CSE 111

Fall 2010

October 18 – 22

Announcements

- Lab 3 due this week (week of October 18th)
- Labs this week – exam review
- In-lecture activity – Wednesday Oct 20th
- Exam 2 – Friday, October 22nd in lecture
- Lab 4 begins week of October 25th

Security in Operating Systems

- Administrators
- Login for users
- Auditing software
  - software that is always running & looking for strange behavior

Security in Operating Systems

- Priviledge mode
  - run priviledged instructions
  - small amount of time
- Non-priviledge mode
  - what the computer runs most of the time

Security on a Network

Fedreal

— Malware is biggest threat

- Virus
- Worm - self-propogating
- Trojan horse
- Spyware
- Phishing
- Denial of Service Attack

How can Computers (and Users) Protect themselves?

Firewalls – Gateway to a network or computer

Proxy server – Intermediary between client & server

Anti-virus software

Practice Problems For Exam 2

- Questions at the end of Chapter 2 (pages 113-117)
  - 4
  - 5
  - 7
  - 9
  - 11
  - 12
  - 13
  - 14
  - 15
  - 16
  - 17
  - 18
  - 20
  - 21
  - 22
  - 23
  - 26
  - 27

Practice Problems For Exam 2

- Questions at the end of Chapter 3 (pgs 146-149)
  - 1
  - 3
  - 5
  - 7
  - 8
  - 10
  - 11
  - 18
  - 19
  - 29
  - 31
  - 32
  - 45
  - 49
  - 50

Practice Problems For Exam 2

- Questions at the end of Chapter 4 (pgs 197-199)
  - 1
  - 2
  - 3
  - 4
  - 5
  - 11
  - 17
  - 18
  - 19
  - 20
  - 21
  - 24
  - 25
  - 34
  - 35
  - 37

In-Lecture Activity #4

Encryption

Volunteers (Need 6)

- Volunteers 1-5: Pick a number with 1 or 2 digits and write it on the piece of paper. (Will also need to do some addition in a moment.)

- Volunteer 6: Pick a 3-digit number and write it on the piece of paper.

Volunteers 1-5

- When you receive the pad of paper, add the number you picked to the number on the pad.
- Write the answer on the next page in the pad.
- Rip off the top page (it's yours to keep as a souvenir).

Compute the Average

- Pad of paper comes back to Adrienne

292 comes back

Did we Compute the correct Average?

- Figure it out

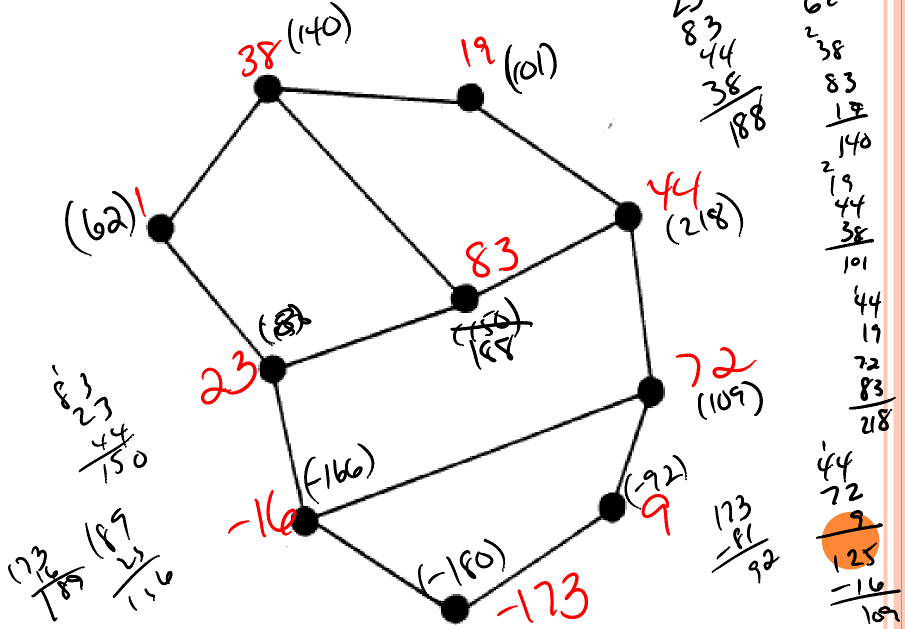
Sending "Secret" Information

- Tell someone the "secret number"
- To send "secret message", take the message and add the "secret number" to it
- To decode, subtract the "secret number" from the message you receive

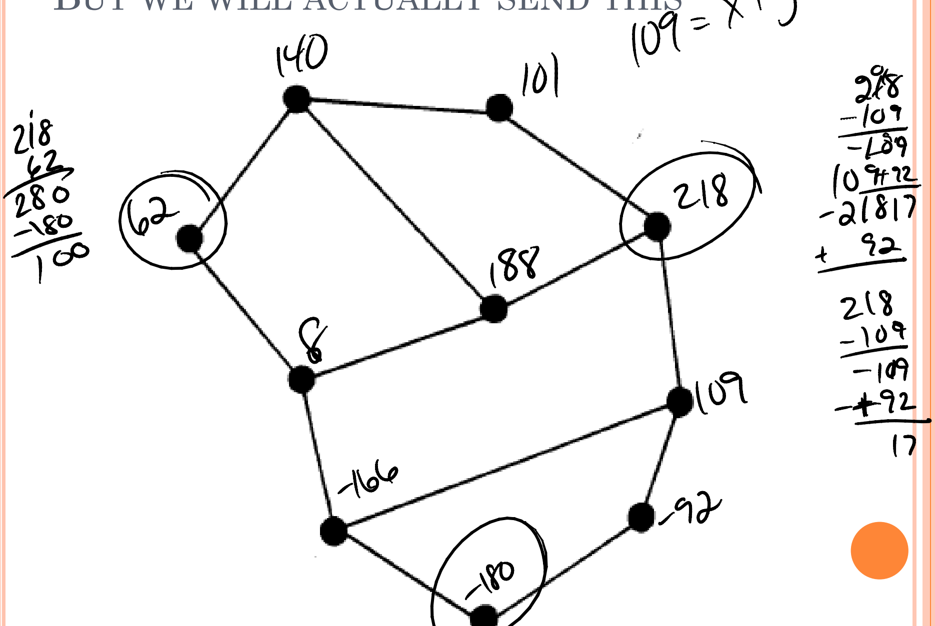
Another "public secret" Example

- Volunteer 1:
  - Pick a number > 50 and < 1000
- Now pick 10 other numbers that will add up to our secret number

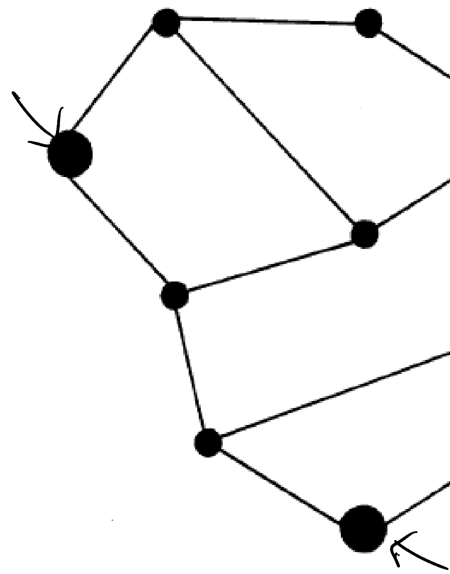
Put the numbers on this Graph



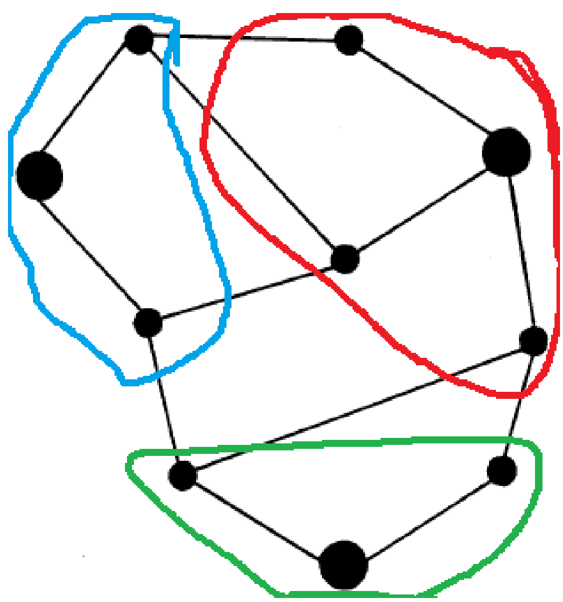
But we will actually send this



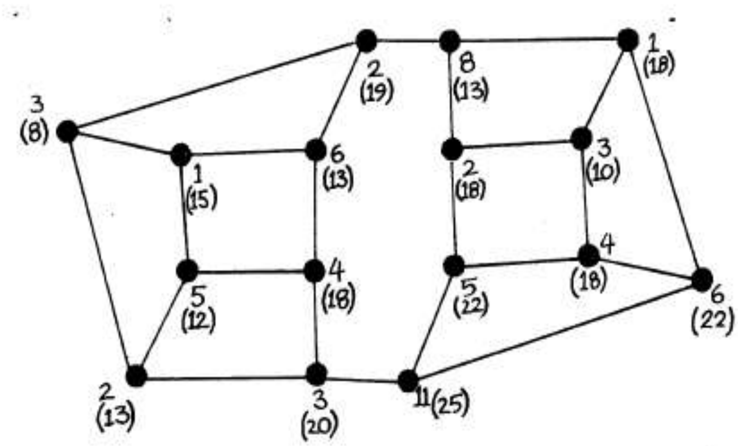
Our receiver will decode using…



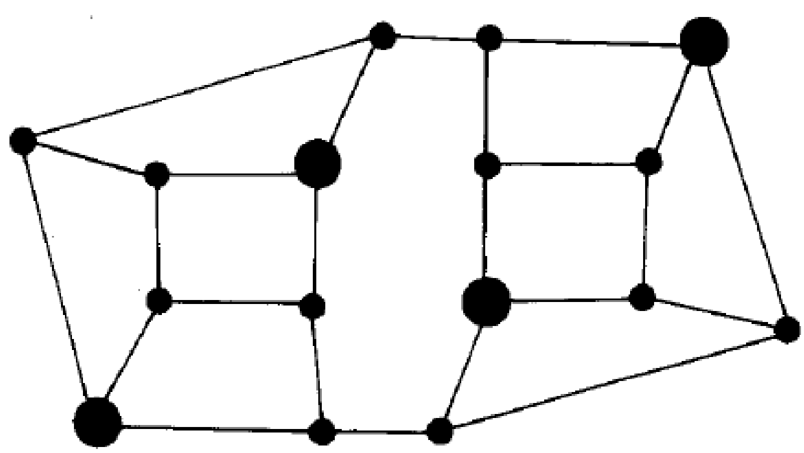
Why Do we only need Three?



More Complex Example



Private Graph



So What is the message we are sending?

Problem

- No matter how complex the graph, we still could break it.
- So, the key to public key cryptosystems is to create keys that are hard to "crack"

Public Key Encryption (RSA)

- My children want to send a message to me
- Step1: They write out the message
- Step 2: Break message into chunks of 4 characters
- Step 3: Convert the chunks to numbers
- Step 4: Use Mom's public key to encrypt message
- Step 5: Send message to Mom

Encryption

- Mom gets message and uses private key to decrypt message and read it.
- To respond, Mom does same steps, but uses the kid's public key to encrypt. The kids use their private key to decrypt.
- Neither party knows the other's private key, only their public keys.

More Details – The Math

- Choose two prime numbers p & q
  - p & q have at least 150 digits each
- Compute n = pq
- Compute k = (p-1) * (q-1)
- Find e: e is a prime number between 1 & k and is relatively prime to k.
  - Relatively prime means that the greatest common divisor between e & k is 1

More Details – The Math

- Then, we solve the following equation for d & v
  - (d*e) – (v*k) = 1
- We keep d, e, and n
  - Public key: e & n
  - Private key: d & n

Converting Message

- To encrypt message:
  - $(\text{Message as number})^e \bmod n$
- Send result

- When receiver gets message, decrypt using:
  - $(\text{Received message})^d \bmod n$

How is it Secure?

- Leaving some of the math details out, in order to get the private key (d), we would need to be able to factor n into p & q.

- n is a 300-digit number

Can we Do it?

- Latest data I could find:
  - We can factor a 232-digit number into its prime factors
  - But
    - It took 2 years
    - And hundreds of machines