Computer Security

Number Theory:
Divisibility, Prime Numbers,
Greatest Common Divisor,
Relative Primality
Groups, Rings and Fields

Why?

- Modern cryptography is based on ***Number Theory***, a branch of mathematics concerned with the properties of integers.
- In order to understand how modern cryptographic techniques work, and to estimate the extent to which they are secure, it is important to understand the basics of number theory.
  - We'll try to keep it as simple as possible!

Sources

- *The Basics of Abstract Algebra,* Paul E. Bland, Freeman
- *Introduction to Cryptography with Java Applets*, David Bishop, Jones & Bartlett
- *Practical Cryptography*, Niels Ferguson and Bruce Schneier, Wiley
- *Concrete Mathematics*, Graham, Knuth, and Patashnik, Addison-Wesley
- *Network Security: Private Communications in a Public World*, *Second Edition* Charlie Kaufman, Radia Perlman, Mike Speciner, Prentice-Hall
- *Applied Cryptography: Protocols, Algorithms and Source Code in C, Second Edition,* Bruce Schneier, Wiley
- *Cryptography and Network Security: Principles and Practices*, William Stallings, Prentice-Hall
- and a number of web sites...

Divisibility and Divisors

- We say that ***m* divides *n*** (or ***n* is divisible by *m*)** if:
  - $m > 0$

  and:
  - the ratio $\frac{n}{m}$ is an integer.
- This property underlies all number theory, so we have a notation for it:

$$m \mid n$$

and we say that *m* is a ***divisor*** of *n*

Divisibility and Divisors

- Here are some relations:
  1) If $a|1$, then $a = \pm 1$
  2) If $a|b$ and $b|a$, then $a = \pm b$
  3) Any $b \neq 0$ divides 0
  4) If $b|g$ and $b|h$, then $b|(mg + nh)$ for arbitrary integers m and n
  5) If $a|b$ and $b|c$, then $a|c$
  6) If n is a positive number > 1, and d is the smallest divisor of n that is greater than 1, then d is prime.

Prime Numbers

- A positive integer p is called ***prime*** if it has just two divisors: 1 and p
- A positive integer that has three or more divisors is known as a ***composite***.
- Every integer > 1 is either prime or composite, but not both.
  - Note:
    - 2 is a prime
    - 1 is ***not*** a prime
- The sequence of primes starts:

  `2,3,5,7,11,13,17,19,23,29,31,37,41,...`

Prime Numbers

- Primes are important because they form the fundamental building blocks of all the positive integers:
  - Any positive integer n can be written as a ***product of primes***:

$$n = p_1 \cdot p_2 \cdot \ldots p_m = \prod_{k=1}^{m} p_k \qquad (p_1 \leq p_2 \leq \cdots \leq p_m)$$

  and ***this expansion is unique*** – there is only one way to write n as a product of primes in non-decreasing order.

- This is known as the ***Fundamental Theorem of Arithmetic***

Prime Numbers

- There are ***an infinite number of primes***
  - *Euclid's proof:
    - Assume that there are a finite number of primes
    - Call the list of primes $p_1, p_2, \ldots p_k$, where k is the number of primes
    - Define the number n, the product of all primes, plus 1:

$$n = p_1 \cdot p_2 \cdot \ldots p_k + 1$$

    - Consider the smallest divisor of n, d, greater than 1 :
      - d must be prime, because if it had divisors, they would also divide n
      - But none of the primes in our finite list is a divisor of n (if you divide n by any of those primes, you will always get a remainder of 1)
      - So d is a prime not in our list
    - This is a contradiction, so there must be an infinite number of primes

***Euclid of Alexandria (325 B.C. - 265 B.C.)**

Prime Numbers

- The nth prime, P_n is about n times the natural logarithm of n:

$$P_n \approx n \ln n$$

- This allows us to estimate the density of primes within a range of integer values.
  - There are 25 primes between 0 and 100, so the density of primes is 1 in 4
  - For 10-digit numbers, the density of primes is only 1 in 23
  - For 100-digit numbers, the density is 1 in 230
  - The density of primes is inversely proportional to their length in digits

Generating Small Prime Numbers

- One simple way of calculating primes is to use the ***Sieve of Eratosthenes****:
  1) Write down all integers from 2 through x
  2) Circle 2, marking it prime, and cross out all other multiples of 2
  3) Repeatedly circle the smallest uncircled, uncrossed number and cross out all its other multiples
  4) When every number has been circled or crossed out, the circled numbers are the primes

Try a Java applet to demonstrate this algorithm.

***Eratosthenes (276 B.C. - 195 B.C.)**

Greatest Common Divisor (GCD)

- The ***greatest common divisor*** of two integers m and n is the largest integer that divides them both:

  gcd(m, n) = max{k | k|m and k|n}

  – Euclid's algorithm to calculate gcd(m,n), for given values $0 \le m \le n$ uses the recurrence:

$$\gcd(0, n) = n;$$

$$\gcd(m, n) = \gcd(n \bmod m, m), \qquad \text{for } m > 0$$

- So, for example, gcd(12, 18) = gcd(6,12) = gcd(0,6) = 6
  – Because any common divisor of m and n must also be a common divisor of both m and the number:

$$n \bmod m = n - \lfloor n / m \rfloor m$$

where $\lfloor a \rfloor$ is the *floor* function, the smallest integer less than or equal to a

Euclid's Algorithm for GCD

```
package primes;

/**
 * Class to calculate the greatest common divisor (gcd)
 * of two integers using Euclid's algorithm
 */

public class GCD
{
   public static int calculate(int m, int n)
   {
      int g;
      if (m < 0)
         m = -m;
      if (n < 0)
         n = -n;
      if ((m + n) == 0)
         throw new java.lang.IllegalArgumentException(
                              "m and n cannot add to zero");
      g = n;
      while (m > 0)
      {
         g = m;
         m = n % m;
         n = g;
      }
      return g;
   }

   public static void main(String[] args)
   {
      int m = 18;
      int n = 12;
      System.out.println("GCD of " + m + " and " +
                           n + " is " + calculate(m, n));
   }
}
```

An implementation in Java

Euclid's Algorithm for GCD

- Euclid's algorithm can be generalized for an array of integer values:

```
/**
 * Calculates the gcd of an array of numbers
 */
public static int calculate(int[] v)
{
   int g = v[0];
   for (int i = 1; i < v.length; i++)
   {
      g = calculate(g, v[i]);
      if (g == 1)
         return 1;
   }
   return g;
}
```

This function is added to the previous Java class.

Relative Primality

- Two integers *m* and *n* are ***relatively prime*** (also known as ***coprimes***) when their gcd(*m*,*n*) = 1
  - That is, they have no common factor other than 1

  For example:
  - 14 and 15 are relatively prime, despite the fact that neither one is a prime
  - 6 and 35 are relatively prime
  - 6 and 27 are not relatively prime because they are both divisible by 3.

- This is an important concept, as we shall see later...

Groups

- A ***group***, *G*, is a *set of elements with an associated binary operation*, $\bullet$. It is sometimes denoted $\{G, \bullet\}$
  - For each ordered pair (*a*, *b*) of elements in G, there is an associated element $(a \bullet b)$, such that the following axioms hold:

1) ***Closure*** : If a and $b \in G$, then $a \bullet b \in G$

2) ***Associative*** : $a \bullet (b \bullet c) = (a \bullet b) \bullet c$ for all $a, b, c \in G$

3) ***Identity element*** : There is an element $e \in G$ such that $a \bullet e = e \bullet a = a$ for all $a \in G$

4) ***Inverse element*** : For each $a \in G$ there is an element $a' \in G$ such that $a \bullet a' = a' \bullet a = e$

Groups

- A ***finite group*** is a group with a finite number of elements, otherwise, a group is an ***infinite group***.
- A group is said to be an ***abelian group*** if it satisfies the following condition:

5) ***Commutative*** : $a \bullet b = b \bullet a$ for all $a, b \in G$

- Examples of abelian groups:
  - The set of integers (negative, zero, and positive), ***Z***, under addition. The identity element of ***Z*** under addition is 0; the inverse of *a* is -*a*, for all *a* in ***Z***.
  - The set of non-zero real numbers, ***R****, under multiplication. The identity element of ***R**** under multiplication is 1; the inverse of *a* is 1/*a* for all *a* in ***R****.

Exponentiation and Cyclic Groups

- ***Exponentiation*** within a group is repeated application of the group operator, such that:

  $a^0 = e$, the identity element

  $a^n = a \bullet a \bullet \cdots \bullet a$ (i.e. $\bullet$ applied n-1 times)

  $a^{-n} = (a')^n$, where a' is the inverse of a
- A group G is ***cyclic*** if every element of G is a power g^k (k is an integer) of a fixed element $g \in G$. The element g is said to ***generate the group***, or to be ***a generator of the group***.
- A cyclic group is always abelian, and may be finite or infinite
  - Example of a cyclic group:
    - The group of positive integers, $\{\boldsymbol{N}, +\}$, ($\boldsymbol{N} = \{1, 2, 3, ...\}$) under addition is an infinite cyclic group generated by the element 1. (i.e. 1 + 1 = 2, 1 + 1 + 1 = 3, etc.)

Rings

- A ***ring***, R, denoted by $\{R, +, \times\}$, is a set of elements with two binary operations, called ***addition*** (+) ***and multiplication*** ($\times$), such that, for a, b, c in R:

  addition and ***multiplication*** are abstract operations here

  1)-5) ***R is an abelian group with respect to addition***; for this case of an additive group, we denote the identity element as 0, and the inverse of a as $-a$.

  6) ***Closure under multiplication:***
  If a and b belong to R, then $a \times b$ is also in R

  7) ***Associativity of multiplication:***
  $a \times (b \times c) = (a \times b) \times c$ for all a, b, c, in R

  8) ***Distributive Laws:***
  $a \times (b + c) = a \times b + a \times c$ for all a, b, c, in R
  $(a + b) \times c = a \times c + b \times c$ for all a, b, c, in R

Note that we often write $a \times b$ as simply ab

Commutative Rings

- A ring is ***commutative*** if it satisfies the following additional condition:

  9) ***Commutativity of multiplication:***
  $a \times b = b \times a$ for all a, b, c, in R

Example of a commutative ring:

The set of even integers, {..., -4, -2, 0, 2, 4, ...}) under the normally defined integer operations of addition and multiplication.

Integral Domains

- An ***integral domain*** is a commutative ring that obeys the following:

  10) ***Multiplicative identity:***
  There is an element 1 in R such that $a \times 1 = 1 \times a = a$ for all a in R

  11) ***No zero divisors:***
  If a, b in R and $a \times b = 0$, then either $a = 0$ or $b = 0$

Example of an integral domain:

The set of all integers ($\boldsymbol{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$) under the normally defined integer operations of addition and multiplication, $\{\boldsymbol{Z}, +, \times\}$

Fields

- A ***field***, F, denoted by $\{F, +, \times\}$, is a set of elements with two binary operations, called *addition* and *multiplication*, such that, for all a, b, c in F, the following apply:

Again, ***addition*** and ***multiplication*** are abstract operations

1)-11) ***F is an integral domain***

11) ***Multiplicative inverse:***

For each a in F, except 0, there is an element a^{-1} in F such that:

$$a \times a^{-1} = a^{-1} \times a = 1$$

Fields

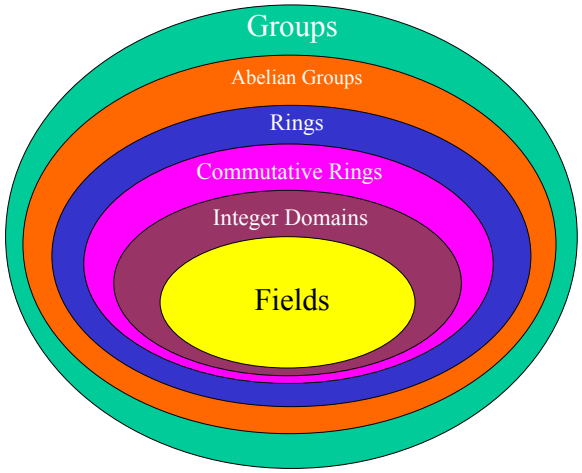
- A field is a set in which we can do addition, subtraction, multiplication, and division without leaving the set.
- Division is defined:

$$a/b = a(b^{-1})$$

Examples:

- The set of rational numbers, ***Q***; the set of real numbers, ***R***, the set of complex numbers, ***C***.
- The set of all integers, ***Z***, is *not* a field, because only the elements 1 and -1 have multiplicative inverses in the integers.

Groups, Rings, and Fields



Summary

- Whew!
- I realize it's a quite a bit of new stuff, and much of it is fairly abstract.
- However, I think we need some mathematical background to understand modern cryptographic algorithms.
- There's more: Modular Arithmetic, which is a very important topic for modern cryptography.