

Midterm Review 461

- in class next week • 8.5x11" double sided HANDWRITTEN ^{cheat} sheet
- Calculator

- Topics

- Everything that has been covered

- Videos, papers, lectures, HW

• Cryptographic hash fns

• Properties

- Uses

- Merkle trees

- Merkle proof

- Bitcoin Blockchain construction

- Terms

- Data structure (blocks & tx) tree & DAG

- Header contents

- Proof of Work

- $\text{hash} < \text{target}$

- Why?

- Difficulty adjustment

- Double spend attack concept & eqn

- Probability Poisson Process, basic probability

- Selfish mining

- Sybil attack

- 4 Lemmas (fifth - can't tell whether
being sybil attacked)

NOT

• No python programming

• No ECC formation!

• No deriving Double spend
eqn.

Brick app

(apple)

- Group theory
- Formation & properties
- $\mathbb{Z}_p^+$ $\mathbb{Z}_p \leftarrow$ integers mod p group op is either $*$ or $+$

- Bitcoin Networking

- eclipse attack
 - Lamport's Logical clock
 - totally ordered messages
 - Bloom filters, IBLT, cuckoo filter
- graphene

Attacks

- Double spend
- eclipse
- Sybil
- Schnorr exploits
- 51% attack



