6.857 - Welcome!

1/31/2022

Syllabus:

Intro: security policies, Kilian lecture, OTP

Encryption: PRF, CPA or CCA, AES
MACs

Hash fns: collision-resistant, applications
SHA-256, SHA-3

Math: secret-sharing, DH key exchange
elliptic curves

PK crypto: El Gamal, RSA, digital signature

crypto protocols: ID schemes, ZK proofs, Fiat-Shamir

Topics: Find My
Voting
Post-quantum, FHE

Guest-lecturers: HCG, SB

Projects: | About security
Interesting
No jail

- Baseball
- Enigma scheme
- Secure games
- Password mgrs
- MIT card - no!

Security is about communicating or computing in presence of Adversary

Information system: everything is digital

Defined: roles
information items
functional requirements
} supposed to happen

Security: what should not happen?

Security policy: principals (roles)
giving permissable actions are possible
and what are not

Examples: Each registered voter may vote at most once.
Only an administrator can modify this file.

Security goals: ("CIA" triad)

Confidentiality

=

Integrity

=

Availability

=

Security mechanisms: (security controls)

= end