**Big Idea 5.5**

1. The GNU GPL v2.0, MIT License, Apache License 2.0, and GNU GPL v3.0 are just a few of the license types you can choose from when creating a repository on GitHub. Under each of these licenses, your repository must continue to be an open source of code with various access restrictions for users. For instance, the MIT License permits third parties to use, modify, and distribute the owner's software without having to pay the owner a dime. This license is probably the most typical for this class as long as you include the original copyright and license notice in any copies of the software or source.
2. I learned that there are many options depending on how private the software's owner wants it to be and that licensing is quite complicated. Digital rights are crucial because they enable distributors, streaming music services, and social media platforms to negotiate deals with online users.
3. It already had an Apache License v2 installed when I copied my personal blog from the template. Because we want anyone who uses our code to give us credit and acknowledge the license, we have a MIT License for our group frontend repository. The same holds true for our backend repository. It was necessary to create a file called LICENSE and add or update a license using the GitHub MIT License template.

**Big Idea 5.6**

1. In order to use Slack, we had to create an account, and since we signed up for Google accounts, Slack now has access to the personal data that was kept there. In terms of our group project, we will only collect a user's full name so that it can be shown on the leaderboard. The additional data that will be gathered includes the token count, user ID, and password. Personal information and emails will not be gathered.
2. My mother is a software engineer for Sony, and she is aware of the risks associated with disclosing personal information online. As a result, she has taught me to use PII online with the utmost caution. Because of this, whenever I've had the chance, I've opted not to customize accounts or enter personal information, keeping my online identity a secret. She advised me to check to see if some websites were saving even my passwords.
3. A bad password might be something like a well-known phrase or a string of characters that are simple to decipher, while a good one might be based on an inside joke or the language you speak in another country. Additional authentication assistance is provided by 2FA. As a result of the requirement for accurate account information, it is extremely secure. It operates by sending you a code to the phone number or email associated with your account. This code must be entered for it to confirm that you are the person attempting to access your account.
4. Symmetric encryption is the process of scrambling or encrypting a single string of characters in one step and then decrypting it in the same steAsymmetric encryption protects data by encrypting it with both a public and private key. n. The deploy and security keys are configured in my fastpages repository in the manner described above.
5. In AWS, we created the instance using symmetric encryption.
6. I don't recall ever being the target of a phishing attack, but I am aware that email is one of the most common methods. In order to hide their scam, phishers will attempt to appear to be part of an organization.