CSE 539: Applied Cryptography

Class: 09 **Date:** 1/9

Spring 2018

Note Title

Textbook — ? Bruce Schneier

reference — wikipedia

Web page

Prerequisites — CS degree

Cryptography & Security

→ part of ↗

Overlap with other classes

Number theory → x ↦ sym encr x
↳ hash functions
↳ asym encryption

↳ integers

↳ positive

↳ finite set

prime #s

# of prime # $\rightarrow \infty$

300 BC - Euclid

$p \rightarrow$ largest prime

$((1 \times 2 \times 3 \times 5 \times 7 \cdots \times p) + 1)$

↑ prime? $\rightarrow$ Yes

$\rightarrow$ No

Course coverage

- INTRO → random #s
  → hash functions
  → sym encryption
  → asym "