

# Cybersecurity & Cryptography Lab

## Overview

In today's lab, you are going to explore Cybersecurity and Cryptography. The lab will be broken down into three parts: Password Hashing, Ciphers, and Cybersecurity Research.

In part 1, you will implement password hashing into a signup/login page. You will need to be able to hash a user's password, and save the hash into your local database. Then a user must be able to sign in with their password.

In part 2 you will create your own cipher... and code it out too!

In part 3 you will research any major security breach over the past 20 years and write a short response to it.

## Part 1 - Password Hashing

Download the material for today's lab and open it in VS Code. You will notice you already have a front-end and back-end setup. The front end has two options, log in and register. These two options are linked to two different endpoints, `/api/login` and `/api/register`, respectively.

Install `bcryptjs` and require it in your controller file. Then build out the `register` function to hash the users password and then store that new user to the local database of users. Note: You should be storing all properties on the user object, except the password. Instead, you should be storing the password hash.

Then build out the `login` function to receive a username and password. First, make sure the username exists in the database, if it does, compare the password being passed in to the hashed password in the database with the appropriate `bcrypt` method. If the password is correct, send a copy of the user object back to the front-end. However, make sure you delete the hashed password off of the object copy you send.

## Part 2 - Ciphers

Open up a text editor and create your very own cipher. State all the logic behind your cipher. Then, using your cipher, encipher the phrase “I love cryptography!” Display the result. Using your cipher again, decipher the ciphered phrase. Do you get “I love cryptography!”?

Take this one step further and create your cipher in code.

## Part 3 - Cybersecurity Research

1. Research major cybersecurity breaches over the past 20 years and pick one to write a short essay on.
2. Give an overview of what the breach was and the motivations behind it.
3. Explain where the “tech flaws” were, and how hackers were able to breach their system.
4. What has the company done to protect against that vulnerability since?

## Submit

Initialize a git repo containing all your work and push it to GitHub.