CS 70 Spring 2015 — Discrete Mathematics and Probability Theory — Vazirani — Discussion 6M

1. RSA with a partner

Find a partner and run through the RSA algorithm. This means:

- One of you picks two primes p and q.[1] Compute $N = pq$.
- Pick an encryption key e (relatively prime to $(p-1)(q-1)$) and compute the decryption key d, which is a multiplicative inverse of e mod $(p-1)(q-1)$.
- Tell your partner N and e; keep p, q, and d secret.
- Your partner chooses a message m, encrypts it by computing $E(m) = m^e \pmod N$, and tells you $E(m)$.
- You decrypt by computing $D(m) = m^d \pmod N$. Confirm with your partner that you have succeeded in transmitting the correct message.
- Switch places with your partner, and repeat.

2. Baby Fermat

Assume that a does have a multiplicative inverse $\pmod m$. Let us prove that its multiplicative inverse can be written as $a^k \pmod m$ for some $k \geq 0$.

- Consider the sequence $a, a^2, a^3, \ldots \pmod m$. Prove that this sequence has repetitions.

- Assuming that $a^i \equiv a^j \pmod m$, where $i > j$, what can you say about $a^{i-j} \pmod m$?

- Prove that the multiplicative inverse can be written as $a^k \pmod m$. What is k in terms of i and j?

[1] In practice, we use very large primes for RSA, but for the purpose of this exercise, choose smaller numbers to make the computations less complicated.

3. Bijections

Consider the function

$$f(x) = \begin{cases} x, & \text{if } x \geq 1; \\ 3x-2, & \text{if } \frac{1}{2} \leq x < 1; \\ -x, & \text{if } -1 \leq x < \frac{1}{2}; \\ 2x+3, & \text{if } x < -1. \end{cases}$$

- If the domain and range of f are $\mathbb{N}$, is f injective (one-to-one), surjective (onto), bijective?

- If the domain and range of f are $\mathbb{Z}$, is f injective (one-to-one), surjective (onto), bijective?

- If the domain and range of f are $\mathbb{R}$, is f injective (one-to-one), surjective (onto), bijective?

4. RSA

In this problem you play the role of Amazon, who wants to use RSA to be able to receive messages securely.

a. Amazon first generates two large primes p and q. She picks $p = 13$ and $q = 19$ (in reality these should be 512-bit numbers). She then computes $N = pq$. Amazon chooses e from $e = 37, 38, 39$. Only one of those values is legitimate, which one? (N, e) is then the public key.

b. Amazon generates her private key d. She keeps d as a secret. Find d. Explain your calculation.

c. Bob wants to send Amazon the message $x = 102$. How does he encrypt his message using the public key, and what is the result?
Note: For this problem you may find the following trick of fast exponentiation useful. To compute x^k, first write k in base 2 then use repeated squaring to compute each power of 2. For example, $x^7 = x^{4+2+1} = x^4 \cdot x^2 \cdot x^1$.

d. Amazon receives an encrypted message $y = 141$ from Charlie. What is the unencrypted message that Charlie sent her?