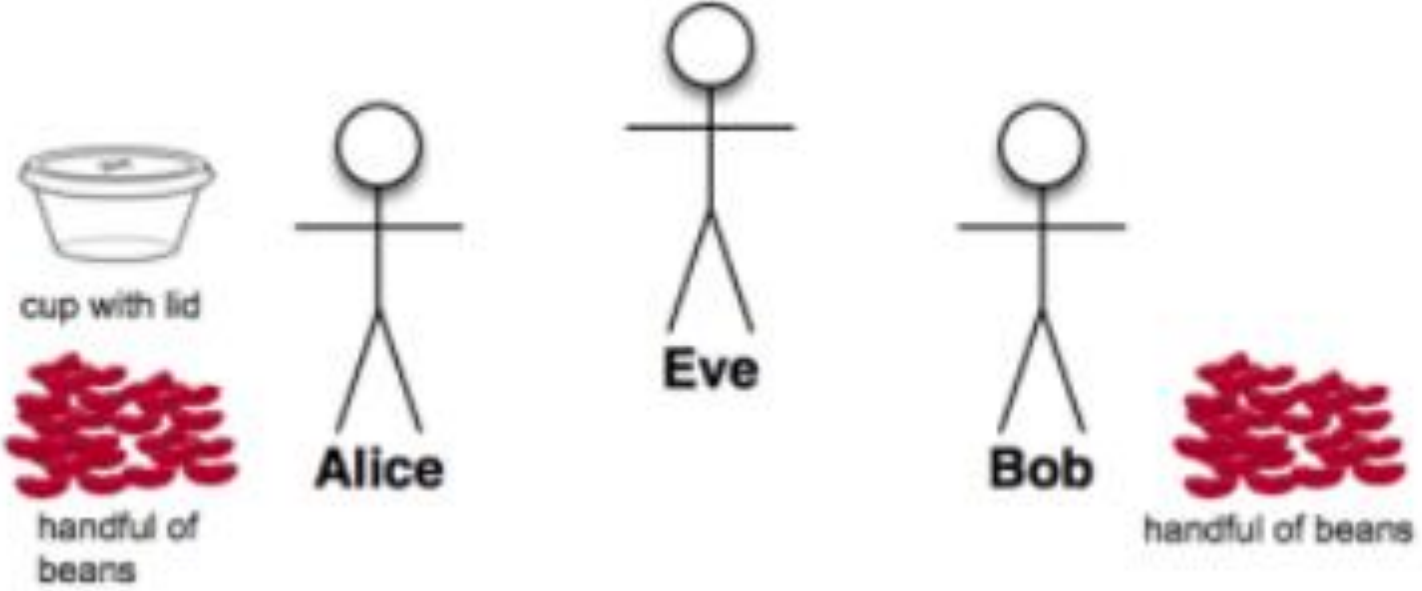
Today we're going to dig in a little bit deeper to how this idea of using different keys actually works. The ideas behind how it works are sophisticated, and so to get a deeper understanding we're going to do a series of short activities that stringing together several different ideas, bringing them all together in the end.

Ready? Here we go!

Activity #1 - Cups and Beans (15-minutes)

Needed: 3 students to demonstrate

What is this? An analogy to demonstrate the idea of Public Key Cryptography



What's the point of the cups and beans activity?

Public key cryptography is what makes secure transactions on the Internet possible. Obviously, computers don't exchange information with beans in plastic cups; they use data (numbers mostly) and the methods of encryption use some math, which we will see in a later lesson. Here the number of beans represented data and the cups represented encrypted data. In order to see how the real thing works, we need to know some terms so we can talk about it accurately.

What's the point of the cups and beans activity?

First, NOTICE:

- At no point did Bob or Alice agree on any secret password, number, or key.
- They only exchanged information in public.
- Bob can encrypt a secret message for Alice by using something that Alice puts out in public
- Eve could not tell what was going back forth without simply guessing either Alice or Bob's private number.

What's the point of the cups and beans activity?

Main Takeaways and Terminology:

- Obviously on the Internet information is not exchanged as beans in cups.
- Our demonstration **DOES NOT show or explain** how the math or encryption works (we'll get to that next)
- What it **DOES show are the mechanics of public key communication**: How public and private keys are used to encrypt information.

Terms that you'll need to know:

Term	Description	Cups and Beans Metaphor
Private Key	A secret piece of information, like a password.	Alice's secret number of beans
Public Key	Information produced using the private key, but transformed in such a way that it's difficult to determine the private key. This can be safely shared in public, and used to encrypt other information.	Alice's secret beans sealed inside a plastic cup

Terms that you'll need to know (continued):

Term	Description	Cups and Beans Metaphor
Encrypted Message	Information encrypted using the public key. Because the <i>private key is subtly mixed into the public key</i> , this transforms a secret message in such a way that only the person who knows the private key can decrypt it	Bob adding beans to Alice's public cup. The "encrypted" cup of beans contains Bob's secret message and Alice's private key, but only Alice knows how many beans were in there in the first place. So only she can decrypt the message.
Asymmetric Encryption	Encryption that uses <i>different</i> keys for encrypting and decrypting. It allows for sender and receiver to communicate without having to agree on a shared encryption key ahead of time.	Bob used the public key to encrypt his message, but Alice used her private key to decrypt.

Okay so that's one step. We now have a clearer idea of the public key encryption process. If we can keep extending this we'll have a solution to the problem of how two people can encrypt messages without meeting ahead of time.

Next we need to see how actual data is encrypted rather than beans in cups.

To learn that, we'll need to string a few more ideas together.

Activity #2 (30 - 45 min.)

Modulo - The Operation Behind Public Key Encryption

The next idea we need to add is an important mathematical operation called "modulo".

The cups and beans demonstration showed us how the mechanics of public key cryptography works.

It's a big deal that asymmetric encryption allows for two parties to send secret messages to each other over public channels without having to agree on a secret encryption key ahead of time.

Now let's look at the mathematical principles that allow private and public keys to work.

Activity #2: Modulo - Clock Arithmetic Thought Experiment

Any kind of encryption requires transforming information in a way that is hard to reverse without a key.

A “one-way function” is a math operation that is impossible to reverse or solve even if you know some of the inputs that went into it. But it’s not random. Given the same inputs, it will produce the same result. There is just no way to reverse the process.

Activity #2: Modulo - Clock Arithmetic Thought Experiment

As an example, let's do a thought experiment:

(Have your notes ready)

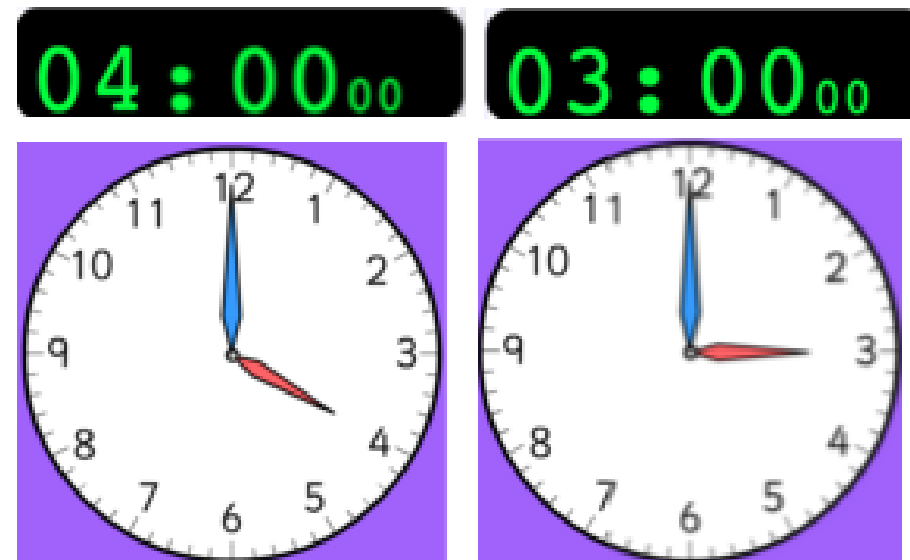
Imagine that you are a person who loses complete track of time when you close your eyes. When you open your eyes, a minute could have passed or an hour...or a day...or a week...or a year...you don't know.

Activity #2: Modulo - Clock Arithmetic Thought Experiment

So, now imagine a clock that reads 4:00.

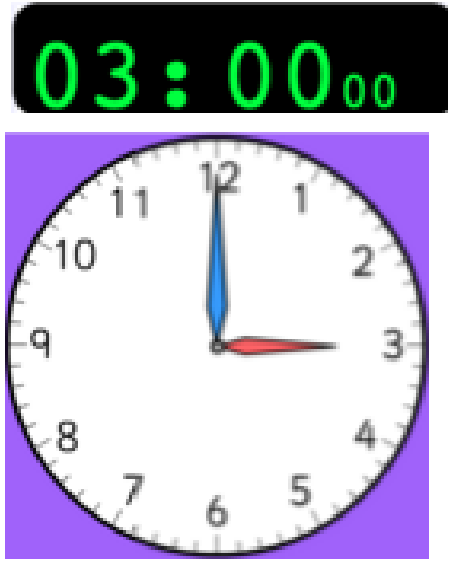
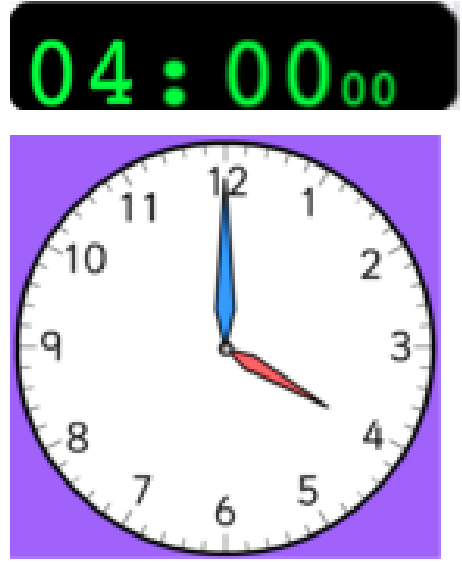
Now close your eyes and I'm going to add some time to the clock - I'm going to simulate that some amount of time is passing. Remember, with your eyes closed, any amount of time could be going by.

*Now open your eyes, look at the clock and, without saying anything to anyone, write down **IN YOUR NOTES** how much time has passed.*



Activity #2: Modulo - Clock Arithmetic Thought Experiment

Verbal Prompt: So, how much time passed? What are the possibilities?



There are an infinite number of possibilities, including: 11, 23, 35, 47 hours, etc. Or 1 day and 11 hours, and so on.

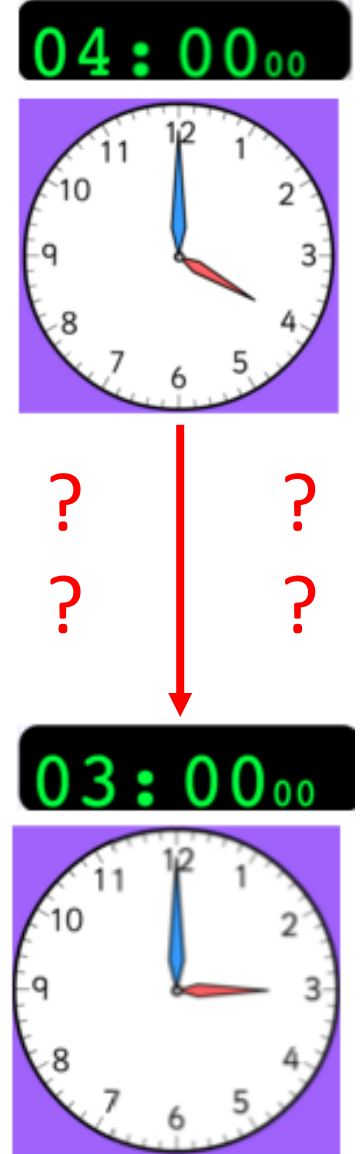
Activity #2: Modulo - Clock Arithmetic Thought Experiment

Takeaway: Clock is 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 cannot know what the original number was that went into the clock.

Clock is a metaphor for modulo

Real cryptography uses this “clock” technique to obscure information, but with clocks that can have a wide range of possible values on their faces. **The operation is called modulo.** It is important for cryptography because it can act as a one-way function - the output obscures the input.



Activity #3: Multiplication + Modulo Activity

Distribute: Activity guide [Multiplication + Modulo Activity Guide](#)

In groups of 2 - 3, complete the worksheet using the widget in U4L9 bubble. But first, let's take a look at how this widget works.

Changing the speed will help with efficiency....

[ANSWER KEY - MULTIPLICATION + MODULO](#)

Lesson 9: Public Key Crypto 5 MORE

The Modulo Clock

Experiment with this "clock" and different numbers to see what happens.

247 MOD 37 Go

Enter a number Pick a clock size

0

1 Speed

Activity #3: Multiplication + Modulo Activity

Discussion: Why is it hard to guess which numbers multiplied together produce the result?"

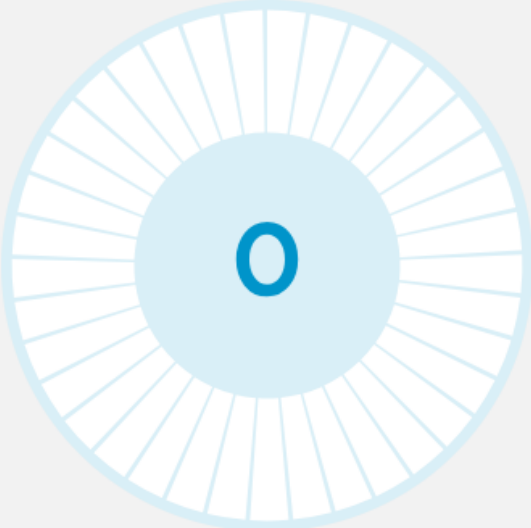
Lesson 9: Public Key Crypto ◊◊◊◊ 5 ◊◊◊◊◊◊◊◊◊◊ ▼ MORE

The Modulo Clock

Experiment with this "clock" and different numbers to see what happens.

MOD

Enter a number Pick a clock size

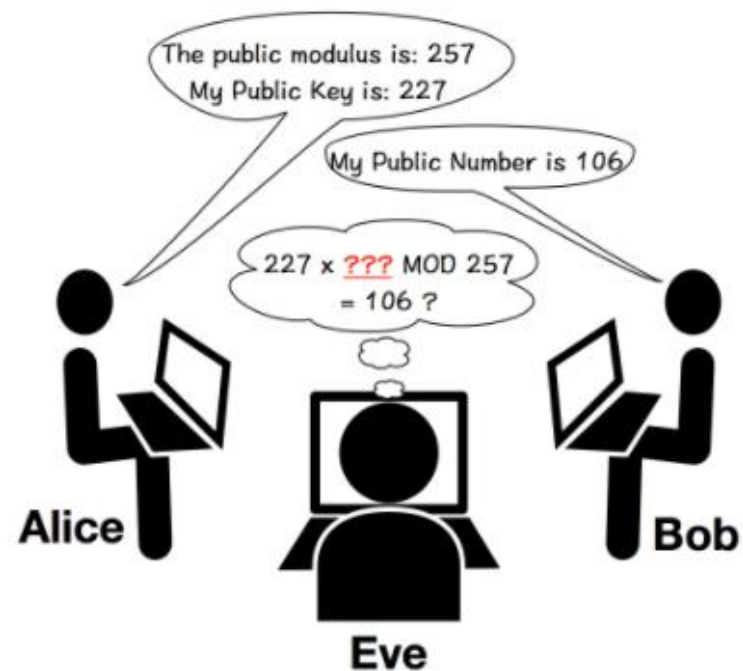


▼
Speed

Activity #4: Using the Public Key Crypto Widget

Okay, now to finally bring everything together. This is the last and final step in which we'll see how we can use the math we just learned about how to create public and private keys.

- Form a group of 3 people.
- Choose your character: Alice, Bob, or Eve
- Follow the instructions on the screen, each are individual to the character.
- NOTE: Alice acts first - announcing two numbers publicly.
- Notice that Bob's first instruction (shown at right), for example, is to wait until he hears Alice announce something.

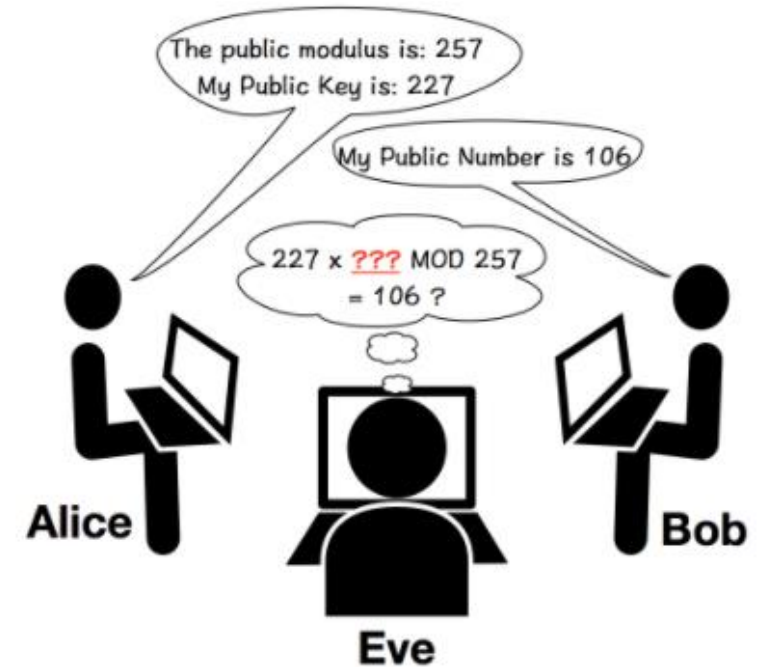


Activity #4: Using the Public Key Crypto Widget

- Complete three rounds (each person should try each character)
- In each round, complete 2 or more trials, using small numbers at first, followed by larger numbers
- After all three rounds are completed, answer the following *IN*

YOUR NOTES:

- What makes things easy or hard for Eve?
- At what point would you feel safe (as Alice or Bob), that your message was secure?



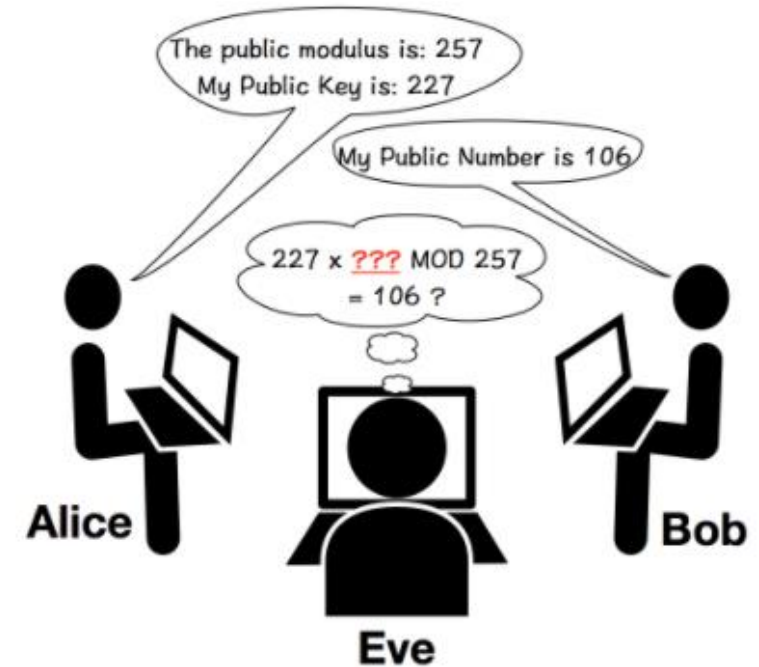
Activity #4: Using the Public Key Crypto Widget

- Complete three rounds (each person should try each character)
- In each round, complete 2 or more trials, using small numbers at first, followed by larger numbers
- After all three rounds are completed, answer the following *IN*

YOUR NOTES:

- What makes things easy or hard for Eve?
- At what point would you feel safe (as Alice or Bob), that your message was secure?

(discuss as class)



Wrap Up (10-minutes):

This is as far as we're going to take the public key analogy. The public key crypto widget is a superficial version of RSA encryption. Instead of basic multiplication, RSA:

- Uses numbers raised to powers of large prime numbers
- Very large (256-bit) values for the modulo divisor (clock size)
- Crack the encryption requires finding the prime factors of EXTREMELY large numbers. Prime factorization is much harder computational problem to solve than our little multiplication+mod problems here.

But from these activities hopefully you have a better sense of how public key encryption works and how making asymmetric keys is at least mathematically possible.

Wrap Up (continued):

Public Key Encryption was (and is) considered a major breakthrough in CS.

- 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, or keep our own conduct on the Internet secret or private.
- 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.
- The implications of this are huge. It means any person can send any other person a secret message transmitting information over insecure channels!

Wrap Up (continued):

Written Prompt: We just spent a lot of time learning about Public Key Cryptography through a bunch of different analogies, tools and activities. And what you've been exposed to mimics the real thing pretty closely. But what are the essential elements? Let's do a brain dump! ***IN YOUR NOTES***, list out what you think are the most important or crucial elements of Public Key Cryptography that you've learned/experienced.

1. Public Key Cryptography is a form of asymmetric encryption
2. For Bob to send Alice a message, Bob must obtain Alice's public key
3. The underlying mathematics ensure that both the public key and a message encrypted with the public key are computationally hard to crack while making it easy to decrypt with a private key
4. It is strong because the method of encryption is publicly known, but keys are never exchanged.

To finish things up, make sure that you.....
(HINT: it's a Caesar Cipher shift of 1)

Bnlokdsd sgd Bgdbj Xntq Tmcdqrszmchmf

Complete the Check Your Understanding

Original:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Maps to:	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

▼ Lesson 9: Public Key Crypto

- 1 Lesson Overview
- 2 Encryption and Public Keys
- 3 Cups and Beans Activity
- 4 Modulo Clock Instructions
- 5 The Modulo Clock
- 6 Public Key Crypto Widget Instructions
- 7 Public Key Cryptography Widget
- 8-13 Check Your Understanding

