1 RSA Practice

Note 7

Consider the following RSA scheme and answer the specified questions.

(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 $9^{-1} \bmod (5-1)(11-1) = 9^{-1} \bmod 40$. 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 $D(m) \equiv m^d \equiv 4^9 \equiv 14 \pmod{55}$. 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 supposed to be 4.

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 $D(E(x)) = x$.

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 Trust No One

Note 8

Gandalf has assembled a fellowship of nine peoples to transport the One Ring to the fires of Mount Doom: five humans, two hobbits, 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 five humans, two hobbits, 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 five humans agreeing to use the ring is not enough to know the instructions. One hobbit and four humans is not enough. However, all five humans and one hobbit agreeing is enough. Both hobbits and the dwarf agreeing is enough.

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.

The high-level idea is that the secret of the ring requires both the unanimity and multi-people conditions to be satisfied, so we encode the original secret in a polynomial $R(x)$ determinable by the two values U and M; each of U and M themselves are encoded within polynomials as independent secrets determinable when the unanimity and multi-people conditions, respectively, are satisfied. Thus, once both U and M are recovered, they can then be combined to reveal the original secret, since each will be a point of the degree-1 polynomial $R(x)$ whose y-intercept contains the secret of the ring.

We will now detail U and M in order below.

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 humans will each have distinct points of a degree-4 polynomial and the hobbits 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(7) since $s < 7$ and $n < 7$ (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, $R(x) = 6x + 4$ has these properties (e.g. $R(1) = 6 \cdot 1 + 4 = 10 \equiv 3$).

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 $P_m(2) = 5$, each of the humans $P_m(3) = 6$, and the dwarf $P_m(4) = 7 \equiv 0$. 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 hobbits will each have a point on the degree-1 polynomial $P_{hobbits}(x)$. Suppose $P_{hobbits}(x) = 2x + 2$. Then the first hobbit receives $P_{hobbits}(1) = 4$ and the second receives $P_{hobbits}(2) = 4 + 2 = 6$. When they interpolate using these values, they will discover the original polynomial and therefore $P_{hobbits}(0) = U = 2$. The humans will have a similar secret but with a degree-4 polynomial.

Now suppose that two hobbits and one human come together. The two hobbits 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 8 polynomial (which requires 9 points to interpolate) and distribute 1 point to each human, 4 points to each hobbit, 8 points to the elf, and 8 points to the dwarf.

- Suppose all the humans agree. They will need 4 more points in order to interpolate successfully. Each member of all the other peoples are given at least 4 points. Moreover, each of the other peoples have 8 points in total, meaning that if all the hobbits, 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 8, from the group consisting of one hobbit and all but one of the humans. This would be insufficient to interpolate the polynomial so the scheme fulfills the requirements.

4 Equivalent Polynomials

Note 7
Note 8

This problem is about polynomials with coefficients in $\mathrm{GF}(p)$ 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 $x \in \mathrm{GF}(p)$.

(a) Show that $f(x) = x^{p-1}$ and $g(x) = 1$ are **not** equivalent polynomials under $\mathrm{GF}(p)$.

(b) Use Fermat's Little Theorem to find a polynomial with degree strictly less than 5 that is equivalent to $f(x) = x^5$ over $\mathrm{GF}(5)$; then find a polynomial with degree strictly less than 11 that is equivalent to $g(x) = 4x^{70} + 9x^{11} + 3$ over $\mathrm{GF}(11)$.

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

Solution:

(a) For f and g to be equivalent, they must satisfy $f(x) \equiv g(x) \pmod{p}$ for all values of x, including zero. But $f(0) \equiv 0 \pmod{p}$ and $g(0) \equiv 1 \pmod{p}$, so they are not equivalent.

(b) Fermat's Little Theorem says that for any nonzero integer a and any prime number p, $a^{p-1} \equiv 1 \mod p$. We're allowed to multiply through by a, so the theorem is equivalent to saying that $a^p \equiv a \mod p$; note that this is true even when $a = 0$, since in that case we just have $0^p \equiv 0 \pmod{p}$.

The problem asks for a polynomial $\tilde{f}(x)$, different from $f(x)$, with the property that $\tilde{f}(a) \equiv a^5 \mod 5$ for any integer a. Directly using the theorem, $\tilde{f}(x) = x$ will work. We can do something similar with $g(x) = 4x^{70} + 9x^{11} + 3$ modulo 11; since $x^{11} \equiv x \pmod{11}$, we repeatedly substitute x^{11} with x, effectively reducing the exponent by 10. We can only do this as long as the exponent remains greater than or equal to 11, so we end up with $\tilde{g}(x) = 4x^{10} + 9x + 3$.

(c) One proof uses Fermat's Little Theorem. As a warm-up, let $d \geq p$; we'll find a polynomial equivalent to x^d. For any integer, we know

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

In other words x^d is equivalent to the polynomial $x^{d-(p-1)}$. If $d-(p-1) \geq q$, 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 know it must be equivalent to $f(x)$ because f also passes through the same p points.

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?

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 $0 \le k \le i$, 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.