6.857 - Welcome!

Syllabus:

- Intro: security policies
  Kilian
  OTP
- Encryption: PRF, CPA, AES, MACs, CCA
- Hash fns: collision-resistance, one-wayness
  SHA-256, SHA-3
  applications

- Math: secret-sharing
  DH key exchange
  assume "discrete log" is hard
  elliptic curves
- PK crypto: El Gamal, RSA, digital signature
  ring signatures
- cryptoprotocols: ID schemes
  ZK proofs: zero knowledge
  Fiat-Shamir

- Topics: Contact tracing
  Crypto currencies!
  Voting
  Post-quantum, FHE
  fully-homomorphic encryption

- Guest lectures: TBD
- Project presentations

Projects:

"About security"

"Interacting"

"No jail"

- Baseball signs
- Enigma
- Secure "battleship"
- Password mgrs

¬ MIT (card)

Content:

Security is about computing or communicating in the presence of **Adversaries**

System: desired functionality

Security policy: what is not supposed to happen

e.g. "each voter should be able to vote at most once"

Security has 3 flavors "CIA":

Confidentiality:

Integrity:

Availability:

Security mechanisms: way of achieving goals

- Prevention:
- Detect & Recover

Who is Adversary?

- what does Adversary **know**?
- what resources does Adv have

well-resourced

- identification
- authentication
- authorization
- physical protection

- cryptography
- economics
- **randomness**