

# Cyber Connexion Self-Assessment

Cyber Connexion Admissions Team

The questions in this self-assessment are not meant to be hard knowledge requirements for admission to the program. You should instead view them as samples of the kinds of prior knowledge that will be strong assets for program applicants. If you can answer some or all of these questions, and are excited to fill in your knowledge gaps on the others, then you might be a great fit for the program! If you do not know how to answer any of these questions, you should consider reaching out to staff to see if the program is right for you.

## 1 Linux Command Line

Write a bash command that will write the names of all files in the current directory which have a “.log” file extension into a file called “logs.txt”. If logs.txt does not already exist, your command should create it. If logs.txt does exist, you should append the file names to the existing contents.

## 2 Modular Arithmetic/Number Theory

- (a) Compute  $\phi(7387)$ , where  $\phi$  denotes Euler’s totient function.
- (b) Find the multiplicative inverse of 7 modulo  $\phi(7387)$ .
- (c) Suppose  $0 \leq x < 7387$  and  $x^7 \equiv 4 \pmod{7387}$ . Find the value of  $x$ .

## 3 NIST Cybersecurity Framework

Name, and briefly describe, the core 5 functions from the NIST cybersecurity framework.

## 4 Computer Networking

How many IP addresses are available for assignment on a network with network address 64.231.128.0 and subnet mask 255.255.248.0?

## 5 Cryptography

**Bonus points if you include the answer to this question in your application!** You may find it helpful to write some code to assist you.

Consider the encryption scheme that encrypts English words of 13 characters or less in the following way:

1. A secret key consisting of a list of 13 random integers between 0 and 26 inclusive is set.
2. Every letter is translated into an integer from 0 to 25 inclusive ( $a = 0$ ,  $b = 1$ ,  $c = 2$ ,  $\dots$ ,  $z = 25$ ). The text is now a list of numbers.
3. If the word is less than 13 characters long, the number 26 is repeatedly added to the end of the list until the length is 13. For example,  $[1, 2, 24, 5, 13, 14, 2, 1]$  would become  $[1, 2, 24, 5, 13, 14, 2, 1, 26, 26, 26, 26, 26]$
4. The resulting list is added modulo 27, element by element, with the secret key. For example, the sum modulo 27 of the lists  $[1, 2, 3, 4]$  and  $[26, 3, 25, 1]$  would be  $[0, 5, 28, 5]$ .
5. The encrypted list of numbers is translated back to a string of letters, with the number 26 decrypting to a colon (':') character.

As an example, if the secret key was  $[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13]$ , then the word 'canada' would encrypt to 'dcqeigghijklm'.

3 words were encrypted using the above scheme. The encrypted words are:

1. 'fxvxgfcbsimfx'
2. 'edqmnrcbsimfx'
3. 'fdzmejhem:vzv'

Find all 3 words. Find the secret key, and use it to encrypt the word 'cryptography'