Synopsis:

This guide shows you how to run the “Cups & Beans” Demonstration as a teacher. Detailed instructions are below.

1. Introduce the characters "Alice, Bob and Eve"

2. Explain the "Cups & Beans" metaphor - how beans in a cup represents encrypted information

3. Demonstrate the Information Exchange process
   ○ Alice make a public key
   ○ Bob use public key to encrypt message
   ○ Alice decrypt
   ○ (Eve sees all information going back and forth but cannot decrypt)

4. Recap the mechanics of how public key cryptography works

5. Cups and Beans - What’s the point?

Detailed instructions:

1. Introduce the characters "Alice, Bob and Eve"

   ● Explain by saying:

   In cryptography scenarios computer scientists use stock characters:
   
   ● Alice and Bob (“A” and “B”) who are trying to send messages to each other
   (This is because many diagrams show messages going from point “A” to point “B”)
   
   ● Eve the ‘eavesdropper’ is listening in.
   
   You should always assume that Eve can see everything that Alice sends to Bob and vice versa. Eve is a smart adversary who knows what Alice and Bob are trying to do. The goal is to make it hard for Eve to crack the encryption even if she knows how it’s done.

   ● Then select 3 student volunteers to act as Alice, Bob and Eve
   ● Have them stand in the front of the room, an arm's width apart, with Eve standing between Alice and Bob.
2. Explain the "Cups & Beans" metaphor - how beans in a cup represents encrypted information

- Explain the metaphor by saying

  - Have you ever been to a carnival or fair where there's a big glass jar of candy (usually jelly beans) and you're supposed to guess how much candy is in the jar?

  - *We're going to use that idea as a metaphor for an encryption function*

  - It's easy to count out some candies and put them into a jar, but really hard, if not impossible, to guess how many there are once the jar is closed and locked.

- Explain how the demonstration will work, saying:

For today:

  - Our secret information will be some number of beans

  - We’ll “encrypt” that information by putting some beans into a clear plastic cup and then putting a lid on the cup.

  - We’ll simulate information traveling across the Internet by passing this cup of beans from one person to another.

  - We’ll have to imagine that whoever puts the lid on the cup also locks it - so only the person who put the lid on, can take it off

  - Anyone can try to count the beans in the cup 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, since it reduces your ability to count the beans to essentially random guessing

  - One wrinkle: We’ll allow a person to add beans to the cup after the lid has been put on by pushing them through the slot in the top of the lid.  
    
    *(Note: if you don’t have lids it’s okay, imagine that too)*

3. Demonstrate the Information Exchange process

Now we’re ready for the demonstration.

  - Give Alice a cup and a handful of beans
  - Give Bob a handful of beans.

Read aloud these instructions and aid in counting out beans and passing the cup.
The Setup

1. **Alice Bob and Eve** none of you can move. You can only pass a cup of beans back and forth.

2. Our goal is for Bob to send a secret message to Alice. For this to work though, Alice must produce a public key for Bob to use. So...

3. **Alice**: secretly count out some number of beans place them in the cup. Don't let anyone see (except me)

4. **Alice**: put a lid on the cup and pass the cup to Bob out in the open where everyone, including Eve, can see the cup. We'll call this the **public key cup**.

   (Remark that in our metaphor Eve cannot tell how many beans are in the cup, she can only guess. Typically for this the teacher might carry the cup across the room, or ask Alice to pass it to Bob right in front of Eve, or even have Eve hand it to Bob, or even have every student in the class pass it around until it ends up at Bob)

5. **Bob**: pick a secret number you wish to send to Alice and add that many beans to the cup. So the cup now contains Alice's Beans and Bob's Beans.

6. **Bob**: pass the cup back to Alice in plain view of everyone.

   (Again, the metaphor here is that we've just added beans to the cup, it's still just takes random guesses to know what's in there)

7. **Alice**: upon receipt of the cup, dump out the beans, and subtract the number of beans you secretly placed in the cup in the first place.

   The remainder is the secret number Bob sent you!

Verify that this worked with Alice and Bob - Did Alice correctly receive Bob’s “secret message”?

(Applause Applause Applause)

4. Recap the mechanics of how public key cryptography works

Review with students the following points about the demonstration. Did you notice…?

- At no point did Bob or Alice agree on any secret password or key.
They only exchanged information in public.

Crucial: If Bob wants to send a message to Alice, Alice has to act first by producing a cup of beans that Bob could use (her public key).

Bob can encrypt a secret message for Alice by using something that Alice puts out in public -- If Alice wanted to send a message to Bob, then Bob would have to produce his own cup to put out in public.

Eve could not tell what was going back forth without simply guessing either Alice or Bob’s private number.

5. Cups and Beans - What’s the point?

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.
- Here are the terms you should know:

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
<th>Cups and Beans Metaphor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private Key</td>
<td>A secret piece of information, like a password.</td>
<td>Alice's secret number of beans</td>
</tr>
<tr>
<td>Public Key</td>
<td>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.</td>
<td>Alice's secret beans sealed inside a plastic cup</td>
</tr>
<tr>
<td>Encrypted Message</td>
<td>Information encrypted using the public key. Because the private key is subtly mixed into the public key, this transforms a secret message in such a way that only the person who knows the private key can decrypt it</td>
<td>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.</td>
</tr>
<tr>
<td>Asymmetric Encryption</td>
<td>Encryption that uses different 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.</td>
<td>Bob used the public key to encrypt his message, but Alice used her private key to decrypt.</td>
</tr>
<tr>
<td></td>
<td>Point of confusion: there is some amount of encryption involved to produce the public/private pair of keys in the first place. But Alice isn’t encrypting a message to send, rather she is producing a key that others can use to send her a message.</td>
<td></td>
</tr>
</tbody>
</table>

Next we’ll learn about the mathematical principles that make public/private keys possible.