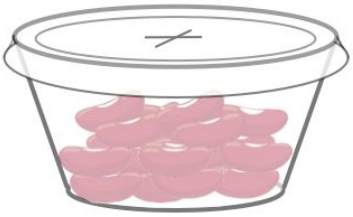
Name(s)_____ Period _____ Date _____

Activity Guide - Public Key Bean Counting

Sending Secret Messages without agreeing a on a secret key ahead of time
In this activity, cups filled with beans will represent information going back and forth between Alice and Bob. We do this activity to show you a simple version of something called **Public Key Encryption** so we can introduce you to the basic process of information exchange and to some of the terminology involved (which we'll get to later).

This activity will show a technique for Alice and Bob to send secret messages to each other, *without agreeing on a secret key ahead of time*, and only by exchanging messages over public, insecure channels.

Background: A metaphor -- cup of beans as one-way function

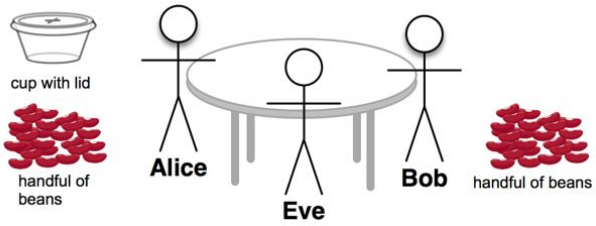


- Imagine that putting some beans into a clear plastic cup and then putting a lid on the cup is a **one-way function**. Only the person who put the lid on is able to remove it.
- Everyone else can try to count the beans but they can't take the lid off; they just have to stare into the cup (like trying to count the jelly beans in a jar at the carnival). This represents a **computationally hard problem.**
- In this activity, there is a wrinkle: a person *can add beans* to the cup 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.

Information Exchange Procedure

Materials

- A clear plastic cup
- A few handfuls of dried beans
- (optional) A lid with a slot in the top that would allow a bean to be pushed through. **If you don't have lids,** you could use plastic wrap, or just use your powers of imagination.



Setup

- Decide who is playing Alice, Bob and Eve.
- Give all of the cups and lids to Alice to start.
- Alice and Bob should each have a handful of beans.

Eve:

Eve, you will direct all the action. You should read all the instructions of the procedure out loud to everyone, and Alice and Bob should follow along accordingly. (Alice and Bob can follow along on their sheets as well.)
Eve reads….

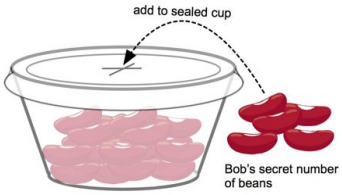
Alice:

1. Alice, turn your back to Eve and Bob while you do this: • Put a random number of beans into a cup -- *Remember this number (or write it down in a secret location).* • Put the lid on the cup. 	**2.** Then put the cup onto the table in front of Bob and Eve. NOTE: Eve and Bob can only guess how many beans are in the cup.

Bob:

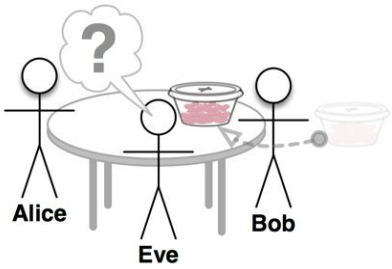
1. Bob, take the cup off the table and turn your back to Alice and Eve while you do this:

- Pick a secret number to send to Alice. *Remember this number.*
- Count out that many beans and add them to the cup.



2. Then put the cup back onto the table.

NOTE: Even though she might be able to see the number of beans is different, Eve can still only guess how many are in the cup.



Eve:

Quick question for Eve: Do you have any idea what secret number Bob is sending to Alice? *Note:* Unless Bob and Alice put so few beans into the cup that you can clearly see from the outside how many there were, your answer should be "No." You might be able to make a guess, but you wouldn't know for sure whether it was right. Okay...move on.

Alice:

Once more, turn your back to Bob and Eve while you do this:

- Take the cup off the table
- Remove the lid and dump out the beans.
- Count off the number of beans originally in the cup.

- What's left is Bob's secret number!

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.
- Eve 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.

Try it again?

- Change roles and try the procedure again to see how it works. Try to make it hard for Eve to guess the secret number. And, Eve, do try to guess.

- Here's a fun wrinkle that makes it even more impossible for Eve: Use 3 cups!
  - Alice, put a random number of beans into 3 different cups (you need to remember how many total beans you used, or you could remember the 3 separate numbers).
  - Bob, for the number you wish to send, distribute the beans randomly into the 3 cups; it doesn't matter how many go into each cup as long as the total is the number you want to send.
  - Alice, once you have the 3 cups back, either dump all the beans out and take away the total number of beans you originally put into the cups, or subtract the individual amounts from each cup. Either way, the beans left over are the ones Bob sent you.

Cups and Beans -- What's the point?

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.

Symmetric Keys
Up to this point, the encryption schemes we've studied have been **symmetric**. This means that the key used to encrypt the message is the same key needed to decrypt the message.

Asymmetric Keys
The cups and beans represent **asymmetric** (pronounced "A-symmetric") encryption because the procedure for encrypting a message (which Bob does) is different from the procedure for decrypting the message (which Alice does).

Private Key
In order for this to work, though, Alice has to provide something for Bob to use that she knows how to undo. In the case of this activity, the number of beans that Alice put into the cup originally is known as her **private key**. Only she knows it, and she never shares it with anyone.

One-way Function
Alice, putting the lid on the cup represents a **one-way function**. Only she knows how to take the lid off, and anyone who wants to discover her private key has to solve the "hard" problem of counting beans in a sealed container.

Public Key
The sealed container sitting on the table represents Alice's **public key**. Anyone, not just Bob, could grab it and use it to send Alice a private message, secure in the knowledge that only Alice could decrypt the message.

Encrypting (a message)
Here, a message is represented by some number of beans. When Bob adds beans to the sealed cup, he is again using a **one-way function** to alter the contents of the cup. Once Bob has added beans to the cup, the message is **encrypted.** Since they get mixed in with the other cup, no one, not even Bob, knows how many total beans there are.

Decrypting (the message)
When Alice receives the cup back from Bob, she can **decrypt** the message by opening the lid and counting the beans. Since she knows how many beans she put in in the first place, she can subtract that number of beans and arrive at the number that Bob intended to send.

Public Key Cryptography
This entire form of exchange is called **Public Key Cryptography**. In this form of secure communication, every participant has *both* a public and a private key. When sending a message, the sender encrypts his message using the **public key** of the recipient.

Due to the mathematical properties of the **one-way functions** used in this type of encryption, the only way to decrypt the message is to use the **private key**, which only the recipient knows. Without knowing this private key, someone trying to crack the message is left to solve a **computationally hard problem**. Thanks to public key encryption, the parties do not need to meet ahead of time to agree on any secret keys, no one exchanges secret keys in public, and the sender can be confident that only the intended recipient can decipher the message.

The *real math* is actually not that complicated. It essentially uses multiplication and division instead of addition and subtraction. The next lesson shows how it works.