due-02-05.sagews

January 29, 2014

Contents

1 Homework 3 Due Feb 5, 2014

1.1 Instructions

- Put your solutions in the empty space below the problem.
- Create a new cell by clicking on the horizontal cell dividers.
- If you put
  - If you then press shift-enter youll see the rendered math.
  - If you double click on the output then you can edit the input again.
  -
  -
  -
- Put this worksheet in a folder called homework in your project.
- When youre done, open the worksheet, and copy/paste the URL into an email to wstein@gmail.com with the subject math 480: homework 02-05.

1.2 Problems

1.2.1 Problem 1: Multiplicative Functions

Recall that a multiplicative function is a function f on the positive integers such that if $\gcd(a, b) = 1$, then $f(ab) = f(a)f(b)$. Give four different examples of multiplicative functions.

[Hint: you can either try to make something up yourself or search around online and in books. This isnt a problem that involves searching for 3 such functions that Ive mentioned in class or the book.]

1.2.2 Problem 2: Diffie-Hellman

Suppose Whitfield and Martin would like to agree on a secret shared number using their key exchange. They agree on working modulo the number $p = 2^{1279} - 1$ and they use element $g = 2$. Whitfield chooses the secret random number $n = 923840$ and Martin chooses the secret random number $m = 13423498590$.

1. Compute $3^{p-1} \pmod{p}$. Does this increase your confidence that p is really prime? If not, try the is_pseudoprime function in Sage.
2. Compute $t = 2^n \pmod{p}$ and $t' = 2^m \pmod{p}$.
3. Compute the secret number that Whitfiled and Martin share.

1.2.3 Problem 3: RSA

Suppose Ron, Adi, and Leonard would like to send each other secret emails about super secret stuff.
Rons public key is $(e, n) = (94958501, 26540744087555672615854231057578952347 1)$.
Adis public key is $(e, n) = (74853241, 764419222724527166689559258873002163 27)$.
Leonards public key is $(e, n) = (327581, 22650405915855398304337099662941588736 1)$.

1. Determine Ron, Adi and Leonards private keys. (How long does this take? Obviously, the n is not big enough for serious work!)
2. Adi would like to encrypt a message encoded as the number 12345 to Ron. What number does he send?
3. Adi would like to encrypt a message encoded as the number 12345 to Leonard. What number does he send?
4. Adi receives a message encrypted as the number 111373459313176521528430053533407367 65. What is the number that was encrypted?
5. Adi creates a message encoded as the number 13333337. He wants to digitally sign this message, to prove it is from him. What is the signature? (Hint, encrypt 13333337 using Adis private key instead of his public key.)
6. Adi sees a document that purports to be from Ron. The document is 20141337 with digital signature 8354621376417766953137494319451119080 8. Is the digital signature correct? (Hint: encrypt the signature using Rons public key.)

1.2.4 Problem 4: Computational Complexity: 10^{100} operations

1. Search around online for an estimate for the number of operations (lets say floating point operations or FLOPS) that the worlds faster supercomputer can do in 1 second. Call this integer B. (If youre curious, you might also search for estimates of the number of FLOPS being wasted on bitcoin mining or searching for large prime numbers right now)
2. Assuming you have a dedicated computer that can do B operations per second, how many years will it take to do 10^{100} operations. (Obviously, completely ignore things like your computer breaking, getting better, etc.!)
3. Assume that our universe has a lifespan of 34 billion years old. How many lifespan of the universes would it take to do 10^{100} operations?

1.3 Problem 5: Create a GPG key

Evidently, many really smart people find public key cryptography extremely hard to use for email in practice. I have professional colleagues who are amazing programs and world-class experts in number theory, and still they seem incapable of setting up GPG to exchange encrypted emails with me.

So your turn. Create a GPG (Gnu Privacy Guard) key and paste the public key below. I can now use this key to send you messages.

(You can install GPG on your computer, or if you dont care too much, just type +New in SageMathCloud, create a Terminal, and in the terminal you can use the gpg command. You may have to type man gpg or google for tutorials to figure out how to use it. Please succeed, since I want to be able to tell my colleagues that every undergrad in my elementary number theory class was able to do this!)

1.3.1 Problem 6: Your Project

Write a really rough draft of your project. Include a link here so I can look at it.