

Due: Saturday, 10/1, 4:00 PM
Grace period until Saturday, 10/1, 6:00 PM

Sundry

Before you start writing your final homework submission, state briefly how you worked on it. Who else did you work with? List names and email addresses. (In case of homework party, you can just describe the group.)

1 RSA Practice

Consider the following RSA schemes and solve for asked variables.

- (a) Assume for an RSA scheme we pick 2 primes $p = 5$ and $q = 11$ with encryption key $e = 9$, what is the decryption key d ? Calculate the exact value.
- (b) If the receiver gets 4, what was the original message?
- (c) Encode your answer from part (b) to check its correctness.

2 Tweaking RSA

You are trying to send a message to your friend, and as usual, Eve is trying to decipher what the message is. However, you get lazy, so you use $N = p$, and p is prime. Similar to the original method, for any message $x \in \{0, 1, \dots, N-1\}$, $E(x) \equiv x^e \pmod{N}$, and $D(y) \equiv y^d \pmod{N}$.

- (a) Show how you choose e and d in the encryption and decryption function, respectively. Prove that the message x is recovered after it goes through your new encryption and decryption functions, $E(x)$ and $D(y)$.
- (b) Can Eve now compute d in the decryption function? If so, by what algorithm?
- (c) Now you wonder if you can modify the RSA encryption method to work with three primes ($N = pqr$ where p, q, r are all prime). Explain how you can do so, and include a proof of correctness showing that $D(E(x)) = x$.

3 Secret Sharing

Suppose the Oral Exam questions are created by 2 TAs and 3 Readers. The answers are all encrypted, and we know that:

- Two TAs together should be able to access the answers
- Three Readers together should be able to access the answers
- One TA and one Reader together should also be able to access the answers

Design a Secret Sharing scheme to make this work.

4 Trust No One

Gandalf has assembled a fellowship of eight peoples to transport the One Ring to the fires of Mount Doom: four hobbits, two humans, one elf, and one dwarf. The ring has great power that may be of use to the fellowship during their long and dangerous journey. Unfortunately, the use of its immense power will eventually corrupt the user, so it must not be used except in the most dire of circumstances. To safeguard against this possibility, Gandalf wishes to keep the instructions a secret from members of the fellowship. The secret must only be revealed if enough members of the fellowship are present and agree to use it.

Gandalf has hired your services to help him come up with a secret sharing scheme that accomplishes this task, summarized by the following points:

- There is a party of four hobbits, two humans, an elf, and a dwarf, and a secret message that must remain unknown to everyone if not enough members of the party agree.
- A group of people consisting of at least two people from different people classes and at least one people class that is fully represented (i.e., has all members present) can unlock the secret of the ring.

A few examples: only four hobbits agreeing to use the ring is not enough to know the instructions. One human and three hobbits is not enough. However, all four hobbits and one human agreeing is enough. Both humans and the dwarf agreeing is enough.

5 Lagrange? More like Lamegrage.

In this problem, we walk you through an alternative to Lagrange interpolation.

- (a) Let's say we wanted to interpolate a polynomial through a single point, (x_0, y_0) . What would be the polynomial that we would get? (This is not a trick question.)

- (b) Call the polynomial from the previous part $f_0(x)$. Now say we wanted to define the polynomial $f_1(x)$ that passes through the points (x_0, y_0) and (x_1, y_1) . If we write $f_1(x) = f_0(x) + a_1(x - x_0)$, what value of a_1 causes $f_1(x)$ to pass through the desired points?
- (c) Now say we want a polynomial $f_2(x)$ that passes through (x_0, y_0) , (x_1, y_1) , and (x_2, y_2) . If we write $f_2(x) = f_1(x) + a_2(x - x_0)(x - x_1)$, what value of a_2 gives us the desired polynomial?
- (d) Suppose we have a polynomial $f_i(x)$ that passes through the points (x_0, y_0) , ..., (x_i, y_i) and we want to find a polynomial $f_{i+1}(x)$ that passes through all those points and also (x_{i+1}, y_{i+1}) . If we define $f_{i+1}(x) = f_i(x) + a_{i+1} \prod_{j=0}^i (x - x_j)$, what value must a_{i+1} take on?

6 Equivalent Polynomials

This problem is about polynomials with coefficients in $\text{GF}(q)$ for some prime $q \in \mathbb{N}$. We say that two such polynomials f and g are *equivalent* if $f(x) = g(x)$ for every $x \in \text{GF}(q)$.

- (a) Use Fermat's Little Theorem to find a polynomial with degree strictly less than 5 that is equivalent to $f(x) = x^5$ over $\text{GF}(5)$; then find a polynomial with degree strictly less than 11 that is equivalent to $g(x) = 1 + 3x^{11} + 7x^{13}$ over $\text{GF}(11)$.
- (b) Prove that whenever $f(x)$ has degree $\geq q$, it is equivalent to some polynomial $\tilde{f}(x)$ with degree $< q$.

7 The CRT and Lagrange Interpolation

Let n_1, \dots, n_k be pairwise co-prime, i.e. n_i and n_j are co-prime for all $i \neq j$. The Chinese Remainder Theorem (CRT) tells us that there exist solutions to the following system of congruences:

$$x \equiv a_1 \pmod{n_1} \tag{1}$$

$$x \equiv a_2 \pmod{n_2} \tag{2}$$

$$\vdots \tag{(\cdot)}$$

$$x \equiv a_k \pmod{n_k} \tag{k}$$

and all solutions are equivalent $\pmod{n_1 n_2 \cdots n_k}$. For this problem, parts (a)-(c) will walk us through a proof of the Chinese Remainder Theorem. We will then use the CRT to revisit Lagrange interpolation.

- (a) We start by proving the $k = 2$ case: Prove that we can always find an integer x_1 that solves (1) and (2) with $a_1 = 1, a_2 = 0$. Similarly, prove that we can always find an integer x_2 that solves (1) and (2) with $a_1 = 0, a_2 = 1$.
- (b) Use part (a) to prove that we can always find at least one solution to (1) and (2) for any a_1, a_2 . Furthermore, prove that all possible solutions are equivalent $\pmod{n_1 n_2}$.

- (c) Now we can tackle the case of arbitrary k : Use part (b) to prove that there exists a solution x to (1)-(k) and that this solution is unique $(\text{mod } n_1 n_2 \cdots n_k)$.
- (d) For polynomials $p_1(x)$, $p_2(x)$ and $q(x)$ we say that $p_1(x) \equiv p_2(x) \text{ mod } q(x)$ if $p_1(x) - p_2(x)$ is of the form $q(x) \times m(x)$ for some polynomial $m(x)$.

Define the polynomials $x - a$ and $x - b$ to be co-prime if they have no common divisor of degree 1. Assuming that the CRT still holds when replacing x, a_i and n_i with polynomials (using the definition of co-prime polynomials just given), show that the system of congruences

$$p(x) \equiv y_1 \pmod{(x - x_1)} \quad (1')$$

$$p(x) \equiv y_2 \pmod{(x - x_2)} \quad (2')$$

$$\vdots \quad (\vdots)$$

$$p(x) \equiv y_k \pmod{(x - x_k)} \quad (k')$$

has a unique solution $(\text{mod } (x - x_1) \cdots (x - x_k))$ whenever the x_i are pairwise distinct. What is the connection to Lagrange interpolation?

Hint: To show that a unique solution exists, you may use the fact that the CRT has a unique solution when certain properties are satisfied.