CS 70 Discrete Mathematics and Probability Theory
Fall 2021

HW 5

Due: Saturday 10/02, 4:00 PM
Grace period until Saturday 10/02, 5:59 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 RSA with Multiple Keys

Members of a secret society know a secret word. They transmit this secret word x between each other many times, each time encrypting it with the RSA method. Eve, who is listening to all of their communications, notices that in all of the public keys they use, the exponent e is the same. Therefore the public keys used look like $(N_1, e), \ldots, (N_k, e)$ where no two N_i's are the same. Assume that the message is x such that $0 \le x < N_i$ for every i.

(a) Suppose Eve sees the public keys $(p_1q_1, 7)$ and $(p_1q_2, 7)$ as well as the corresponding transmissions. Can Eve use this knowledge to break the encryption? If so, how? Assume that Eve cannot compute prime factors efficiently. Think of p_1, q_1, q_2 as massive 1024-bit numbers. Assume p_1, q_1, q_2 are all distinct and are valid primes for RSA to be carried out.

(b) The secret society has wised up to Eve and changed their choices of N, in addition to changing their word x. Now, Eve sees keys $(p_1q_1, 3)$, $(p_2q_2, 3)$, and $(p_3q_3, 3)$ along with their transmissions. Argue why Eve cannot break the encryption in the same way as above. Assume $p_1, p_2, p_3, q_1, q_2, q_3$ are all distinct and are valid primes for RSA to be carried out.

(c) Let's say the secret x was not changed ($e = 3$), so they used the same public keys as before, but did not transmit different messages. How can Eve figure out x?

4 How Many Polynomials?

Let $P(x)$ be a polynomial of degree at most 2 over GF(5). As we saw in lecture, we need $d+1$ distinct points to determine a unique d-degree polynomial, so knowing the values for say, $P(0)$, $P(1)$, and $P(2)$ would be enough to recover P. (For this problem, we consider two polynomials to be distinct if they return different values for any input.)

(a) Assume that we know $P(0) = 1$, and $P(1) = 2$. Now consider $P(2)$. How many values can $P(2)$ have? How many distinct possibilities for P do we have?

(b) Now assume that we only know $P(0) = 1$. We consider $P(1)$ and $P(2)$. How many different $(P(1), P(2))$ pairs are there? How many distinct possibilities for P do we have?

(c) Now, let P be a polynomial of degree at most d on GF(p) for some prime p with $p > d$. Assume we only know P evaluated at $k \le d+1$ different values. How many different possibilities do we have for P?

(d) A polynomial with integer coefficients that cannot be factored into polynomials of lower degree on a finite field, is called an irreducible or prime polynomial.

Show that $P(x) = x^2 + x + 1$ is a prime polynomial on GF(5).

5 Polynomials over Galois Fields

Real numbers, complex numbers, and rational numbers are all examples of *fields*. A field is a set of numbers on which operations such as addition, multiplication, and inverses behave as they do on rational and real numbers. Galois fields are fields with only a finite number of elements, unlike fields such as the real numbers. Galois fields are denoted by GF(p), where p is a prime number and is also the number of elements in the field. Working over a GF(p) can be thought of as working with numbers in $\pmod{p}$.

(a) In the field GF(p), where p is a prime, how many roots does $q(x) = x^p - x$ have? Use this fact to express $q(x)$ in terms of degree one polynomials. Justify your answers.

(b) Prove that in GF(p), where p is a prime, whenever $f(x)$ has degree $\geq p$, it is equivalent to some polynomial $\tilde{f}(x)$ with degree $< p$.

(c) Show that if P and Q are polynomials over the reals (or complex numbers, or rationals) and $P(x)Q(x) = 0$ for all x, then either $P(x) = 0$ for all x, $Q(x) = 0$ for all x, or both.

(d) Show that the claim in part (c) is false for finite fields GF(p), where p is a prime.

6 Lagrange? More like Lamegrange.

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?

7 Secret Sharing

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

- Both TAs should be able to access the answers
- All 3 Readers can also access the answers
- One TA and one Reader should also be able to do the same

Design a Secret Sharing scheme to make this work.

8 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.

Requiring all eight members to agree is certainly a sufficient condition to know the instructions, but it seems excessive. However, we also know that the separate peoples (hobbits, humans, elf, and dwarf) do not completely trust each other so instead we decide to require members from at least two different peoples in order to use the ring. In particular, we will require a unanimous decision by all members of one group in addition to at least one member from a different group. That is, if only the four hobbits want to use the ring, then they alone should not have sufficient information to figure out the instructions. Same goes for the two humans, the elf, and the dwarf.

More explicitly, only four hobbits agreeing to use the ring is not enough to know the instructions. Only two humans agreeing is not enough. Only the elf agreeing is not enough. Only the dwarf agreeing is not enough. However, all four hobbits and a man agreeing is enough. Both humans and a dwarf agreeing is enough. Both the elf and the dwarf agreeing is enough.

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.
- There is a secret message that needs to be known if enough members of the party agree.
- The message must remain unknown to everyone if not enough members of the party agree.
- If only the members of one people agree, the message remains a secret.
- If all the members of one people agree plus at least one additional person, the message can be determined.