Announcements

- Exam 3 available now
  - Due Thursday, December 3 @ midnight
  - Two files to upload: Exam questions and essay
- Office hours posted to onCourse

Few final points

- All of our secure cryptographic methods depend upon some hard underlying math problem
  - RSA: Difficulty of factoring large integers
  - DHKE, DSA: Discrete log problem
  - AES: Brute force only *known* vulnerability

- In principle, all easy to break
  - Only a finite number of possibilities
  - Just go down the list until you find your solution!

- However, not *practical* if number of possibilities is extremely large

- We've seen a few algorithms to simplify computations
  - Extended Euclidean algorithm for finding $a^{-1} \mod n$
  - Square and multiply algorithm for computing $a^k \mod n$

Cryptography - It's not just for secret messages

- Hash functions can ensure integrity (e.g. digital resources not modified)
- Hash functions and digital signatures used in underlying framework for Bitcoin
- AES used in solid state drives
- Examples from Crypto in the News

Next Semester

- Assume we have a secure symmetric key system (like AES)
- Focus on public key cryptography
- How do we find large primes?
  - Need p and q to form $n = pq$ for RSA
  - Need p where $p - 1$ has a large prime factor for DHKE
  - Need p and q where $q|(p - 1)$ for DSA
- How can we attack the DLP?
  - Shanks' Babystep-Giantstep algorithm
  - Pohlig-Hellman algorithm

    Shows why want α to have large prime order in DHKE
  - Pollard's ρ -algorithm

    General purpose algorithm can also be used to factor $n = pq$

Next Semester (cont)

- Understand Elliptic Curve Cryptography (e.g. ECDHKE)
- And it all falls apart once Shor's algorithm can be implemented
  - Shows need for new methods
  - Look at framework for lattice-based methods, like NTRU
- Group presentations on topics of student interest

An Introduction to Mathematical Cryptography, 2nd edition

by Hoffstein, Pipher, Silverman

ISBN 978-1-4939-1710-5