Requirements

Functional

Inputs:

1. User defined plaintext messages from keyboard
2. Ciphertext messages received from another user
3. (optional) Random numbers used for key establishment

Outputs:

1. Encrypted ciphertext made from user defined plaintext
2. Decrypted plaintext from another user

Data to be stored:

1. Key
2. (optional) Encrypted files

Computations to perform:

1. Key establishment (exponential modulation)
2. Scan user input from keyboard/clipboard and files
3. Using input, encrypt ciphertext
4. Send ciphertext automatically over discord
5. If ciphertext message is sent over sever, automatically download it
6. Decrypt message file and print to screen

Timing and Synchronization:

1. Key establishment and initialization of scheme will come first and should take no longer than a few seconds depending on user decisions.
2. All computations will be in real time based off user input and instantaneous

Non-functional

1. Languages to be used will be Python and JavaScript (for cross platform support)
2. Target user base is anyone to whom privacy and security are a concern, and who uses Discord to send 1 on 1 messages
3. Software functions are all quick, simple, and reliable. Once a message is read on one end it will be encrypted, sent, downloaded, and decrypted in under a second.
4. Once user messages are encrypted, it would require a computing time complexity of about 2^{248} to crack without the key. As of 2015 there are no known attacks to crack it. ChaCha20 is a variant of Salsa20, one of the few alternatives to AES widely used.