CS 70 Discrete Mathematics and Probability Theory
Fall 2023 Rao, Tal

HW 05

Due: Saturday, 9/30, 4:00 PM
Grace period until Saturday, 9/30, 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

Note 7

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

Note 7

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 $x \in \{0, 1, \ldots, N-1\}$, $E(x) \equiv x^e \pmod{N}$, and $D(y) \equiv y^d \pmod{N}$.

(a) Show how you choose e and d in the encryption and decryption function, respectively. Prove the correctness property: 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 the modifications made to encryption and decryption and include a proof of correctness showing that $D(E(x)) = x$.

3 Secret Sharing

Note 8

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
- One TA by themself or two Readers by themselves should not be able to access the answers.

Design a Secret Sharing scheme to make this work.

4 One Point Interpolation

Note 8

Suppose we have a polynomial $f(x) = x^k + c_{k-1}x^{k-1} + \cdots + c_2x^2 + c_1x + c_0$.

(a) Can we determine $f(x)$ with k points? If so, provide a set of inputs $x_0, x_1, \ldots, x_{k-1}$ such that knowing points $(x_0, f(x_0)), (x_1, f(x_1)), \ldots, (x_{k-1}, f(x_{k-1}))$ allows us to uniquely determine $f(x)$, and show how $f(x)$ can be determined from such points. If not, provide a proof of why this is not possible.

(b) Now, assume each coefficient is an integer satisfying $0 \leq c_i < 100 \quad \forall i \in [0, k-1]$. Can we determine $f(x)$ with one point? If so, provide an input x_* such that knowing the point $(x_*, f(x_*))$ allows us to uniquely determine $f(x)$, and show how $f(x)$ can be determined from this point. If not, provide a proof of why this is not possible.

5 Lagrange? More like Lamegrange.

Note 8

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. A degree 0 polynomial is fine.)

(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

Note 7
Note 8

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

(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 GF(5); then find a polynomial with degree strictly less than 11 that is equivalent to $g(x) = 4x^{70} + 9x^{11} + 70$ over GF(11).

(b) In GF(p), prove that whenever $f(x)$ has degree $\geq p$, it is equivalent to some polynomial $\tilde{f}(x)$ with degree $< p$.