**Team Members:** Jonah Simpson and Brennan Widner

For our midterm project, we successfully implemented a symmetric encryption algorithm and thoroughly enjoyed the process. Building on that experience, we now aim to explore asymmetric encryption by implementing one of its algorithms.

Asymmetric encryption is a cryptographic method that uses a pair of keys—a public key for encryption and a private key for decryption. Popular algorithms in this category include RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC). Compared to symmetric encryption, asymmetric encryption offers several advantages:

* Enhanced security through public/private key separation
* Utility for authentication
* Non-repudiation of messages
* Elimination of the need for secure key distribution

### **Research Questions**

Through this project, we aim to answer the following questions:

1. Are asymmetric encryption algorithms inherently more challenging to implement than symmetric ones?
2. What steps are required to create an application that can encrypt and decrypt data using asymmetric encryption?
3. Which asymmetric encryption algorithm is best suited for our use case?

### **Planned Approach**

To answer these questions, we will:

* Select an asymmetric encryption algorithm to implement (e.g., RSA, Diffie-Hellman, or ECC).
* Develop an application that demonstrates encryption and decryption using this algorithm.
* Present our findings and deliverables to the class, including the application and its underlying code, to showcase how the algorithm works in practice.

This project will deepen our understanding of cryptography and provide a practical demonstration of the power and versatility of asymmetric encryption