# 428 Project: SecureDove

Team LMMT

# Project Topic

We developed a web chat application called SecureDove. We implemented two major kinds of encryption: symmetric and asymmetric.

Goals:

- Multiple rooms with multiple users
- Rooms are secured
  - Difficult to enter without given explicit permission
- Chat messages are secured
  - Encrypted
  - Rebroadcastable

# Team Members

- Matthew Gerola - Contributed back end reorganization
- Logan Kloft - Contributed symmetric code, asymmetric code, communication format design and implementation, and user interface design and implementation
- Manjesh Puram - Contributed user interface polishing and username criteria checking
- Taylor West - Contributed asymmetric encryption code and deployed environment

# Demo Application

# Lessons Learned & Experience Gained

- Mechanisms for protecting a server from threat actors can be different than mechanisms used to protect a client from threat actors
    - For chat rooms we generate a hard-to-guess room key. Whereas for servers, we ensure functionality is only accessible through well-defined and regulated interfaces - ignore improper communication.
- How to effectively use WebSockets for communication and how one might secure WebSockets
    - We define our own http-like communication standard and secure through symmetric encryption
- How to protect from information leaks caused by poor uniqueness criteria or lifetime constraints
    - Client-side and Server-side input validation checking
- How end-to-end encryption and Diffie-Hellman work
    - Implemented Diffie-Hellman key sharing algorithm to perform E2E encryption via symmetric encryption
- How symmetric encryption can be used in a real-time application
    - Use a well-established library that provides symmetric encryption such as the Fernet or AES ciphers for example
- How to interface between JavaScript and Python using different libraries for WebSockets and Public / Private Key Encryption
    - Trial and error to satisfy library interfaces or use libraries that are ported over from Python to JavaScript or the other way around.

# Link to Youtube Video

https://m.youtube.com/watch?v=zypGUbhqbPk