Welcome to Unit 1 of Intro Cybersecurity! 👋

This unit, we'll work on building a cybersecurity mindset. We'll explore how to analyze risk, threats, and vulnerabilities for a company's assets, and learn from real-world events to find ways to minimize the risk to the best of our ability.

We'll also engage with the culture of cybersecurity, practicing some recreational cybersecurity skills and solving [CTF](https://en.wikipedia.org/wiki/Capture_the_flag_(cybersecurity)) challenges!

## **Unit 1 Lab: Intro to Cyberchef**

### **Overview**

This lab will walk you through some fun "Capture The Flag" type challenges while showing you how to use a powerful tool called Cyberchef. Your exercises today will require you to use some critical thinking and problem solving skills. You are encouraged to collaborate and bounce ideas off of one another!

### **🎯 Goals**

By the end of this lab you will be able to...

* Understand how to use Cyberchef
* Use Cyberchef to solve various cybersecurity challenges and exercises

## **Lab Instructions**

In this lab, you will be working with a breakout group to discuss and problem solve various challenges. After you work through the problems within your group, the whole class will meet again to discuss each of the groups' experiences.

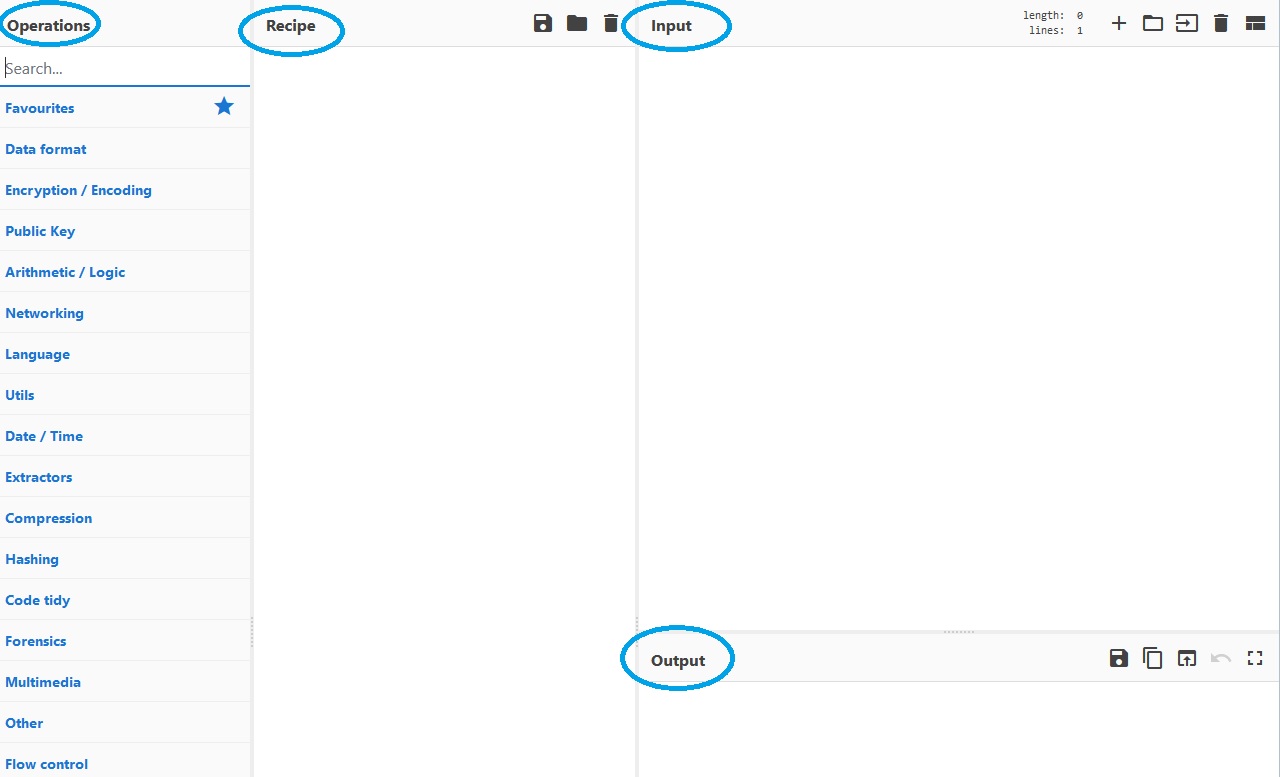
* Download the [Lab1Images.zip](https://courses.codepath.org/course_files/cyb101/lab_1/Lab1Images.zip) folder

### **👥 Exercise 1: Decode a Simple Cipher**

Ciphers, also called encryption algorithms, are simply methods for encrypting and decrypting data. In other words, they are methods for transforming a message to conceal its meaning. Ciphers use algorithms and systems of fixed rules in order to transform data. Luckily, there are tools out there, such as Cyberchef, that we can use that will do all the hard work for us!

#### **Step 0: A quick tour of CyberChef**

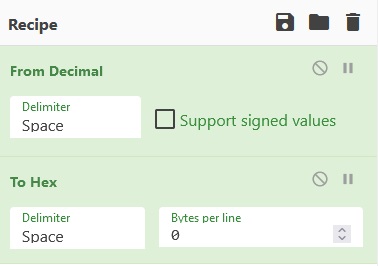
Before we get to decoding, let's make sure we're comfortable with our tool!

* Open up [Cyberchef](https://gchq.github.io/CyberChef/)
* You will see four panels: **Input**, **Output**, **Operations**, and **Recipe**.
  + 📸 *Screenshot  
    *
* The **Input** panel is for just that ... *input*. You can paste, type, upload, or drag the text or file you want to operate on into this panel. You can also click the **"+"** icon to have more than one tab of input.
  + 📸 *Screenshot  
    Add File *
* **Let's go ahead and type 100 into this Input panel.**
  + 📸 *Screenshot  
    *

##### **🤔 So, what are we seeing here?**

* The **Output** panel on the bottom right hand will show you the result of any operations that you use. Right now, it should just be showing you the number 100.
  + There are a few quick processes you can do with the icons on the right such as save your output to a file, copy the output, and even replace the input with the output.
* Sometimes, a **magic wand** will appear next to the Output panel's title.
  + This means that Cyberchef has detected some applicable operations and you can click the magic wand to *automatically apply it's suggested operations*.
  + 📸 *Screenshot  
    *
* The **Operations** panel on the left hand side is where you can find all the operations that CyberChef is capable of in categorized lists, or by searching. When you find the recipe you want to use, you will drag and drop it into the Recipe panel.
  + 📸 *Screenshot  
    *

##### **🚀 Let's try it out! We'll try to convert the number 100 into** [**hexadecimal format**](https://en.wikipedia.org/wiki/Hexadecimal)**.**

* First, we need to indicate what base the input is currently in. Find the "**From Decimal**" recipe and drop it into the Recipe panel.
  + 📸 *Screenshot  
    *
* Now, let's find the "**To Hex**" recipe and drop it into the Recipe panel.
  + 📸 *Screenshot  
    *
* Take a look at the Output ... it should now be displaying the value of 64
  + That's 6 in the 16s place, and 4 in the ones place... and 6\*16 + 4 equals 100!

The **Recipe** panel, as you just learned, is where you can drag the recipe operations that you want to use and specify arguments and options. You can add as many recipe operations as you want or need!

You can also set breakpoints on any operation in your recipe to **pause** execution before running it or step through the recipe one operation at a time using the **stop** feature in order to see what the data looks like at each stage.

* 📸 *Screenshot  
  *

💡 TIP: You can go [here](https://github.com/gchq/CyberChef) to read more about Cyberchef's features!

#### **Step 1: Let's decode!**

Can you decode this simple cipher? Wait how do I know which encoding algorithm was used?? Great question! Open the "**Encryption/Encoding**" Operation tab and try some recipes ... see if you can find the right one!

**Message:** Terng wbo qrpbqvat lbhe svefg pvcure!

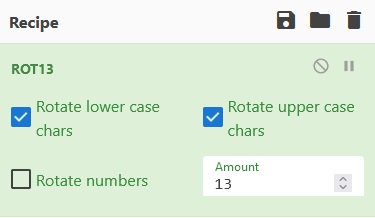
*Make sure you document the cipher or encoding algorithm used as well as the decrypted message!*

**Click me for a hint**

**Sometimes the simplest ciphers are just shifting or rotating by a certain number of places. I don't know about you, but my favorite number is 13!**

**Click me if you're really, really stuck**

**Use the ROT13 recipe! It will rotate each letter by 13 characters, so an A would end up being an N for example.**

****

### **👥 Exercise 2: Let's Build a Fence! Wait ... I Need a *!#CTOAHDPE!#* Key!**

There are some ciphers that are polyalphabetic and require you to enter a key in order to decrypt the data. Can you figure out which popular polyalphabetic cipher is used for this message?

*Tip*: The key is also encoded but not with a polyalphabetic cipher. Can you figure out which cipher is used on the key ... after you figure out what the encoded key is of course!

**Message:** Acx'vt dhppu dqpzbui! Yhie im br!

**Click me for a hint finding the key**

**The title of the exercise has an encoded text ... CTOAHDPE.**

**While this *is* the key, it is also encoded! The title of the exercise has a clue ("*Let's Build a Fence*"). Try Googling "fence cipher" and see what you find!**

**Click me for a hint finding the cipher used on the message**

**The information for this exercise told you that this cipher will be one that uses a key, or a polyalphabetic cipher. Try Googling "popular polyalphabetic cipher" and see what you find!**

**Click me if you're stuck on finding the key**

**Googling "*fence cipher* will give you the result of a Rail Fence Cipher.**

**Once you put this Rail Fence Cipher Decode recipe into Cyberchef with the input of CTOAHDPE you will need to play with the key option of the recipe until the output is a recognizable word/words**

****

**Click me if you're stuck on finding the cipher**

**Googling "*popular polyalphabetic cipher*" will lead you to the most popular cipher of this type which is the Vigenere Cipher. Find the recipe and give it a try!**

****

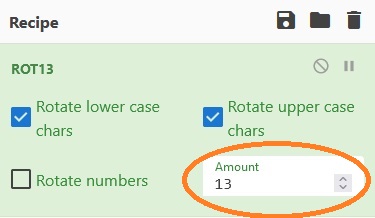
### **👥 Exercise 3: Is a ROT13 Always a Shift of 13?**

Now that you are starting to get the hang of this ... try decoding this message:

**Message:** Ijhtinsl rjxxfljx nx kzs, gzy bmfy jqxj hfs bj it?!

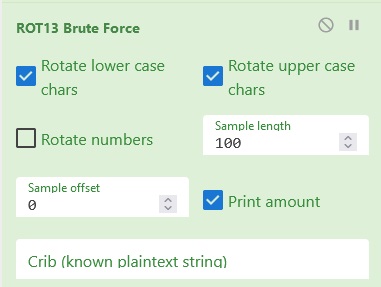
**Click me for help with this exercise**

**Notice the up and down options in the ROT13 recipe! Try using them to change the rotation number until the message is clear!**

****

**Tip: You won't need to go beyond the number of letters in the alphabet or into negative values**

**You could also try using the ROT13 Brute Force recipe which will output all possibilities for you.**

****

### **👥 Exercise 4: Broken Image File**

Did you know that an image is just a bunch of data?! One way that a computer knows what type of file the data should be formatted in is by something called [Magic Numbers](https://gist.github.com/leommoore/f9e57ba2aa4bf197ebc5) (*click on the link to check out examples*). These are the first group of numbers in the data that the computer will read which will tell the computer what type of file the data is supposed to be.

Knowing this information, can you use Cyberchef to figure out how to get the **Lab1\_Ex4.png** image to show up?

**Click me for a hint with how to solve this exercise**

**Once you upload the file into the input, copy the data from the Output panel.**

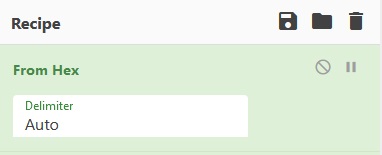
**You can do this by either copy the output and then paste it into the Input panel or click the icon that will copy the output into the Input panel for you.**

**Click me for help with the required recipes**

**Copy output to input **

**Once you get the output into the Input panel, you then need to fix the Magic Numbers.**

**After you fix the magic numbers for a PNG file, you will finally need to use the From Hex recipe operation**

****

**At this point, you should see the Magic Wand appear in the Output panel!**

**Close Section**

### **👥 Exercise 5: Hidden Message**

As you can see, Cyberchef can do a lot more than decode ciphers! See if you can figure out how to get the **Lab1\_Ex5.png** image to reveal the hidden message text!

**Click me for a hint**

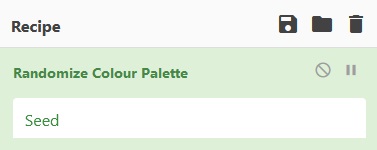
**The color of the hidden text is *very* close to the background color which, as you can see, makes it hard to see!**

**Perhaps there is a recipe that has to do with color!**

**Click me for more help with this exercise**

**The recipe you need to use is one that will randomize the detected colors in the image. This will result in the background and the text both being given random colors and, more than likely, they will not end up being close to the same color as they are now - which means you'll be able to see the text!**

**The recipe you need to use is the Randomize Colour Palette recipe!**

****

### **👥 Exercise 6: Hashes Anyone?**

Your last exercise will require you to use what you've learned so far *and* one more tool called [Crack Station](https://crackstation.net/).

*Tip: Don't give up!! You got this!!!*

**Message:** Qfw ech'uv rkoqb wox huh gruxrfk! **Key:** 8621ffdbc5698829397d97767ac13db3

**Click me for a hint**

**Since there is a key, this is your indication that it might be a Vigenere cipher. Give it a try and see what happens!**

**Close Section**

**Click me for another hint**

**Once you put the key into the Vigenere Cipher recipe, you should have received an error message about the key only containing letters.**

**Hmmm ...**

**Perhaps this is where the new Crack Station tool comes in!**

**Close Section**

**🎉 Congratulations, you've completed your first lab! 🎉 These challenge-cracking skills will serve you well in this week's project!**

**Click me for another hint**

🎉 Congratulations, you've completed your first lab! 🎉 These challenge-cracking skills will serve you well in this week's project!