Chapter 11 Cryptology

Jason Pearson and Sam Demorest

March 30, 2015

Overview

Number Theory
- Composite and Prime Numbers
- Greatest Common Divisor
- Prime Factorization
- Least Common Multiple

Euclid's Algorithm
- Euclid's Algorithm
- Extension to Euclid's Algorithm

Modular Arithmetic
- Group Theory
- Congruency Modulo n
- Subgroups

Solving Modular Linear Equations
- Solving Modular Linear Equations

Computing Modular Powers
- Computing Modular Powers

Finding Large Prime Numbers
- Searching for a Large Prime
- Checking if a Number is Prime

RSA Public-Key Cryptosystem
- Public-Key Cryptosystems
- RSA Cryptosystem

Composite and Prime Numbers

Composite Numbers have a divisor other than itself and one.
For example $4|20$ means that $20 = 5 * 4$
The divisors of 12 are 1,2,3,4,6 and 12
Prime numbers have no divisors but 1 and itself
First 10 Primes
2, 3, 5, 7, 11, 13, 17, 19, 23, 29

Greatest Common Divisor

A common divisor is a number that is a factor of both numbers

For example gcd(12,15) $= 3$

The greatest common divisor is the largest factor for both numbers

Prime Factorization

Every integer X $>$ 1 can be written as a unique product of primes
That is X $=$ $p_1^{k_1} * p_2^{k_2} * \ldots * p_n^{k_n}$
Where $p_1 < p_2 < \ldots p_n$ and this representation of n is unique
Example being $22{,}275 = 3^4 * 5^2 * 11$
There is no polynomial time algorithm for finding determining the factorization of an integer

Least Common Multiple

Euclid's Algorithm

Extension to Euclid's Algorithm

Group Theory

Congruency Modulo n

Subgroups

Solving Modular Linear Equations

Computing Modular Powers

Searching for a Large Prime

Checking if a Number is Prime

Public-Key Cryptosystems

RSA Cryptosystem