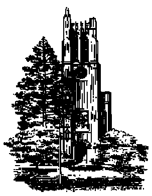
Thursday June 16, 2016
Lecture 19

Number Theory



574

Notables

- Homework #11
  - Page 329, Problem 4
  - Page 330, Problem 16
  - Page 330, Problem 18
  - Page 357, Problem 2
  - Page 358, Problem 8
  - Due Tuesday June 21
- Read Chapters 5 and 8

575

Public Key for Confidentiality

- Scenario: *A* wants to send a confidential message to *B*
  - *A* encrypts the message using *B*'s Public Key
  - *B* decrypts message using *B*'s Private Key
- Note that
  - *B* does not need to know *A*'s Public Key
  - *A* does not need to have it's own Keys
  - Only *B* can read the message
  - Message
    - Is confidential
    - May not be authentic (i.e., Not really from *A*)

576

Public Key For Authenticity

- Scenario: *A* wants to send an authentic message to *B*
  - *A* encrypts the message using its own Private Key and sends it to *B*.
  - *B* decrypts the message with *A*'s Public Key
- Note that
  - *B* needs to know *A*'s Public Key
  - *B* does not need to have it's own Keys
  - Anyone can read the message
  - Message
    - Is not confidential
    - Is authentic (i.e., Really from *A*)

577

Public Key For both Confidentiality and Authenticity

- Scenario: *A* wants to send an authentic and confidential message to *B*
  - *A* encrypts the message using its own Private Key and then encrypts the result using *B*'s public key, and sends it to *B*.
  - *B* decrypts the message with *B*'s private Key, and then decrypts it further using A's public key.
- Note that
  - *B* needs to know *A*'s Public Key
  - *A* needs to know *B*'s Public Key
  - Message
    - Is confidential
    - Is authentic (i.e., Really from *A*)

578

RSA (special case)

- Relies on laboriousness of finding prime factorization.
- The Public Key is just a number *k* which is the product of two private prime numbers
- The Private Key is a number which is computed using factors of *k*
- Heavy math is involved here. What is presented here is a special case of RSA code.
  - Think of the message as a "number"

579

RSA Public key system

- The *Public Key* is public to everyone!
- Sender encrypts using the Public Key
- Only receiver knows how to decrypt

580

RSA (special case)

1. Select two different prime numbers p and q such that
   $p \bmod 3 = 2$ and $q \bmod 3 = 2$
2. Compute $s = \dfrac{2(p-1)(q-1)+1}{3}$
3. The Public Key is k, where $k = pq$
4. The Private Key is s.
5. Note that RSA can be broken if we know p and q.

581

RSA-640

- P = 1634733645809253848443133883865090859841783670033092312181110852389333100104508151212118167511579
- Q = 1900871281664822113126851573935413975471896789968515493666638539088027103802104498957191261465571

582

RSA Example

- $p = 5$
- $q = 11$
  - The corresponding public key is $k = 55$,
  - The corresponding private key $s = 27$

583

RSA Example (confidentiality)

- My public key is $k = 55$
- If you to send me a secret message, say 4, encrypt it using my public key as follows:

  C = (4**3) % 55 = 9

  and then you send message 9 to me
- I will find your secret message by decrypting your message using my private key as follows:

  T = (9**27) % 55 = 4

- Note how big of a number this is:
  - 9**27 = 58149737003040059690390169

584

RSA Example (authenticity)

- My public key is $k = 55$
- If I want to send you a message, say 4, that you can be certain it came from me, I encrypt it using my private key as follows:

  C = (4**27) % 55 = 49

  and then send you message 49
- To make sure message 49 came from me, you (or any body) can decrypt the message using my public key as follows:

  T = (49**3) % 55 = 4

585

RSA (recap)

Confidentiality	Authenticity
(message**3)%public key	(message**private key)%public key
(received message**private key)%public key	(received message**3)%public key

586

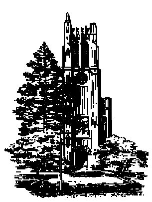
Sample Public Key

- 6nfX01TUfFaliu1wit5RJ5JQNFBzxWSePsviIml PKReIFSjpktWW6RbGk4pNj+fqh2DOWquaMz dXI27YFVuFJQ==
- This is a number in base 64, using the following symbols
  - 0-25 is 'A'-'Z'
  - 26-51 is 'a'-'z'
  - 52-61 is '0'-'9'
  - 62 is '+'
  - 63 is '/'
  - Pad is '='

587

Induction and Recursion

Chapter 5



588

Example

- Consider the predicate
  $P(n)$ = ``$1 + 3 + \cdots + (2n-1)$ is equal n^2''
- Let's verify the truth value of $P(n)$ for some n:
  - $P(1) = 1 = 1 = 1^2$
  - $P(2) = 1 + 3 = 4 = 2^2$
  - $P(3) = 1 + 3 + 5 = 9 = 3^2$
  - ....
  - $P(9) = 1 + 3 + 5 + 7 + 9 + 11 + 13 + 15 + 17 = 9^2$
  - …
- How can we show that $\forall n P(n)$ is true?

589

Example… (no calculators!)

- Suppose, *without verifying*, that
  $P(21) = 1 + 3 + 5 + \ldots + 39 + 41 = 21^2$
- Given above, can we prove that
  $P(22) = 1 + 3 + 5 + \ldots + 39 + 41 + 43 = 22^2$?
  - $P(22) = 1 + 3 + 5 + \ldots + 39 + 41 + 43 = 22^2$?
  - $P(22) = P(21) + 43 = 22^2$?
  - $P(22) = 21^2 + 43 = 22^2$?
  - $P(22) = (22 - 1)^2 + (22\times2 - 1) = 22^2$?
  - $P(22) = 22^2 - 22\times2 + 1 + 22\times2 - 1 = 22^2$ ✔

590

Example (no calculators!)

- How general is our method?
- Let's replace 21 with a place holder k.
- Suppose, *without verifying*, that
  $P(k) = 1 + 3 + 5 + \ldots + (2k-1) = k^2$
- Given this, can we prove that
  $P(k+1) = 1 + 3 + 5 + \ldots + (2(k+1)-1) = (k+1)^2$?
  - $P(k+1) = 1 + 3 + 5 + \ldots + (2k-1) + (2(k+1)-1) = (k+1)^2$?
  - $P(k+1) = P(k) + (2(k+1)-1) = (k+1)^2$?
  - $P(k+1) = k^2 + (2(k+1)-1) = (k+1)^2$?
  - $P(k+1) = ((k+1) - 1)^2 + (2(k+1)-1) = (k+1)^2$?
  - $P(k+1) = (k+1)^2 - 2(k+1) + 1 + 2(k+1) - 1 = (k+1)^2$ ✔

591

Example…

- What have we accomplished so far?
  - We have shown that $P(k) \Rightarrow P(k+1)$, for any k. For instance:
    - $P(1) \Rightarrow P(2)$,
    - $P(2) \Rightarrow P(3)$,
    - …
    - $P(6) \Rightarrow P(7)$,
    - …
    - $P(19) \Rightarrow P(20)$,
    - …
    - $P(2000) \Rightarrow P(2001)$, ….
  - Note that, we do NOT know if, for example, $P(6)$ or $P(19)$ … is true. All we know is that IF, for example, $P(6)$ is true, then $P(7)$ is also true.
- What do we need to show that $P(n)$ is true for all n?
  - All we need is to PROVE that $P(1)$ is indeed true.

592

Mathematical Induction

- Let $P(n)$ be some propositional function involving integer n.
  - $P(n)$ = "$n\,(n+3)$ is an even number"
  - $P(n)$ = "$1 + 3 + \cdots + (2n-1) = n^2$"
  - …..
- To prove that $P(n)$ is true for all positive integers n, we can do the following:
  - Give a proof (usually a straight verification) that $P(1)$ is true.
  - Give a proof that for an arbitrary k, IF $P(k)$ is true THEN $P(k + 1)$ is true. That is, we validate the logical implication: $P(k) \Rightarrow P(k+1)$

593