CS530
Public Key Cryptography

Bill Cheng

http://merlot.usc.edu/cs530-s10

Copyright © William C. Cheng

Public Key Cryptography

- aka asymmetric cryptography
- Based on some NP-complete problem
  - traveling salesman problem
    - *n* cities, connected
    - find shortest tour, all cities must be visited
    - solution complexity is *n!*
  - unique factorization
    - factor an integer into product of prime numbers (unique solution)
  - discrete logarithms
    - for any integers *b*, *n*, *y*: Find *x* such that $b^x \bmod n = y$
    - modular arithmetic produces folding

Copyright © William C. Cheng

A Short Note on Primes

- Why are public keys (and private keys) so large?
  - because key space is *sparse*
- What is the probability that some large number *p* is prime?
  - about 1 in *1/ln(p)*
    - 2 digit numbers: 25 primes (1 in 4)
    - 10 digit numbers: 1 in 23 are primes
    - 100 digit numbers: 1 in 230 are primes
    - but... the more digits, the more primes!
  - when $p \approx 2^{512}$ ($\approx 10^{150}$), equals about 1 in 355
    - about 1 in 355^2 numbers $\approx 2^{1024}$ is product of two primes (and therefore valid RSA modulo)

Copyright © William C. Cheng