CSE 321 Discrete Structures

Winter 2008
Lecture 11
Number Theory: Applications

Announcements

- Readings
  - Friday:
    - Applications of Number Theory
      - 3.7 (5th Edition: 2.6)
  - Next week
    - Induction and recursion
      - 4.1-4.2 (5th Edition: 3.3-3.4)
  - Midterm:
    - Friday, February 8

Highlights from Lecture 10

- Primality
  - Discrete Log Problem
  - Euclid's Theorem
    - Infinitude of Primes
  - Density of Primes
  - Factorization vs. Primality Testing
  - Probabilistic Primality Testing

Greatest Common Divisor

- GCD(a, b): Largest integer d such that d|a and d|b
- GCD(100, 125) =
- GCD(17, 49) =
- GCD(11, 66) =

Euclid's Algorithm

- GCD(x, y) = GCD(y, x mod y)

```
int GCD(int a, int b){   /* a >= b,   b > 0 */
      int tmp;
      int x = a;
      int y = b;
      while (y > 0){
            tmp = x % y;
            x = y;
            y = tmp;
      }
      return x;
}
```

Extended Euclid's Algorithm

- If GCD(x, y) = g, there exist integers s, t, such sx + ty = g;
- The values x, y in Euclid's algorithm are linear sums of a, b.
  - A little book keeping can be used to keep track of the constants

Chinese Remainder Theorem

Find an x in [0 . . . 11484] such that

x mod 11 = 9
x mod 29 = 7
x mod 36 = 14

Simple version:
Suppose: p, q prime
$x \equiv a \pmod{p}$
$x \equiv b \pmod{q}$
What is x mod pq ?

p, q prime, x mod p = a, x mod q = b

- Choose s, t such that sp + tq = 1
- Let f(a, b) = (atq + bsp) mod pq
- f(a, b) mod p = a; f(a, b) mod q = b
- f is 1 to 1 between $[0..p-1]\times[0..q-1]$ and $[0..pq-1]$
- Corollary:
  - x mod p = a; x mod q = a, then x mod pq = a

Cryptography

Perfect encryption

- Alice and Bob have a shared n-bit secret S
- To send an n-bit message M, Alice sends $M \oplus S$ to Bob
- Bob receives the message N, to decode, Bob computes $N \oplus S$

Public Key Cryptography

- How can Alice send a secret message to Bob if Bob cannot send a secret key to Alice?

My public key is:

13890580304018329082310291
80219821092381083012982301
91280921830213983012923813
20498068029809347849394598
17847938828739845792389384
89288237482838299293840200
10924380915809283290823823

RSA

- Rivest – Shamir – Adelman
- n = pq. p, q are large primes
- Choose e relatively prime to (p-1)(q-1)
- Find d, k such that de + k(p-1)(q-1) = 1 by Euclid's Algorithm
- Publish e as the encryption key, d is kept private as the decryption key

Message protocol

- Bob
  - Precompute p, q, n, e, d
  - Publish e, n
- Alice
  - Read e, n from Bob's public site
  - To send message M, compute $C = M^e \bmod n$
  - Send C to Bob
- Bob
  - Compute C^d to decode message M

Decryption

- $de = 1 + k(p-1)(q-1)$
- $C^d \equiv (M^e)^d = M^{de} = M^{1 + k(p-1)(q-1)} \pmod{n}$
- $C^d \equiv M\,(M^{p-1})^{k(q-1)} \equiv M \pmod{p}$
- $C^d \equiv M\,(M^{q-1})^{k(p-1)} \equiv M \pmod{q}$
- Hence $C^d \equiv M \pmod{pq}$

Practical Cryptography