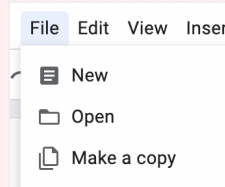


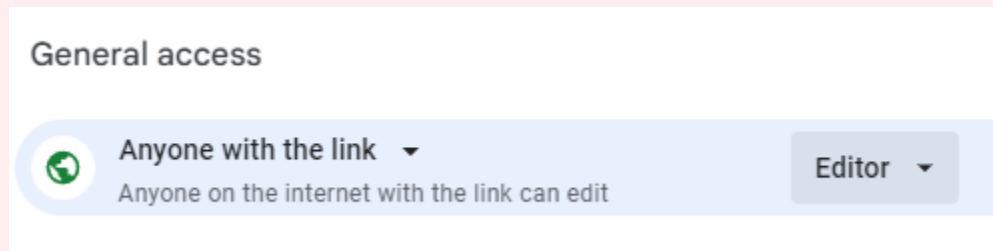
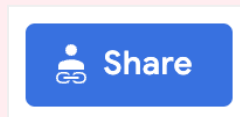
## Instructions for Copying and Sharing this Document

 **DELETE THIS BOX BEFORE SUBMITTING!!**

Step 1: **Click** “File -> Make a Copy” to make a copy of this document that you can edit.




Step 2: **Change** the Share settings to “Anyone with Link -> Editor”. This will allow our graders to leave comments on your submission.




## CYB101 Project 1

( [Instructions Page](#))

 Student Name: Jonathan Siegel

 Student Email: jsiegel0516@gmail.com


## Reflection (Required)

 **Reflection Question #1:** If I had to **describe this CTF experience in 3 emojis**, they would be...  
(Feel free to put other comments about your experience this unit here, too!)



## **Reflection Question #2:** How do CTFs and other practice exercises help build a cybersecurity mindset?

Capture the flag allows developers to develop a cybersecurity mindset when dealing with factors when thinking about questions such as “how can i defend my flag?” and “how can i take the flag of others?” When those questions are asked it allows developers to come up with different strategies. These strategies are derived from the type of attack and how a certain type of encryption defends that attack. For instance, brute forcing a password can most likely be avoided when the defender makes a specific key that shifts characters in the string, and that key is shared amongst trusted individuals. For capturing other flags, it is mostly through trial and error practice. The cyber chef lab encouraged users to test out different shift amounts and keys in order to decrypt a string

 **Shoutouts:** Share appreciation for anyone who helped you out with this project or made your day a little better!

Shoutout to group 52 in the Saturday 10am-12pm class.

## **CTF Challenges (Required)**


Use the answer boxes below to document any CTF challenges you completed. Be sure to include information about **how** you solved the problem – Imagine you’re writing a how-to guide for future cybersecurity students!

### **Trivia Challenges**

 **Challenge 1:** Honesty is Best Policy

**Solution: Integrity**

**How to Solve: Checksums are usually placed in order to detect high level data orders. Checksums are usually checked through MD5 to see if a file has been altered or not. Usually when two files have very similar MD5’s, they the file has not been altered much or the file is exactly the same.**

 **Challenge 2:** Lots of Jobs!

**Solution: 1. California  
2. Texas  
3. Virginia  
4. Florida**

### How to Solve:

I opened up the website [cyberseek.org](https://cyberseek.org), then I clicked on Heatmap and then I just compared the numbers amongst the states.

### Challenge 3: Hostage

**Solution: Ransomware**

**How to Solve:** Malware is received through electronic communication (via email, messages, website etc) then the malware downloads malicious code on the victims computer. Afterwards, said malicious code then encrypts files on the victim's computer, a ransom note is then attached to the victim's computer encouraging the victim to pay money to the attacker.

## Reconnaissance Challenges

### Challenge 4: 11,185,272

**Solution: 12,837,064**

**How to Solve:** First I tried to see what was the relation between all three numbers with simple mathematics (how 11 was related to 185 and/or 272). The numbers are related to each other through something called the Mersenne prime. The equation for this is  $2^n - 1$  where n is a prime number. There are 51 iterations of this specific prime number. The 45th is 11,185,272 and the 46th number is 12,837,064

### Challenge 5: Read Me

**Solution:**

**How to Solve:**

### Challenge 6: Three Even, Two Odd

**Solution:**


**How to Solve:**

## Cryptography Challenges

### Challenge 7: Shifty


**Solution: The password is PleaseChangeMe**

**How to Solve:**How to Solve: On cyber chef, the title of the challenge is shifty, so figured it had to do with ROT13 encryption. I used the bruteforce option and that was the only result that had strings that made sense.

 **Challenge 8:** Encoded Message

**Solution:** itgetsharderfromhere

The = sign at the end was a clear indication of base64 encryption. Upon decrypting with a base64 decoder, I was able to get that string of text.

 **Challenge 9:** Kasiski Who?

**Solution:**

**How to Solve:**

 **Challenge 10:** But are there eggs?

**Solution:**

**How to Solve:**


 **EXTRA Challenge 11:** Arch EXIF!

**Solution:**

**How to Solve:**

---

## Submission Checklist

 Check off each of the features you have completed. **You will only be graded on the features you check off.**

### Reflection

- ☒ Reflection Question #1 answered above
- ☒ Reflection Question #2 answered above

### CTF Challenges (6+ needed for full credit, 9+ needed for extra credit)

- ☒ Challenge #1: Honesty is Best Policy

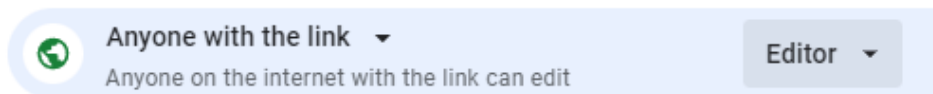
- ☒ Challenge #2: Lots of Jobs!
- ☒ Challenge #3: Hostage
- ☒ Challenge #4: 11,185,272
- ☐ Challenge #5: Read Me
- ☐ Challenge #6: Three Even, Two Odd
- ☒ Challenge #7: Shifty
- ☒ Challenge #8: Encoded Message
- ☐ Challenge #9: Kasiski Who?
- ☐ Challenge #10: But are there eggs?
- ☐ EXTRA Challenge #11: Arch EXIF!

### Submit your work!

Step 1: **Click** the Share button at the top of your screen double check that anyone with the link can edit. (This allows our grading team to input your grade below!)



#### General access



Step 2: **Copy** the link to this document.



Step 3: **Submit** the link on the portal.

### Grader Comments

*Once your project has been assessed, our graders will leave feedback for you in this space. Please do not delete.*

### Grading Rubric

Reflection Questions	Total Received Points	Total Possible
Reflection Question #1 answered above	2	2
Reflection Question #2 answered above	2	2
<b>PART A TOTAL</b>	4	<b>4</b>
CTF Challenges	Total Received Points	Total Possible
Complete 3+ CTF challenges and document your process	6	6
Complete 6+ CTF challenges and document your process	6	6
Complete 9+ CTF challenges and document your process	0	(+2 bonus)
Complete all 11 CTF challenges and document your process	0	(+2 bonus)
<b>PART B TOTAL</b>	<b>12</b>	<b>12 (+4)</b>
<b>Total Possible Points (Part A + Part B)</b>	<b>16</b>	<b>16 (+4)</b>

### Grader Feedback

Nice work! You've successfully completed the first assignment and taken your first step towards building a Cybersecurity mindset!