CS 70 Discrete Mathematics and Probability Theory
Fall 2021 HW 5

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.

Solution:

(a) The private key d is defined as the inverse of $e \pmod{(p-1)(q-1)}$. Thus we need to compute $9^{-1} \bmod (5-1)(11-1) = 9^{-1} \bmod 40$. Find inverse of e mod $(5-1)(11-1) = 40$. Compute egcd$(40,9)$:

$$\begin{aligned} \text{egcd}(40,9) &= \text{egcd}(9,4) && [4 = 40 \bmod 9 = 40 - 4(9)] \\ &= \text{egcd}(4,1) && [1 = 9 \bmod 4 = 9 - 2(4)]. \\ 1 &= 9 - 2(4). \\ 1 &= 9 - 2(40 - 4(9)) \\ &= 9 - 2(40) + 8(9) = 9(9) - 2(40). \end{aligned}$$

We get $-2(40) + 9(9) = 1$. So the inverse of 9 is 9. So $d = 9$.

(b) 4 is the encoded message. We can decode this with $D(m) \equiv m^d \equiv 4^9 \equiv 14 \pmod{55}$. $4^9 \equiv 14 \pmod{55}$. Thus the original message was 14.

(c) The answer from the second part was 14. To encode the number x we must compute $x^e \bmod N$. Thus, $14^9 \equiv 14 \cdot (14^2)^4 \equiv 14 \cdot (31^2)^2 \equiv 14 \cdot (26^2) \equiv 14 \cdot 16 \equiv 4 \pmod{55}$. This verifies the second part since the encoded message was suppose to be 4.

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

(a) Show how you choose e and d in the encryption and decryption function, respectively. Prove 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 $D(E(x)) = x$.

Solution:

(a) Choose e such that it is coprime with $p-1$, and choose $d \equiv e^{-1} \pmod{p-1}$.
We want to show x is recovered by $E(x)$ and $D(y)$, such that $D(E(x)) = x$.
In other words, $x^{ed} \equiv x \pmod{p}$ for all $x \in \{0, 1, \ldots, N-1\}$.
Proof: By construction of d, we know that $ed \equiv 1 \pmod{p-1}$. This means we can write $ed = k(p-1)+1$, for some integer k, and $x^{ed} = x^{k(p-1)+1}$.

- x is a multiple of p: Then this means $x = 0$, and indeed, $x^{ed} \equiv 0 \pmod{p}$.
- x is not a multiple of p: Then

$$\begin{aligned} x^{ed} &\equiv x^{k(p-1)+1} \pmod{p} \\ &\equiv x^{k(p-1)}x \pmod{p} \\ &\equiv 1^k x \pmod{p} \\ &\equiv x \pmod{p} \end{aligned}$$

  , by using FLT.

And for both cases, we have shown that x is recovered by $D(E(x))$.

(b) Since Eve knows $N = p$, and $d \equiv e^{-1} \pmod{p-1}$, now she can compute d using EGCD.

(c) Let e be co-prime with $(p-1)(q-1)(r-1)$. Give the public key: (N, e) and calculate $d = e^{-1} \pmod{(p-1)(q-1)(r-1)}$. People who wish to send me a secret, x, send $y = x^e \pmod{N}$. We decrypt an incoming message, y, by calculating $y^d \pmod{N}$.

Does this work? We prove that $x^{ed} - x \equiv 0 \pmod{N}$, and thus $x^{ed} = x \pmod{N}$.
To prove that $x^{ed} - x \equiv 0 \pmod{N}$, we factor out the x to get
$x \cdot (x^{ed-1} - 1) = x \cdot (x^{k(p-1)(q-1)(r-1)+1-1} - 1)$ because $ed \equiv 1 \pmod{(p-1)(q-1)(r-1)}$.

We now show that $x \cdot (x^{k(p-1)(q-1)(r-1)} - 1)$ is divisible by p, q, and r. Thus, it is divisible by N, and $x^{ed} - x \equiv 0 \pmod{N}$.
To prove that it is divisible by p:

- if x is divisible by p, then the entire thing is divisible by p.
- if x is not divisible by p, then that means we can use FLT on the inside to show that $(x^{p-1})^{k(q-1)(r-1)} - 1 \equiv 1 - 1 \equiv 0 \pmod{p}$. Thus it is divisible by p.

To prove that it is divisible by q:

- if x is divisible by q, then the entire thing is divisible by q.
- if x is not divisible by q, then that means we can use FLT on the inside to show that $(x^{q-1})^{k(p-1)(r-1)} - 1 \equiv 1 - 1 \equiv 0 \pmod{q}$. Thus it is divisible by q.

To prove that it is divisible by r:

- if x is divisible by r, then the entire thing is divisible by r.
- if x is not divisible by r, then that means we can use FLT on the inside to show that $(x^{r-1})^{k(p-1)(q-1)} - 1 \equiv 1 - 1 \equiv 0 \pmod{r}$. Thus it is divisible by r.

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 $0 \leq x < N_i$ 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?

Solution:

(a) Normally, the difficulty of cracking RSA hinges upon the believed difficulty of factoring large numbers. If Eve were given just p_1q_1, she would (probably) not be able to figure out the factors.

However, Eve has access to two public keys, so yes, she will be able to figure it out. Note that $\gcd(p_1q_1, p_1q_2) = p_1$. Taking GCDs is actually an efficient operation thanks to the Euclidean Algorithm. Therefore, she can figure out the value of p_1, and from there figure out the value of q_1 and q_2 since she has p_1q_1 and p_1q_2.

(b) Since none of the N's have common factors, she cannot find a GCD to divide out of any of the Ns. Hence the approach above does not work.

(c) Eve observes $x^3 \pmod{N_1}$, $x^3 \pmod{N_2}$, $x^3 \pmod{N_3}$. Since all N_1, N_2, N_3 are pairwise relatively prime, Eve can use the Chinese Remainder Theorem to figure out $x^3 \pmod{N_1 N_2 N_3}$. However, once she gets that, she knows x, since $x < N_1$, $x < N_2$, and $x < N_3$, which implies $x^3 < N_1 N_2 N_3$. Uh oh! (Binary search can compute compute x from x^3 in the integers since one can tell if some number is too large or too small.)

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 $k \leq d+1$ 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).

Solution:

(a) 5 polynomials, each for different values of $P(2)$.

(b) Now there are 5^2 different polynomials.

(c) p^{d+1-k} different polynomials. For $k = d+1$, there should only be 1 polynomial.

(d) We can try all possible inputs for x and show that in each case $P(x) \pmod{x} \neq 0$, which means

that $P(x)$ does not have any root on the finite field GF(5).

$$\begin{aligned} x = 0 &\Rightarrow P(0) \equiv 1 \pmod 5 \\ x = 1 &\Rightarrow P(1) \equiv 3 \pmod 5 \\ x = 2 &\Rightarrow P(2) \equiv 2 \pmod 5 \\ x = 3 &\Rightarrow P(3) \equiv 3 \pmod 5 \\ x = 4 &\Rightarrow P(4) \equiv 1 \pmod 5 \end{aligned}$$

Hence $P(x)$ is a prime polynomial.

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.

Solution:

(a) We can factor $q(x) = x^p - x$ into $x(x^{p-1} - 1)$. By Fermat's Little Theorem, for any $a \in \{1, 2, \ldots p-1\}$, $q(a) = a(a^{p-1} - 1) = a(1-1) = 0$. And $q(0) = 0(0^{p-1} - 1) = 0$. So every element of $GF(p)$ is a root. The polynomial $q(x)$ has p roots.

We can write $q(x)$ as a product of its roots:

$$q(x) = \prod_{k=0}^{p-1} (x - k)$$

(b) One proof uses Fermat's Little Theorem. Let $d \geq p$; we'll find a polynomial equivalent to x^p. For any integer, we know

$$\begin{aligned} a^d &= a^{d-p}a^p \\ &\equiv a^{d-p}a \mod p \\ &\equiv a^{d-p+1} \mod p. \end{aligned}$$

In other words x^d is equivalent to the polynomial $x^{d-(p-1)}$. If $d-(p-1) \geq p$, we can show in the same way that x^d is equivalent to $x^{d-2(p-1)}$. Since we subtract $p-1$ every time, the sequence $d, d-(p-1), d-2(p-1), \ldots$ must eventually be smaller than p. Now if $f(x)$ is any polynomial with degree $\geq p$, we can apply this same trick to every x^k that appears for which $k \geq p$.

Another proof uses Lagrange interpolation. Let $f(x)$ have degree $\geq p$. By Lagrange interpolation, there is a unique polynomial $\tilde{f}(x)$ of degree at most $p-1$ passing through the points $(0, f(0)), (1, f(1)), (2, f(2)), \ldots, (p-1, f(p-1))$, and we designed it exactly so that it would be equivalent to $f(x)$.

(c) First, notice that if r is a root of P such that $P(r) = 0$, then r must also be a root of R, since $P(r)Q(r) = 0 \cdot Q(r) = 0$. The same is true for any roots of Q. Also notice that if some value s is neither a root of P nor Q, such that $P(s) \neq 0$ and $Q(s) \neq 0$, then s cannot be a root of R since $P(s)Q(s) \neq 0$. We therefore conclude that the roots of R are the union of the roots of P and Q.

Now we will show the contrapositive. Suppose that P and Q are both non-zero polynomials of degree d_P and d_Q respectively. Then $P(x) = 0$ for at most d_P values of x and $Q(x) = 0$ for at most d_Q values of x. This implies that R has at most $d_P + d_Q$ roots. Since there are an infinite number of values for x (because we are using complex, real, or rational numbers) we can always find an x, call it $x_{\text{not zero}}$, for which $P(x_{\text{not zero}}) \neq 0$ and $Q(x_{\text{not zero}}) \neq 0$. This gives us $P(x_{\text{not zero}})Q(x_{\text{not zero}}) \neq 0$ so R is non-zero.

(d) In GF(p), $x^{p-1} - 1$ and x are both non zero polynomials, but their product, $x^p - x$ is zero for all x by Fermat's Little Theorem.

Examples for a specific p are also acceptable. For example, for GF(2), $P(x) = x$ and $Q(x) = x+1$.

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?

Solution:

(a) We want a degree zero polynomial, which is just a constant function. The only constant function that passes through (x_0, y_0) is $f_0(x) = y_0$.

(b) By defining $f_1(x) = f_0(x) + a_1(x - x_0)$, we get that

$$f_1(x_0) = f_0(x_0) + a_1(x_0 - x_0) = y_0 + 0 = y_0.$$

So now we just need to make sure that $f_1(x_1) = y_1$. This means that we need to choose a_1 such that

$$f_1(x_1) = f_0(x_1) + a_1(x_1 - x_0) = y_1.$$

Solving this for a_1, we get that

$$a_1 = \frac{y_1 - f_0(x_1)}{x_1 - x_0}.$$

(c) We apply similar logic to the previous part. From our definition, we know that

$$f_2(x_0) = f_1(x_0) + a_2(x_0 - x_0)(x_0 - x_1) = y_0 + 0 = y_0.$$

and that

$$f_2(x_1) = f_1(x_1) + a_2(x_1 - x_0)(x_1 - x_1) = y_1 + 0 = y_1.$$

Thus, we just need to choose a_2 such that $f_2(x_2) = y_2$. Putting in our formula for $f_2(x)$, we get that we need a_2 such that

$$f_1(x_2) + a_2(x_2 - x_0)(x_2 - x_1) = y_2.$$

Solving for a_2, we get that

$$a_2 = \frac{y_2 - f_1(x_2)}{(x_2 - x_0)(x_2 - x_1)}.$$

(d) If we try to calculate $f_{i+1}(x_k)$ for $0 \leq k \leq i$, we know one of the $(x - x_j)$ terms (specifically the kth one) will be zero. Thus, we get that

$$f_{i+1}(x_k) = f_i(x_k) + a_{i+1}(0) = y_k + 0 = y_k.$$

So now we just need to pick a_i such that $f_{i+1}(x_{i+1}) = y_{i+1}$. This means that we need to choose a_{i+1} such that

$$f_i(x_{i+1}) + a_{i+1} \prod_{j=0}^{i} (x_{i+1} - x_j) = y_{i+1}.$$

Solving for a_{i+1}, we get that

$$a_{i+1} = \frac{y_{i+1} - f_i(x_{i+1})}{\prod_{j=0}^{i} (x_{i+1} - x_j)}.$$

The method you derived in this question is known as Newtonian interpolation. (The formal definition of Newtonian interpolation uses divided differences, which we don't cover in this class, but it's in effect doing the same thing.) This method has an advantage over Lagrange interpolation in that it is very easy to add in extra points that your polynomial has to go through (as we showed in part (c), whereas Lagrange interpolation would require you to throw out all your previous work and restart. However, if you want to keep the same x values but change the y values, Newtonian interpolation requires you to throw out all your previous work and restart. In contrast, this is fairly easy to do with Lagrange interpolation–since changing the y values doesn't affect the δ_is, you don't have to recalculate those, so you can skip most of the work.

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.

Solution:

Use a degree 2 polynomial and requires at least 3 shares to recover the polynomial. Generate a total of 7 shares, give each Reader a share, and each TA 2 shares. Then, all possible combinations will have at least 3 shares to recover the answer key.

Basically, the point of this problem is to assign different weight to different class of people. If we give one share to everyone, then 2 Readers can also recover the secret and the scheme is broken.

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.

Solution:

Solution 1

There will be two parts to this secret: a unanimity secret U and a multi-people secret M. U ensures that at least all members of one peoples are in agreement while M ensures that members of at least two peoples are in agreement. We will discuss these two in order below. Once both U and M are recovered, they can then be combined to reveal the original secret: each will be a point of the degree-1 polynomial $R(x)$ whose y-intercept contains the secret of the ring.

The *unanimity secret* involves creating a separate secret for each people. We will require all members of that people to join forces in order to reveal the secret. For example, the hobbits will each have distinct points of a degree-3 polynomial and the humans will each have distinct points of a degree-1 polynomial. When all members of a people come together, they will reveal U (encoded, for example, as the y-intercept of each of these polynomials). Note that the elf and the dwarf each know U already since they are the only members of their people.

The *multi-people secret* involves creating a degree-1 polynomial $P_m(x)$ and giving one point to all members of each people. For example, the hobbits may each get $P_m(1)$ while the elf gets $P_m(2)$ and the humans each get $P_m(3)$. In this way if members of any two peoples are in agreement, they can reveal M (encoded, for example, as the y-intercept of $P_m(x)$).

Once U and M are each known, they can be *combined* to determine the final secret. U and M allow us to uniquely determine $R(x)$ and thus $R(0)$, the secret of the ring.

This scheme is an example of hierarchical secret sharing. Let's work out a specific example.

Example: Suppose the secret is $s = 4$, $M = 3$, and $U = 2$. From now on, we can work in GF(5) since $s < 5$ and $n < 5$ (n is the number of people who have pieces of the secret).

First we need to create a degree-1 polynomial $R(x)$ such that $R(0) = s = 4$, $R(1) = M = 3$, and $R(2) = U = 2$. By inspection, $R(x) = 4x + 4$ has these properties (e.g. $R(1) = 4 \cdot 1 + 4 = 8 \equiv 3$).

Now we can create the multi-people secret M. We choose degree-1 polynomial $P_m(x) = x + 3$ and tell each hobbit $P_m(1) = 4$, the elf $P_m(2) = 5 \equiv 0$, each of the humans $P_m(3) = 6 \equiv 1$, and the dwarf $P_m(4) = 7 \equiv 2$. Now any two members of distinct peoples can determine $P_m(x)$ and thus $P_m(0)$ by interpolating their two values.

When creating the unanimity secret U, we first note that each of the dwarf and the elf will be told U directly since they are the only members of their respective people. On the other hand, the humans will each have a point on the degree-1 polynomial $P_{humans}(x)$. Suppose $P_{humans}(x) = 2x + 2$. Then the first human receives $P_{humans}(1) = 4$ and the second receives $P_{humans}(2) = 4 + 2 = 6 \equiv 1$. When they interpolate using these values, they will discover the original polynomial and therefore $P_{humans}(0) = U = 2$. The hobbits will have a similar secret but with a degree-3 polynomial (e.g. $P_{hobbit}(x) = 4x^3 + x^2 + 2$).

Now suppose that two humans and one hobbit come together. The two humans work together to determine U as described above. Together the three of them also know $P_m(3) = 6$ and $P_m(1) = 4$, from which they can find $P_m(x)$ and thus $P_m(0) = M = 3$. Now that they have U and M, they can interpolate to find $R(x)$ and thus $R(0) = s = 4$.

Solution 2

Alternatively, we can construct a single degree 6 polynomial and distribute 1 point to each hobbit, 3 points to each human, 6 points to the elf, and 6 points to the dwarf. We can see that if all the hobbits agree, they will need 3 more points in order to interpolate successfully and each member of all the other peoples are given at least 3 points. Moreover, each of the other peoples have 6 points in total, meaning that if all the humans, the elf, or the dwarf agree, they'll only need one more point which can be provided by any additional member of the party outside their people. On the other hand, the most amount of points that could be obtained from an agreeing group that does not satisfy the requirements would be 6, from the group consisting of one human and all the hobbits. This would be insufficient to interpolate the polynomial so therefore, the scheme fulfills the requirements.