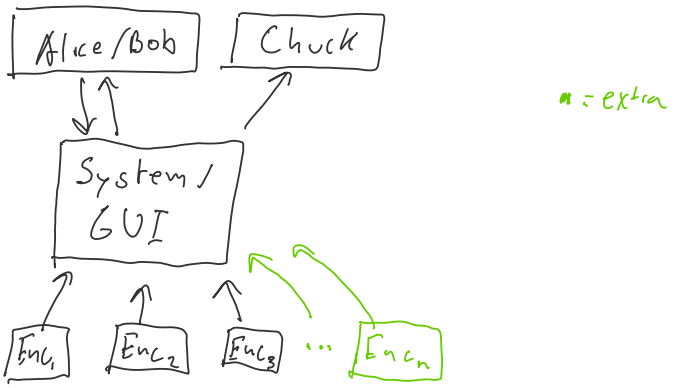
419 Crypto

Tuesday, February 11, 2020 5:27 PM

General layout:



Minimal Requirements:

Users:

Alice/Bob

- Ability to send and receive information
- 3 ciphers(Enc) from scratch
- System can give Alice/Bob same keys
- I think we can all agree functionally there is no difference between Alice and Bob
  ie: if we make Alice then Bob, Emily and the gang are done by default
- Owner's can receive public and private keys(want to ask prof to define what "owner" means in this context

Chuck:

- Can query system for:
  Cipher text only, known plaintexts, chosen plaintexts, and chosen cipher texts
- Basic toolbox for above querying:
  Frequency analysis(not sure if that's something we implement on our side) and brute force(whatever that means, will ask prof to clarify)
- Chuck **NEVER** gets the key
- When Chuck gets the text they query for, call decryption and pass the chosen string + chosen key

Extra Mile:

Everything from above + these changes to user:

Alice/Bob/Emily/Etc

- Support multiple users to communicate with each other
- Key exchange and agreement protocol
- Multiple key protocols(Shred key, PKE)
- More than the 3 from scratch algorithms(can reuse existing algorithms)

Alice/Bob and Chuck are very similar

Way to distinguish alice and bob can send one value, while chuck sends another
Chuck gets access to toolbox and toolbox lets him do all the fun security calls(like CPA CCA whatever else)
Alice/bob only send message to system and receive encrypting strings, have to ask system for decryption after