RSA, Polynomials, Secret Sharing 4

Computer Science Mentors 70

September 24 - 28, 2018

1 RSA

1.1 Introduction

Main idea: Given two large primes, p and q, and a message x (an integer), find an encryption function E and an decryption function D such that $D(E(x)) = x$. In other words, two people can encrypt and decrypt a message if they know E and D.

Mechanism:

N = pq

$E(x) = x^e$ mod N

$D(x) = x^d$ mod N, where $d = e^{-1}$ mod$(p-1)(q-1)$

The pair (N, e) is the recipient's **public key**, and d is the recipient's **private key**. The sender sends $E(x)$ to the recipient, and the recipient uses $D(x)$ to recover the original message. The security of RSA relies on the assumption that given N, there is no efficient algorithm to determine $(p-1)(q-1)$.

1.2 Questions

1. **How does RSA work?**

   a. Alice wants to send Bob a message $m = 5$ using his public key ($n = 26$, $e = 11$). What cipher text E(m) will Alice send?

   Solution:

   $$\begin{aligned} 5^1 &= 5 \mod 26 \\ 5^2 &= 25 \mod 26 \\ &= -1 \mod 26 \\ 5^4 &= (-1)^2 \mod 26 \\ &= 1 \mod 26 \\ 5^8 &= 1 \mod 26 \\ 5^{11} &= 5^8 * 5^2 * 5^1 \mod 26 \\ &= 1 * -1 * 5 \mod 26 \\ &= -5 \mod 26 \\ &= 21 \mod 26 \end{aligned}$$

   b. What is the value of d (Bob's private key) in this scheme? Note that traditional RSA schemes use much larger prime numbers, so its harder to break n down into its prime factors than it is in this problem.

   Solution: $n = 26 \rightarrow$ because $26 = pq$ and $p \neq a * q$ for all a within integers, $p = 13$, $q = 2$

   $$\begin{aligned} d &= e^{-1} \mod (13-1)(2-1) \\ d &= 11^{-1} \mod 12 \\ d &= 11 \end{aligned}$$

2. In RSA, if Alice wants to send a confidential message to Bob, she uses Bob's public key to encode it. Then Bob uses his private key to decode the message. Suppose that Bob chose $N = 77$. And then Bob chose $e = 3$ so his public key is (3, 77). And then Bob chose $d = 26$ so his private key is (26, 77).
   Will this work for encoding and decoding messages? If not, where did Bob first go wrong in the above sequence of steps and what is the consequence of that error? If it does work, then show that it works.

Solution: e should be co-prime to $(p-1)(q-1)$.
$e = 3$ is not co-prime to $(7-1)(11-1) = 60$, so this is incorrect, since e does not have an inverse $\mod 60$.

2 Polynomials

2.1 Introduction

There are two fundamental properties of polynomials:

1. A non-zero polynomial of degree d has at most d real roots.
2. $d+1$ distinct points uniquely define a polynomial of degree at most d.

We can represent polynomials in 2 ways:

1. **Coefficient Representation:** This representation is probably what you've seen before. We could represent a polynomial of degree d like this:

$$p(x) = a_d x^d + a_{d-1}x^{d-1} + a_{d-2}x^{d-2} + ... + a_1 x + a_0$$

   As you can see, we need $d+1$ coefficients ($a_0 ... a_d$).
2. **Value Representation:** Using the second property of polynomials, if we have a collection of $d+1$ distinct points

$$(x_0, y_0), (x_1, y_1), ..., (x_d, y_d)$$

   we actually would have a unique polynomial of degree at most d.

Going from coefficient to value representation is easy: evaluate the polynomial at $d+1$ different points. The other way is slightly harder. There are 2 ways that we can do this:

1. **System of equations** We know the generic equation for a polynomial of degree d is $p(x) = a_d x^d + a_{d-1}x^{d-1} + a_{d-2}x^{d-2} + ... + a_1 x + a_0$. So we "plug in" our $d+1$ points into this equation to obtain $d+1$ equations in $d+1$ unknowns (the coefficients).
2. **Lagrange Interpolation** Solving a system of equations, especially over a modulus space can be difficult, so there's a formula that we can use to directly obtain the coefficient representation.

$$p(x) = \sum_{i=0}^{d} y_i \frac{\prod_{j \neq i} x - x_j}{\prod_{j \neq i} x_i - x_j}$$

You may be used to doing polynomials as functions from $\mathbb{R} \to \mathbb{R}$. In this class, we work over *Galois Field*. This means, for some prime p, our functions are from $\{0, 1, ..., p-1\} to \{0, 1, ..., p-1\}$. To do this, we take the result mod p when we evaluate the function, and our only possible inputs are integers. Addition, subtraction, multiplication, and exponentiation all work the same over Galois field as they do over the real numbers, however, division is slightly different. For example, the expression $\frac{x-1}{3} \mod 7$ would be valid in the real number space, but we can't have fractions in Galois fields. Remember that division in modulus is the same as multiplying by the inverse. So in GF(7) $\frac{x-1}{3} \equiv 5(x-1) \mod 7$.

2.2 Questions

1. Let p be a degree 2 polynomial and q be another degree 2 polynomial in GF(7). Both of them go through the points (1, 2), (2, 1), and (3, 4). Find p and q.

Solution: Using Lagrange interpolation:

$$p(x) = 2 * \frac{(x-2)(x-3)}{(1-2)(1-3)} + 1 * \frac{(x-1)(x-3)}{(2-1)(2-3)} + 4 * \frac{(x-1)(x-2)}{(3-1)(3-2)}$$
$$p(x) = x^2 + 5x + 6 - x^2 + 4x - 3 + 2x^2 - 6x + 4$$
$$p(x) = 2x^2 - 7x + 7$$
$$q(x) = 2x^2(\mod 7)$$

To do this with coefficients, we have the system of equations:

$$p(1) \equiv a_2 + a_1 + a_0 \equiv 2 \mod 7$$
$$p(2) \equiv 4a_2 + 2a_1 + a_0 \equiv 1 \mod 7$$
$$p(3) \equiv 9a_2 + 3a_1 + a_0 \equiv 2a_2 + 3a_1 + a_0 \equiv 4 \mod 7$$

This is a system of 3 equations with 3 variables that can be solved (painfully) to get the same answer.

2. Let $P(x)$ be a polynomial of degree 2 over GF(7).
   1. Suppose $P(0) = 3$ and $P(1) = 2$. How many values can $P(5)$ have? How many distinct polynomials are there?

   Solution: 7 polynomials, one for each different possible value of $P(5)$.

   2. Suppose we only know $P(0) = 3$. How many possible pairs of $(P(1), P(5))$ are there? How many different polynomials are there?

   Solution: 49 polynomials because there are 7 possible values for both $P(1)$ and $P(5)$.

   3. If we only know k different points, where $k \leq d$, of a degree d polynomial over GF(p), how many possible polynomials are there?

   Solution: There are p^{d+1-k} polynomials. Since we need $d+1$ points to uniquely determine the polynomial, we need to choose values for the $d + 1 - k$ remain-

ing points that we don't know, and each point can be one of p possible values. For $k = d + 1$ there is only 1 possible polynomial.

3. Define the sequence of polynomials by $P_0(x) = x+12$, $P_1(x) = x^2-5x+5$ and $P_n(x) = xP_{n-2}(x) - P_{n-1}(x)$. (For instance, $P_2(x) = 17x - 5$ and $P_3(x) = x^3 - 5x^2 - 12x + 5$.) Show that $P_n(7) \equiv 0 \pmod{19}$ for every $n \in N$.

Solution:

4. Prove using strong induction.

Base Case There are two base cases because each polynomial is defined in terms of the two previous ones except for P_0 and P_1.

$$P_0(7) \equiv 7 + 12 \equiv 19 \equiv 0 \pmod{19}$$
$$P_1(7) \equiv 7^2 - 5 \cdot 7 + 5 \equiv 49 - 35 + 5 \equiv 19 \equiv 0 \pmod{19}$$

Inductive Hypothesis Assume $P_n(7) \equiv 0 \pmod{19}$ for every $n \leq k$.

Inductive Step Using the definition of P_{k+1}, we have that

$$\begin{aligned} P_{k+1}(7) &\equiv xP_{k-1}(7) - P_k(7) \pmod{19} \\ &\equiv x \cdot 0 - 0 \pmod{19} \\ &\equiv 0 \pmod{19} \end{aligned}$$

Therefore, $P_n(7) \equiv 0 \pmod{19}$ for all natural numbers n.

3 Secret Sharing

3.1 Introduction

1. Set up: n officials indexed from 1 to n. Secret s is an integer. Use $GF(q)$: q is a prime number such that $q > n$ and $q > s$.
2. Scheme: Pick a random $p(x)$ of degree $k-1$ such that $p(0) = s$. Thus,
   (a) Any k officials can use Lagrange Interpolation to find $p(x)$, therefore x.
   (b) Any $k-1$ officials have no information about s.

3.2 Questions

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

   (a) Together, both TAs should be able to access the answers

   (b) All 3 Readers can also access the answers

   (c) One TA and one Reader should also be able to do the same

   Design a secret sharing scheme to make this work.

   Solution: Use a degree 2 polynomial which requires at least 3 shares to recover the polynomial. Generate a total of 7 points; give each Reader a point and each TA 2 points. Then, all possible combinations will have at least 3 points to recover the answer key. Basically the point of this problem is to assign different weights to different classes of people. If we give one point to everyone, then 2 Readers can also recover the secret and the scheme is broken.

2. The United Nations (for the purposes of this question) consists of n countries, each having k representatives. A vault in the United Nations can be opened with a secret combination s. The vault should only be opened in one of two situations. First, it can be opened if all n countries in the UN help. Second, it can be opened if at least m countries get together with the Secretary General of the UN.

   Propose a scheme that gives private information to the Secretary General and n countries so that s can only be recovered under either one of the two specified conditions.

   Solution: Solution 1: Have two schemes, one for the first condition and one for the second.

For the first condition: just one polynomial of degree n - 1 or less would do, where each country gets one point. The polynomial evaluated at 0 would give the secret.

For the second condition: one polynomial is created of degree m - 1 and a point is given to each country. Another polynomial of degree 1 is created, where one point is given to the Secretary General and the second point can be constructed from the first polynomial if m or more of the countries come together. With these two points, we have a unique 1-degree polynomial, which could give the secret evaluated at 0.

Solution 2: Create a polynomial of degree n-1, and give each country one point. This satisfies the condition that the countries on their own should be able to find s on their own. To account for the Secretary General, give the Secretary General n-m points. That way, any m countries plus the Secretary General together have n points, which allows them to access s.