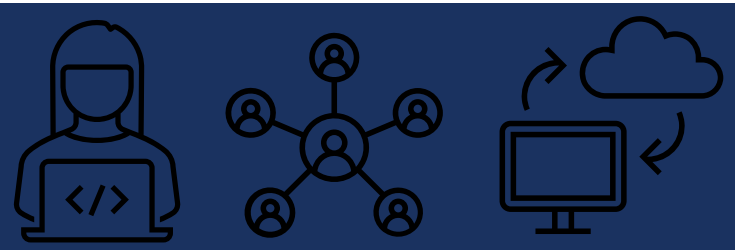
ChatGPT

GROUP 16: ARUSHI GHILDIYAL, ARABELLE BETZWIESER, CONNOR FRENCH, KENYON TINER, TYLER SAIZAN, ABBY DEBENPORT

- Not to be confused with that **Generative Pre-Trained Transformer**
- This is Chat **Good Private Talking**

TEAM BREAKDOWN

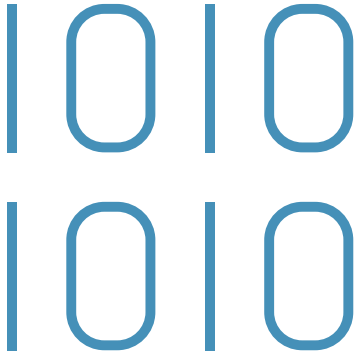


- Encryption:
  - Arushi Ghildiyal : Encryption/ Decryption
  - Connor French : Key generation
  - Kenyon Tiner : Secret Stream API
- Networking:
  - Arabelle Betzwieser : Asio library
  - Tyler Saizan : Data Flow of Messages
  - Abby Debenport : User Authentication

Overview

Networking

+



Encryption

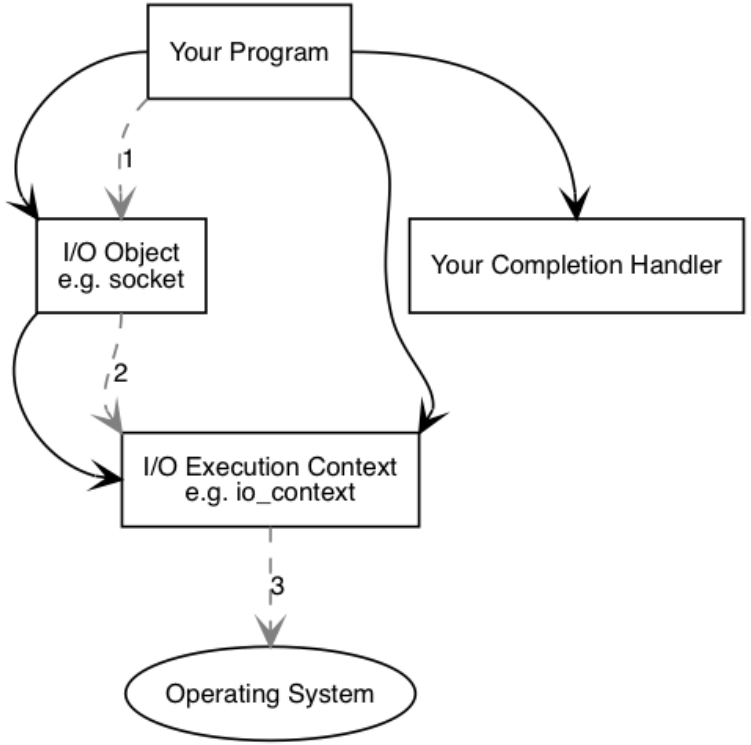
=

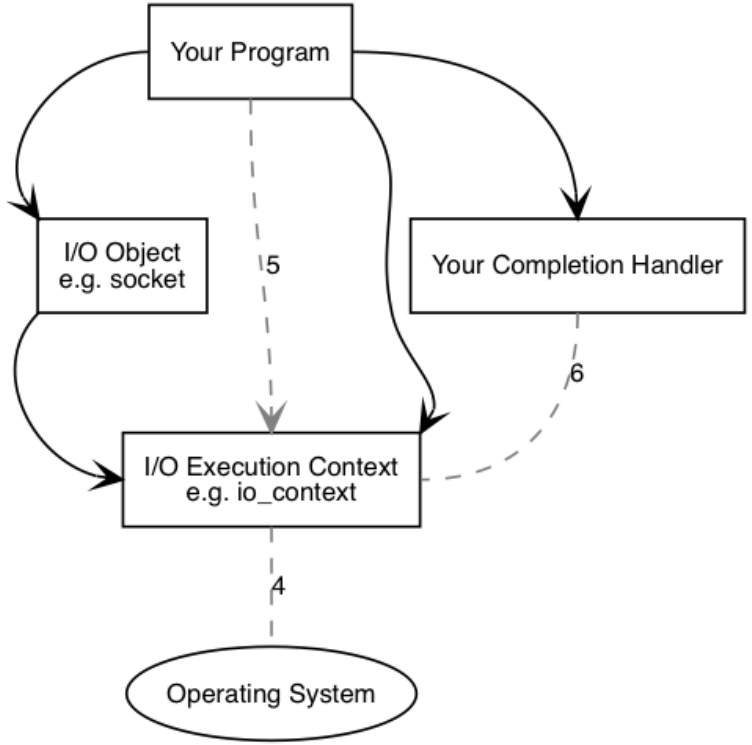
Safe and Secure Communication Line

CREATING AN ENCRYPTED COMMUNICATION CHANNEL

ASIO

- Asio networking library
  - asynchronous I/O functions
    - async_read, async_write
  - Transmission Control Protocol / Internet Protocol – TCP/IP
    - socket, acceptor
  - io_context handles asynchronous tasks



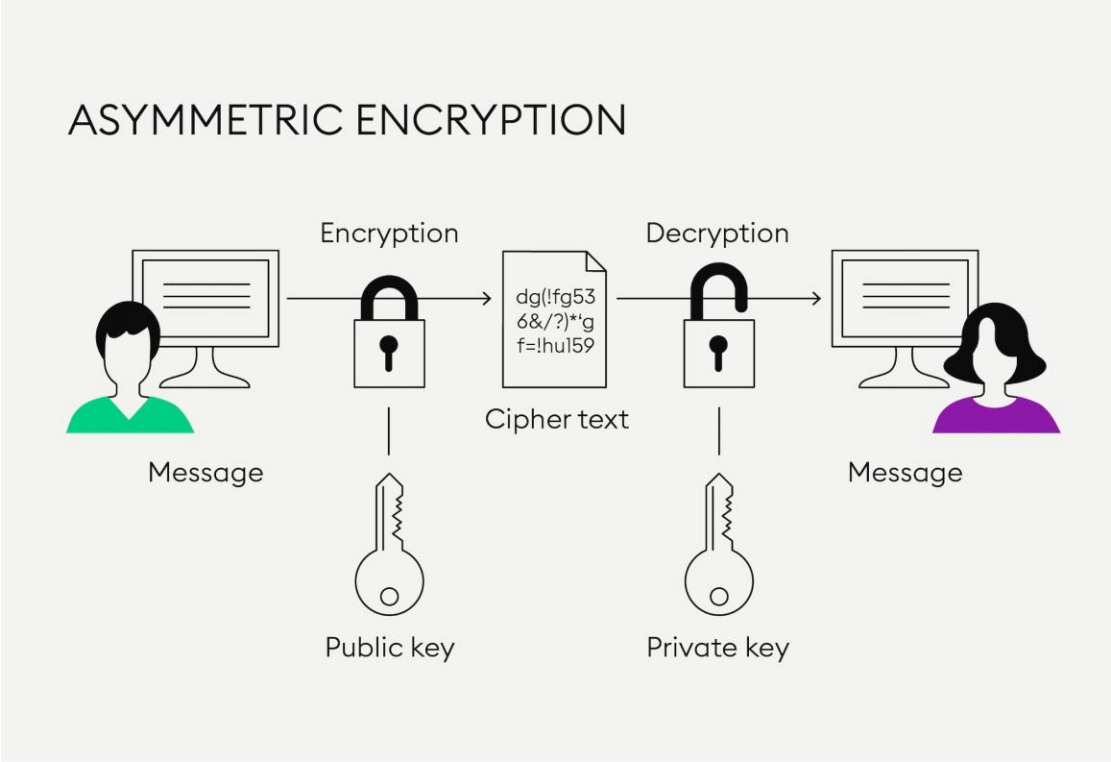


LIBSODIUM

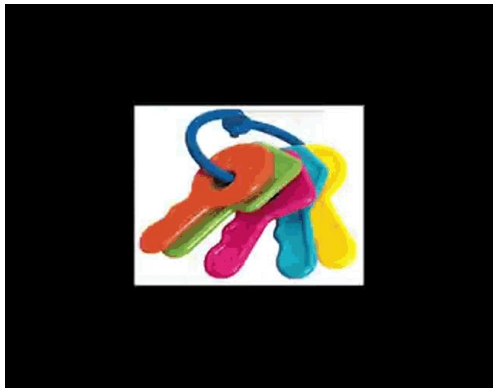
- Open Source Library
  - Encryption/ Decryption
  - Hashing
- Packageable fork of NaCL (Networking and Cryptography Library)
- Symmetric Encryption and Asymmetric Encryption

ENCRYPTION/ DECRYPTION

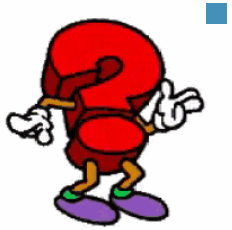
- Using Public Key Encryption Aka Asymmetric Encryption
- Libsodium uses various robust algorithms for different encoding tasks
  - Argon2, AES-GCM, ECC, xSalsa20,



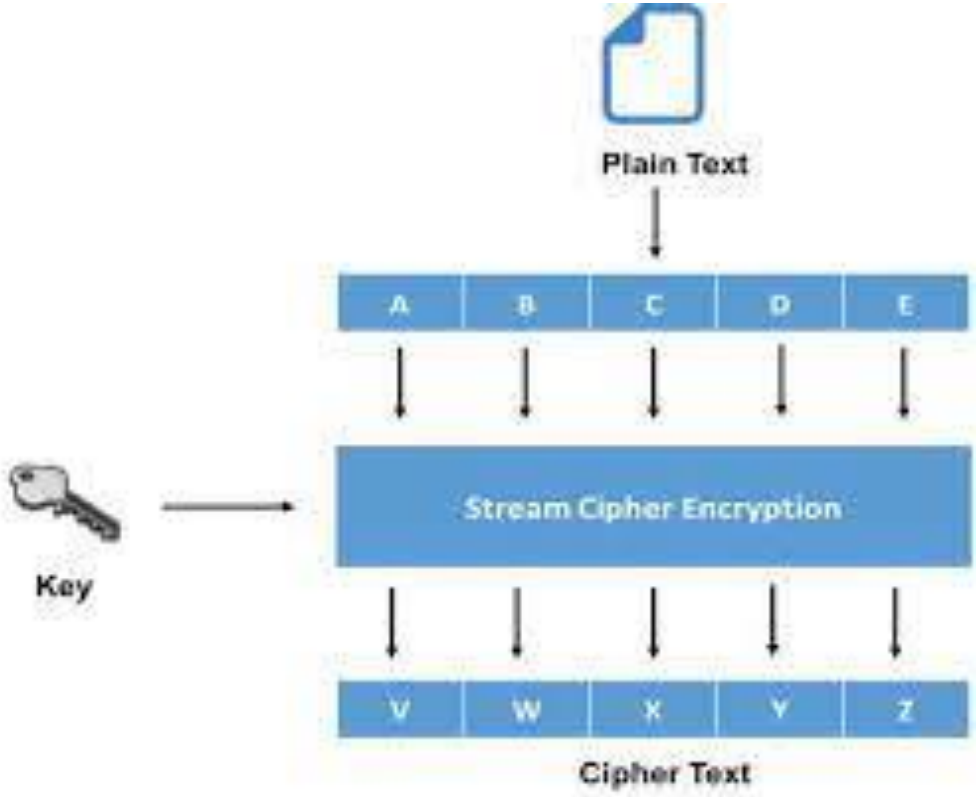
key generation



- password + salt, stretch it out, bake for 0.7 seconds
- delicious password hash, hot and ready
- take the hash, use it as a seed to grow a beautiful public and private key pair
- keys live in memory until (humanely) destroyed at end of session



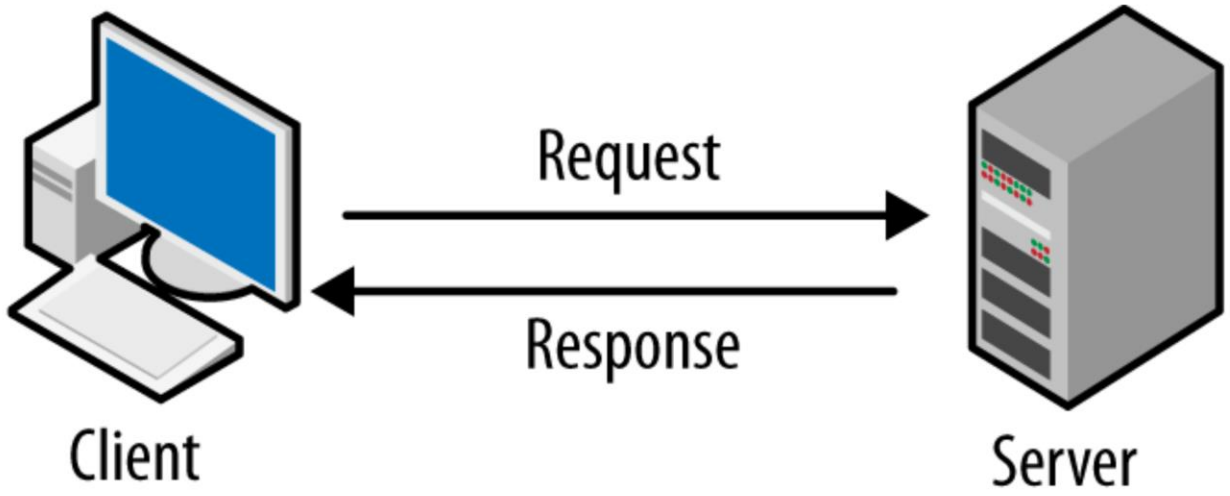
SECRET STREAM API



- Allows for related messages to be encrypted sequentially, using the same public and private key pairs.
- secretstream() over standard secretbox():
  - An open stream allows for constant message encryption which is more efficient for real time communication
- Essential Functions:
  - crypto_secretstream_*_push() - Used to create encrypted data stream
  - crypto_secretstream_*_pull() - Used to "pull" decrypted counterpart
  - crypto_secretstream_*_TAG_PUSH - Signals the end of a set of messages, without closing data stream
  - crypto_secretstream_*_TAG_FINAL – Signals the end of data stream and purges key pairs
  - Where " * " = chosen encryption method

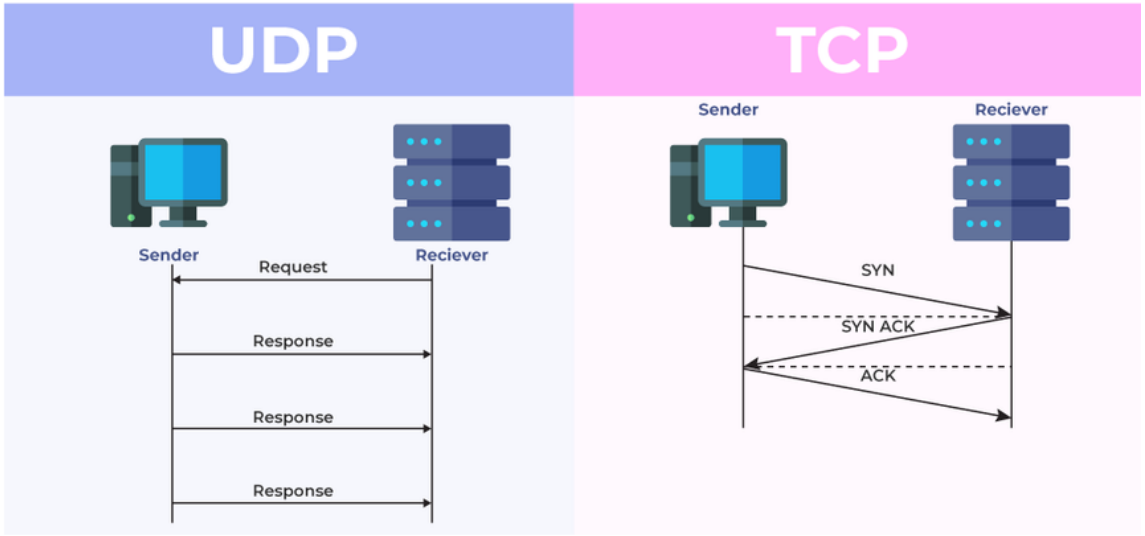
NETWORKING DESIGN

- 2-tier network architecture: server-client
- Asynchronous server
  - Allows servicing concurrent client requests
  - Non-blocking; don't need to wait for one operation to complete to continue a task



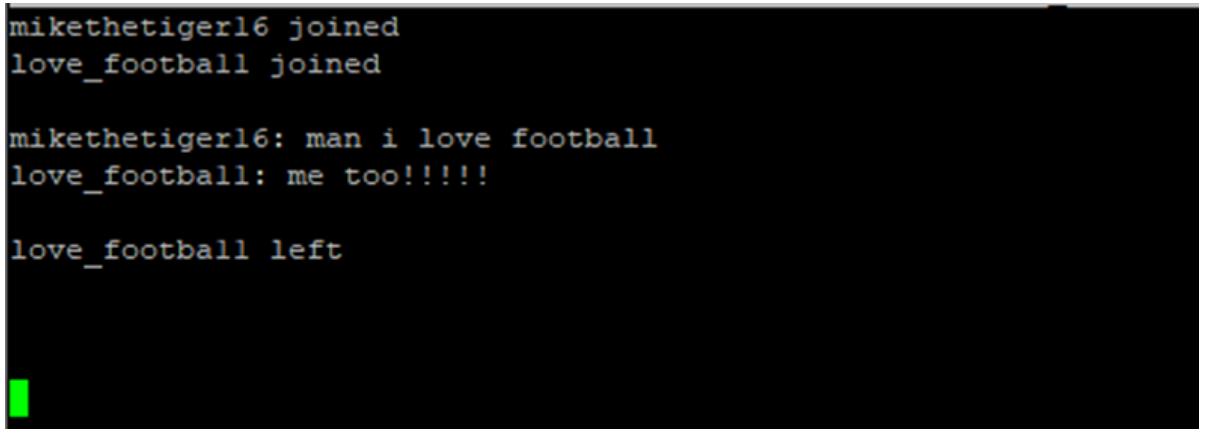
WHAT IS A MESSAGE?

- Asio moves datas into buffers
- These buffers are sent by the OS via TCP sockets
- These "messages" contain all communicated data
- Need to classify messages
  - Homemade headers on strings
  - Logics handles message after reception based on header



USER INTERFACE

- Authenticating
  - User registration
  - Check user inputted password's hash to saved hashes in server files
- Command line interface
- Stretch features
  - GUI
  - Emoticons



THANK YOU

NAMES WE DIDN'T CHOOSE

- C.R.U.S.T. – Controlled Relationships Undertaking Secure Transmission
- S.H.H.H.H – Secure, Hidden, Heavily encrypted, Hush-Hush, High-security
- H.I.D.E.M. – Highly Impenetrable Data Encryption Messenger
- C.L.O.A.K. – Completely Locked Over All Keys

for real this time

Thank You

Address
street number,
city, state

Contact
Numbers:
0123456789

Email Address:
emailaddress@
gmail.com