CS355 Project – Security Analysis
GitHub Repo URL: https://github.com/kyungjaepae/cs355_project

Project Specifications:

- Used C++ language for implementation
- Implemented El Gamal encryption scheme
- Used math library for key generation, modulus, etc.
- Used socket libraries

Security Goals:

- CPA secure
- public key cryptography

Security Analysis:

Our project achieves CPA security through the use of the El Gamal encryption scheme. Knowing that the DDH assumption is hard, we can confirm that the El Gamal encryption scheme is CPA secure. Our project is designed with Alice acting as the server and Bob acting as the client. Bob chooses an arbitrary large *int q* which is passed to the *gen_key* function to compute a key *int a*. Bob then computes *int q* (random number) and *int h* (g^a % q). Bob sends *q, g,* and *h* to Alice. Alice then encrypts her message using the *q, g,* and *h* variables sent from Bob. Alice then enters her encrypted message and private key into the *encrypted_message e* struct. Alice sends *e* back to Bob to decrypt and read as plaintext.

Our project utilizes public key cryptography. The client generates a public key which is then sent to the client's correspondants. The public key is used by each party to compute their own private key. In this scheme, a message can be encrypted by anyone through the use of the public key, but messages can only be decrypted by the private key of the intended recipient.