CSE 113 B

November 29 – December 3, 2010

"Public-Key Encryption"

Adrienne wants to send a message to Michael.

→ Adrienne create 2 keys
- public key
- private key

→ Michael does the same

→ Write out the message

↳ Breaks message into chunks of n characters

↳ Converts the chunks to numbers (binary)

→ Adrienne uses Michael's public key to encrypt the "chunks" & sends it off

→ Michael receives message & uses his private key to decrypt

RSA Encryption

→ Pick 2 numbers p & q

p & q must be prime

p & q must have at least 150 digits

→Compute

$n = p \cdot q$

$k = (p-1) * (q-1)$

Find a number e which is a number between 1 & k and is relatively prime to k and is also prime itself.

Then, solve for d & r

$d * e - v * k = 1$

- Keep d, e & n

d, e & n: private key

n: public key

Encrypt

$$(\text{Message as number})^{e} \bmod n$$

Decrypt

$$(\text{Encrypted Message})^{d} \bmod n$$

300 digits

128

1 x y 128

42 a 32

12b c 25

n

1 . n

.

.

Can factor a 232 digit number

2 years

Today's Lecture

- There are problems we can solve
- There are problems we know we can solve, but they are expensive to solve
- There are problems we know we can not solve

Problems we can solve

- You've solved a few yourself.
- There are obviously many more.
- What kinds of problems have computers solved?

Problems we know we can solve

- These problems have solutions that run in reasonable time
  - When we discuss this formally, we express the time it takes to find a solution to be a function where the variable is the size of the inputs. The function is expressed in terms of the size of the inputs.
  - For example, a reasonable solution may be expressed in terms n^3, so if n = 100, then when we cube it, we get 100,000

Unreasonable time

- When we come across a problem that runs in unreasonable time, we see that for 100 inputs, the resulting function returns a value of 1.27×10^{30}
- Which is the number 1,270,000,000,000,000,000,000,000,000,000
- If the computer uses 1 second to process an input, that would be 21,167,000,000,000,000,000,000,000,000 minutes, or 352,778,000,000,000,000,000,000,000 hours, or 1,469,910,000,000,000,000,000,000 days or 40,271,400,000,000,000,000,000 years

A SIDE NOTE

- 1.27×10^{30} is just shy of the estimate of the total number of atoms in the observable universe, which is guessed to be about 4×10^{81}
- These are the values if the function is 2^n where n is the number of inputs.
- If we use another function n!, the result when n = 100 is 9.3×10^{157} (larger than the estimate of the total number of atoms in the observable universe).

Unreasonable Time

- Just because something runs in unreasonable time doesn't mean we don't keep trying to solve it in reasonable time.
- Sometimes, we can improve the way we think about things and get to solutions that are reasonable.

A "Hard" Problem

- Example: Computer player for chess. The estimate for the total number of board configurations for chess is somewhere in between the values we mentioned on the previous slide (10^{50}).
- Therefore, for the computer player to know how to win, it needs to know each of those board configurations and how to win if the board is in that configuration.
- Well, sort of – there are shortcuts to this, which is how we got a computer that is able to play chess.

Unreasonable Problems

- Putting together an n-piece jigsaw puzzle
- “Tetris” – not quite Tetris, but a similar class of problems using Tetris – like pieces
- Traveling Salesman
- Scheduling problems (N teachers, M hours, P classes) – schedule so that all P classes are covered so that no teacher is teaching at the same time two different classes, nor that the same class is being taught at the same time by two different instructors

Unreasonable Problems

- We know that there are unreasonably-timed solutions to these problems in the general case, but for some if the variables (M, N, etc) are small, we can come up with reasonably-timed solutions.
- Also, for these problems, you can check to see if a proposed solution is in fact valid in reasonable time
- These problems belong to a specific class of problems with these characteristics.

Some unanswered questions

- A currently un-answered (and potentially never-answered) question is whether or not there are reasonably-timed solutions to our currently known unreasonably-timed solution problems. We know that sometimes we can find reasonable solutions, but can we find general-case reasonably-timed solutions?

Two more problems

- If given a description of a problem to solve and a solution to the problem designed by a student – can we write a program to verify that the program solves the problem?
- Can we write a program to verify that there are no infinite loops in a program?

Answers…

- In fact, the answer is no to both of these questions.
- Furthermore, it's not just a "I don't think so", it's a provable fact that we will never be able to solve these problems.
- These problems exist in a class of problems known as "undecideable" problems – we know that we can never solve these problems using a computer.