RSA: Decryption

If you get an encrypted message $C = M^e \bmod n$, how do you decrypt

- Compute $C^d \equiv M^{ed} \pmod{n}$.
  - Can do this quickly using fast exponentiation again

Claim: $M^{ed} \equiv M \pmod{n}$

Proof: Since $ed \equiv 1 \pmod{(p-1)(q-1)}$

- $ed \equiv 1 \pmod{p-1}$ and $ed \equiv 1 \pmod{q-1}$

Since $ed = k(p-1)+1$ for some k,

$$M^{ed} = (M^{p-1})^k M \equiv M \pmod{p}$$

(Fermat's Little Theorem)

- True even if $p \mid M$

Similarly, $M^{ed} \equiv M \pmod{q}$

Since p, q, relatively prime, $M^{ed} \equiv M \pmod{n}$ (Theorem 10).

Note: Decryption would be easy for someone who can factor n.

- RSA depends on factoring being hard!

Digital Signatures

How can I send you a message in such a way that you're convinced it came from me (and can convince others).

- Want an analogue of a "certified" signature

Cool observation:

- To send a message M, send $M^d \pmod{n}$
  - where (n, e) is my public key
- Recipient (and anyone else) can compute $(M^d)^e \equiv M \pmod{n}$, since M is public
- No one else could have sent this message, since no one else knows d.

Probabilistic Primality Testing

RSA requires really large primes.

- This requires testing numbers for primality.
  - Although there are now polynomial tests, the standard approach now uses probabilistic primality tests

Main idea in probabilistic primality testing algorithm:

- Choose b between 1 and n at random
- Apply an easily computable (deterministic) test $T(b, n)$ such that
  - $T(b, n)$ is true (for all b) if n is prime.
  - If n is composite, there are lots of b's for which $T(b, n)$ is false

Example: Compute $\gcd(b, n)$.

- If n is prime, $\gcd(b, n) = 1$
- If n is composite, $\gcd(b, n) \neq 1$ for some b's
  - Problem: there may not be that many witnesses

Example: Compute $b^{n-1} \bmod n$

- If n is prime $b^{n-1} \equiv 1 \pmod{n}$ (Fermat)
- Unfortunately, there are some composite numbers n such that $b^{n-1} \equiv 1 \pmod{n}$
  - These are called *Carmichael numbers*

There are tests $T(b, n)$ with the property that

- $T(b, n) = 1$ for all b if n is prime
- $T(b, n) = 0$ for at least $1/3$ of the b's if n is composite
- $T(b, n)$ is computable quickly (in polynomial time)

Constructing T requires a little more number theory

- Beyond the scope of this course.

Given such a test T, it's easy to construct a probabilistic primality test:

- Choose 100 (or 200) b's at random
- Test $T(b, n)$ for each one
- If $T(b, n) = 0$ for any b, declare b composite
  - This is definitely correct
- If $T(b, n) = 1$ for all b's you chose, declare n prime
  - This is highly likely to be correct

Prelim Coverage

- Chapter 0:
  - Sets
    - Operations: union, intersection, complementation, set difference
    - Proving equality of sets
  - Relations:
    - reflexive, symmetric, transitive, equivalence relations
    - transitive closure
  - Functions
    - Injective, surjective, bijective
    - Inverse function
  - Important functions and how to manipulate them:
    - exponent, logarithms, ceiling, floor, mod
  - Summation and product notation
  - Matrices (especially how to multiply them)
  - Proof and logic concepts
    - logical notions ($\Rightarrow$, $\equiv$, $\neg$)
    - Proofs by contradiction

- Chapter 1
  - You don't have to write algorithms in their notation
  - You may have to *read* algorithms in their notation
- Chapter 2
  - induction vs. strong induction
  - guessing the right inductive hypothesis
  - inductive (recursive) definitions
- Number Theory - everything covered in class:
  - Fundamental Theorem of Arithmetic
  - gcd, lcm
  - Euclid's Algorithm and its extended version
  - Modular arithmetic, linear congruences
  - modular inverse and CRT
  - Fermat's little theorem
  - RSA

  You need to know all the theorems and corollaries discussed in class.
- Chapter 4:
  - Section 4.1, 4.2
  - Sum and product rule

Combinatorics

Problem: How to count without counting.

- How do you figure out how many things there are with a certain property without actually enumerating all of them.

Sometimes this requires a lot of cleverness and deep mathematical insights.

But there are some standard techniques.

- That's what we'll be studying.

Sum and Product Rules

Example 1: In New Hampshire, license plates consisted of two letters followed by 3 digits. How many possible license plates are there?

Answer: 26 choices for the first letter, 26 for the second, 10 choices for the first number, the second number, and the third number:

$$26^2 \times 10^3 = 676,000$$

Example 2: A traveling salesman wants to do a tour of all 50 state capitals. How many ways can he do this?

Answer: 50 choices for the first place to visit, 49 for the second, . . . : 50! altogether.

Chapter 4 gives general techniques for solving counting problems like this. Two of the most important are:

The Sum Rule: If there are $n(A)$ ways to do A and, distinct from them, $n(B)$ ways to do B, then the number of ways to do A *or* B is $n(A) + n(B)$.

- This rule generalizes: there are $n(A) + n(B) + n(C)$ ways to do A *or* B *or* C
- In Section 4.8, we'll see what happens if the ways of doing A and B aren't distinct.

The Product Rule: If there are $n(A)$ ways to do A and $n(B)$ ways to do B, then the number of ways to do A *and* B is $n(A) \times n(B)$. This is true if the number of ways of doing A and B are independent; the number of choices for doing B is the same regardless of which choice you made for A.

- Again, this generalizes. There are $n(A) \times n(B) \times n(C)$ ways to do A *and* B *and* C

Some Subtler Examples

Example 3: If there are n Senators on a committee, in how many ways can a subcommittee be formed?

Two approaches:

1. Let N_1 be the number of subcommittees with 1 senator (n), N_2 the number of subcommittees with 2 senator ($n(n-1)/2$), ...

   According to the sum rule:

   $$N = N_1 + N_2 + \cdots + N_n$$

   - It turns out that $N_k = \frac{n!}{k!(n-k)!}$ (n choose k); this is discussed in Section 4.4
   - A subtlety: What about N_0? Do we allow subcommittees of size 0? How about size n?
     - The problem is somewhat ambiguous.

     If we allow subcommittees of size 0 and n, then there are 2^n subcommittees altogether.
     - This is the same as the number of subsets of the set of n Senators: there is a 1-1 correspondence between subsets and subcommittees.

2. Simpler method: Use the product rule!

- Each senator is either in the subcommittee or out of it: 2 possibilities for each senator:
  - $2 \times 2 \times \cdots \times 2 = 2^n$ choices altogether

General moral: In many combinatorial problems, there's more than one way to analyze the problem.

How many ways can the full committee be split into two sides on an issue?

This question is also ambiguous.

- If we care about which way each Senator voted, then the answer is again 2^n: Each subcommittee defines a split + vote (those in the subcommittee vote Yes, those out vote No); and each split + vote defines defines a subcommittee.
- If we don't care about which way each Senator voted, the answer is $2^n/2 = 2^{n-1}$.
  - This is an instance of the Division Rule.

Coping with Ambiguity

If you think a problem is ambiguous:

1. Explain why
2. Choose one way of resolving the ambiguity
3. Solve the problem according to your interpretation
    - Make sure that your interpretation doesn't render the problem totally trivial

More Examples

Example 4: How many legal configurations are there in Towers of Hanoi with n rings?

Answer: The product rule again: Each ring gets to "vote" for which pole it's on.

- Once you've decided which rings are on each pole, their order is determined.
- The total number of configurations is 3^n

Example 5: How many distinguishable ways can the letters of "computer" be arranged? How about "discrete"?

For computer, it's 8!:

- 8 choices for the first letter, for the second, ...

Is it 8! for discrete? Not quite.

- There are two e's

Suppose we called them e_1, e_2:

- There are two "versions" of each arrangement, depending on which e comes first: discre$_1$te$_2$ is the same as discre$_2$te$_1$.
- Thus, the right answer is 8!/2!

Division Rule: If there is a k-to-1 correspondence between of objects of type A with objects of type B, and there are $n(A)$ objects of type A, then there are $n(A)/k$ objects of type B.

A *k-to-1 correspondence* is an onto mapping in which every B object is the image of exactly k A objects.

Permutations

A *permutation* of n things taken r at a time, written $P(n, r)$, is an arrangement in a row of r things, taken from a set of n distinct things. Order matters.

Example 6: How many permutations are there of 5 things taken 3 at a time?

Answer: 5 choices for the first thing, 4 for the second, 3 for the third: $5 \times 4 \times 3 = 60$.

- If the 5 things are a, b, c, d, e, some possible permutations are:

$$abc \;\; abd \;\; abe \;\; acb \;\; acd \;\; ace$$
$$adb \;\; adc \;\; ade \;\; aeb \;\; aec \;\; aed$$
$$\ldots$$

In general

$$P(n, r) = \frac{n!}{(n-r)!} = n(n-1)\cdots(n-r+1)$$

Combinations

A *combination* of n things taken r at a time, written $C(n, r)$ or $\binom{n}{r}$ ("n choose r") is any subset of r things from n things. Order makes no difference.

Example 7: How many ways are there of choosing 3 things from 5?

Answer: If order mattered, then it would be $5 \times 4 \times 3$. Since order doesn't matter,

$$abc, acb, bac, bca, cab, cba$$

are all the same.

- For way of choosing three elements, there are $3! = 6$ ways of ordering them.

Therefore, the right answer is $(5 \times 4 \times 3)/3! = 10$:

$$\begin{array}{ccccc} abc & abd & abe & acd & ace \\ ade & bcd & bce & bde & cde \end{array}$$

In general

$$C(n, r) = \frac{n!}{(n-r)!r!} = n(n-1)\cdots(n-r+1)/r!$$

More Examples

Example 8: How many full houses are there in poker?

- A full house has 5 cards, 3 of one kind and 2 of another.
- E.g.: 3 5's and 2 K's.

Answer: You need to find a systematic way of counting:

- Choose the denomination for which you have three of a kind: 13 choices.
- Choose the three: $C(4,3) = 4$ choices
- Choose the denomination for which you have two of a kind: 12 choices
- Choose the two: $C(4,2) = 6$ choices.

Altogether, there are:

$$13 \times 4 \times 12 \times 6 = 3744 \text{ choices}$$

0!

It's useful to define $0! = 1$.

Why?

1. Then we can inductively define

$$(n+1)! = (n+1)n!,$$

   and this definition works even taking 0 as the base case instead of 1.

2. A better reason: Things work out right for $P(n,0)$ and $C(n,0)!$

How many permutations of n things from n are there?

$$P(n,n) = \frac{n!}{(n-n)!} = \frac{n!}{0!} = n!$$

How many ways are there of choosing n out of n?
0 out of n?

$$\binom{n}{n} = \frac{n!}{n!0!} = 1$$

$$\binom{n}{0} = \frac{n!}{0!n!} = 1$$

More Questions

Q: How many ways are there of choosing k things from $\{1, \ldots, n\}$ if 1 and 2 can't both be chosen? (Suppose $n, k \geq 2$.)

A: First find all the ways of choosing k things from n—$C(n, k)$. Then subtract the number of those ways in which both 1 and 2 are chosen:

- This amounts to choosing $k-2$ things from $\{3, \ldots, n\}$: $C(n-2, k-2)$.

Thus, the answer is

$$C(n, k) - C(n-2, k-2)$$

Q: What if order matters?

A: Have to compute how many ways there are of picking k things, two of which are 1 and 2.

$$P(n, k) - k(k-1)P(n-2, k-2)$$

Q: How many ways are there to distribute four distinct balls evenly between two distinct boxes (two balls go in each box)?

A: All you need to decide is which balls go in the first box.

$$C(4, 2) = 6$$

Q: What if the boxes are indistinguishable?

A: $C(4, 2)/2 = 3$.

Combinatorial Identities

There all lots of identities that you can form using $C(n, k)$. They seem mysterious at first, but there's usually a good reason for them.

Theorem 1: If $0 \leq k \leq n$, then

$$C(n, k) = C(n, n - k).$$

Proof:

$$C(n, k) = \frac{n!}{k!(n-k)!} = \frac{n!}{(n-k)!(n-(n-k))!} = C(n, n-k)$$

Q: Why should choosing k things out of n be the same as choosing $n - k$ things out of n?

A: There's a 1-1 correspondence. For every way of choosing k things out of n, look at the things not chosen: that's a way of choosing $n - k$ things out of n.

This is a better way of thinking about Theorem 1 than the combinatorial proof.

Theorem 2: If $0 < k < n$ then

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

Proof 1: (Combinatorial) Suppose we want to choose k objects out of $\{1, \ldots, n\}$. Either we choose the last one (n) or we don't.

1. How many ways are there of choosing k without choosing the last one? $C(n-1, k)$.
2. How many ways are there of choosing k including n? This means choosing $k-1$ out of $\{1, \ldots, n-1\}$: $C(n-1, k-1)$.

Proof 2: Algebraic ...

Note: If we define $C(n, k) = 0$ for $k > n$ and $k < 0$, Theorems 1 and 2 still hold.

Pascal's Triangle

Starting with $n = 0$, the nth row has $n + 1$ elements:

$$C(n, 0), \ldots, C(n, n)$$

Note how Pascal's Triangle illustrates Theorems 1 and 2.

Theorem 3: For all $n \geq 0$:

$$\Sigma_{k=0}^{n} \binom{n}{k} = 2^n$$

Proof 1: $\binom{n}{k}$ tells you all the way of choosing a subset of size k from a set of size n. This means that the LHS is *all* the ways of choosing a subset from a set of size n. The product rule says that this is 2^n.

Proof 2: By induction. Let $P(n)$ be the statement of the theorem.

Basis: $\Sigma_{k=0}^{0} \binom{0}{k} = \binom{0}{0} = 1 = 2^0$. Thus $P(0)$ is true.

Inductive step: How do we express $\Sigma_{k=0}^{n} C(n,k)$ in terms of $n-1$, so that we can apply the inductive hypothesis?

- Use Theorem 2!