1. **Title:** Vulnerable Password Storage in Python
   * **Explanation:** Develop a simple Python script that takes a user's password as input and saves it to a file. However, the storage mechanism should be flawed in some way, such as saving the password in plaintext without any encryption. This assignment serves to illustrate the risks associated with insecure password storage and the importance of using proper encryption techniques.
2. **Title:** Analysis of a Major 2022/2023 Data Breach
   * **Explanation:** Conduct a thorough study on one of the major data breaches that occurred in 2022 or 2023. This should cover the timeline of events leading up to the breach, the vulnerabilities exploited, the data that was compromised, and the aftermath. Additionally, provide recommendations on how similar breaches can be prevented in the future. This assignment emphasizes the real-world implications of cybersecurity lapses and the importance of proactive security measures.
3. **Title:** Exploring the Principles of PGP (Pretty Good Privacy)
   * **Explanation:** Dive deep into the world of PGP, a data encryption and decryption program that provides cryptographic privacy and authentication. In this assignment, you'll learn about the foundational principles behind PGP, how it uses both symmetric and asymmetric encryption, and its role in ensuring secure communications. Create a simple demonstration showcasing the process of encrypting and decrypting a message using PGP. This will provide hands-on experience and a deeper understanding of the cryptographic processes behind PGP.