Math 195: Demystifying Mathematics

Homework 7 : Due May 1

This homework assignment will take you through an example of the mathematics which is used to keep credit card numbers safe when they are sent across digital channels (such as during an online purchase). If you enter your credit card number online, the company you are buying from needs to know what your number is, but you don't want to directly send the number, as anyone eavesdropping could steal your credit card number.

Math to the rescue! The basic setup is as follows: Alice wants to send Bob a secret message but on a public channel (like over the internet). Bob will give Alice a "key" that she will use to garble the message before she sends it so it looks like gibberish to the eavesdropper (Eve is the name typically given for the eavesdropper). The process Alice does to send the message is called "encrypting". Bob will then have a way (mathematically) to secretly "ungarble" the sent message in order to find Alice's original message (this process is called "decrypting"). The main point is that the key is publicly known and yet only Bob has the extra information needed to decrypt the message properly.

The scheme we describe is called **RSA public key encryption scheme** for Ron **R**ivest, Adi **S**hamir, and Len **A**dleman, and it was developed in the mid 1970s.

If you're stuck on the math of either of these problems, remember you are welcome to email me to set up an appointment to meet.

1. RSA uses mathematics we talked about earlier in the semester. This first problem just gets you to remember some of those processes. We talked before break about the idea of modular arithmetic, that for integers a, b, and n, the statement $a \equiv b \bmod n$ means that a and b have the same remainder when divided by n. So $7 \equiv 2 \bmod 5$, or we also say $7 \bmod 5 = 2$. Show me how you computed the following two parts (a) and (b), and then read carefully the next two examples.

   (a) What is $356 \bmod 19$ (your answer should be a number between 0 and 18)?

   (b) What is $74 \bmod 11$ (again, your answer should be a number between 0 and 10)?

   Finally we need a special result which gives us a simple way to compute $a \bmod n$ if a is very large. We'll call it **Important Property**: $ab \bmod n = (a \bmod n)(b \bmod n) \bmod n$. Think of this as saying "You can do the mod part before you multiply."

   Ex: Since $357 = 21 \cdot 17$, if we want to know $357 \bmod 13$ we can just apply the Important Property to get $[(21 \bmod 13) \cdot (17 \bmod 13)] \bmod 13 = (8 \cdot 4) \bmod 13 = 32 \bmod 13 = 6$. The idea is that 21 and 17 are easier to determine mod 13 than 357 is.

   We will really use the Important Property to compute when a and b are the same number, so to compute powers like $35^9 \bmod 71$. If you type 35^9 into your calculator you will see that the

number is too large for us to work with directly, even Google writes it in scientific notation shorthand, so we need another way to compute the remainder when 35^9 is divided by 71. First notice $35 \bmod 71 = 35$ and $35^2 \bmod 71 = 1225 \bmod 71 = 18$, by using the Important Property with a and b both being 35. We apply the Important Property yet again to get $35^4 \bmod 71 = (35^2 \bmod 71)(35^2 \bmod 71) \bmod 71 = (18 \cdot 18) \bmod 71 = 324 \bmod 71 = 40$. So $35^4 \equiv 40 \bmod 71$.

Now we use the Important Property once again to see that:

$35^8 \bmod 71 = (35^4 \bmod 71)(35^4 \bmod 71) \bmod 71 = (40 \cdot 40) \bmod 71 = 1600 \bmod 71 = 38 \bmod 71$. And finally, putting all the pieces together $35^9 \bmod 71 = 35^8 \cdot 35 \bmod 71 = (38 \bmod 71)(35 \bmod 71) = 1330 \bmod 71 = 52$. The idea is that instead of trying to compute with the huge number35^9 directly, we work our way up using increasing powers: 2, then 4, then 8, then 16, etc. all of which keep the "mod" part more manageable.

2. So how does the RSA algorithm work? Below I go through it step-by-step. You should turn in your work to answer the green questions below.

   (a) Bob picks 2 primes p and q and a number r that has no divisors (except 1) in common with m where $m = \text{lcm}(p-1, q-1)$ (in language we learned earlier in the semester, we say m and r are relatively prime, or $\gcd(m, r) = 1$). For our example, say Bob picks $p = 5$, $q = 17$, $r = 3$. What is m in this case and is it truly relatively prime to r? Why?

   (b) Bob makes $n = pq$ and r publicly known. In this example $n = 85$. This is the **key**.

   (c) Alice wants to send Bob numbers 9, 2, and 13. She looks up Bob's n and r and encrypts her message by sending: $9^r \bmod n$, $2^r \bmod n$, $13^r \bmod n$. What message does Alice send Bob? In other words, what are $9^r \bmod n$, $2^r \bmod n$, and $13^r \bmod n$? These are smaller, more manageable numbers, but don't forget the Important Property!

   (d) Bob needs to "reverse" the procedure Alice did. First he takes m from above (the least common multiple) and finds an integer s so that $r \cdot s = 1 \bmod m$. For our example where $r = 3$, find an s so that $r \cdot s = 1 \bmod m$. I suggest just trying integers for s, starting at 1. If you get to 15 without finding one, you made a mistake.

   (e) By the way we picked p, q, r, s, m, and n it turns out that $(9^r)^s \bmod n = 9$ (and, in general, for any numbers with the same properties as we defined above: $(a^r)^s \bmod n = a$ - this fact requires knowing a bit more than we've learned in this class in a field of math called number theory). Alice sent Bob 9^r, which you figured out in (c) and which I'll call "x" for the moment. Then Bob can figure out the original message "9" by computing x^s. Compute x^s where x is your answer to $9^r \bmod n$ in (c) and s is the value you found in (d). Don't forget the Important Property! Did you get "9"? If yes, awesome and go on to the next question. If not, go back and re-do (c) and (d) to make sure you didn't make an arithmetic mistake.

   (f) Once you get the right answer in (e), take another value Alice sent Bob (originally either 2 or 13 and which you found the encrypted version in (c)) and decrypt it like you did for 9 in (e). No need to recompute s. Once Bob finds s, he never has to recompute it.

Why is this scheme safe? Why can't Eve read the original message Alice and Bob sent back and forth? To decrypt the message Eve needs the value s above *which only Bob knows*, but to get s she needs $\text{lcm}(p-1, q-1)$ which requires knowing p and q. *Again, only Bob knows*

both primes. Even Alice only knows their product. The only way for Eve to find p and q is to factor n and in general this is very hard to do. Of course, with our example, it's very easy to factor $n = 85$ but in practice, current systems use huge prime numbers. The safety of RSA hinges on the fact that there is no known *fast* algorithm to factor *large* integers. Right now we don't have a fast way to factor, but someone could come along in the future and find a fast factoring algorithm, and then internet security could be in trouble. To emphasize, what you just did above is exactly what is happening behind the scenes with online credit card purchases, just with much bigger numbers.