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 $9^{-1} \pmod{(5-1)(11-1)} = 9^{-1} \pmod{40}$. Find inverse of $e \pmod{(5-1)(11-1)} = 40$. Compute $\text{egcd}(40, 9)$:

$$\text{egcd}(40, 9) = \text{egcd}(9, 4)$$

$$= \text{egcd}(4, 1)$$

$$1 = 9 - 2(4).$$

$$1 = 9 - 2(40 - 4(9))$$

$$= 9 - 2(40) + 8(9) = 9(9) - 2(40).$$

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 $D(m) \equiv m^d \equiv 4^9 \equiv 14 \pmod{55}$. 49 \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 $x^e \pmod{N}$. 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 ≡ e−1 (mod 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 ≡ x (mod p) for all x ∈ {0, 1, ..., N − 1}.

**Proof:** By construction of d, we know that ed ≡ 1 (mod 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 ≡ 0 (mod p).
- x is not a multiple of p: Then
  \[
  x^{ed} \equiv x^{k(p−1)+1} \pmod{p}
  \]
  \[
  \equiv x^{k(p−1)}x \pmod{p}
  \]
  \[
  \equiv 1^k x \pmod{p}
  \]
  \[
  \equiv x \pmod{p}
  \]

, 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 ≡ e−1 (mod 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 (mod (p−1)(q−1)(r−1)). People who wish to send me a secret, x, send y = x^e (mod N). We decrypt an incoming message, y, by calculating y^d (mod N).

Does this work? We prove that x^ed − x ≡ 0 (mod N), and thus x^ed = x (mod N).

To prove that x^ed − x ≡ 0 (mod 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 ≡ 1 (mod (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 ≡ 0 (mod 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 Secret Sharing

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

Design a Secret Sharing scheme to make this work.

**Solution:**

**Solution 1** We can use a degree 2 polynomial, which is uniquely determined by 3 points. Evaluate the polynomial at 7 points, and distribute a point to each Reader and 2 points to each TA. 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 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.

**Solution 2** We construct three polynomials, one for each way of recovering the answer key:

- A degree 1 polynomial for recovering with two TAs, evaluated at 2 points. Distribute a point to each TA.
- A degree 2 polynomial for recovering with three readers, evaluated at 3 points. Distribute a point to each Reader.
- A degree 1 polynomial for recovering with one TA + one reader. Evaluate this polynomial at 2 points, and distribute one point to all TAs and one point to all readers.

All combinations can then use the corresponding polynomial to recover the answer key.
4 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.

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, 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 four hobbits agreeing to use the ring is not enough to know the instructions. One human and three hobbits is not enough. However, all four hobbits and one human agreeing is enough. Both humans 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 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 \( P_{\text{humans}}(x) \). Suppose \( P_{\text{humans}}(x) = 2x + 2 \).

Then the first human receives \( P_{\text{humans}}(1) = 4 \) and the second receives \( P_{\text{humans}}(2) = 4 + 2 = 6 \equiv 1 \). When they interpolate using these values, they will discover the original polynomial and therefore \( P_{\text{humans}}(0) = U = 2 \). The hobbits will have a similar secret but with a degree-3 polynomial (e.g. \( P_{\text{hobbit}}(x) = 4x^3 + x^2 + 2 \)).

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.

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 \((x_0, y_0), \ldots, (x_i, y_i)\) 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 \( k\)th 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 \( \delta \)s, you don’t have to recalculate those, so you can skip most of the work.

6 Equivalent Polynomials

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

(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 \( \text{GF}(5) \); then find a polynomial with degree strictly less than 11 that is equivalent to \( g(x) = 1 + 3x^{11} + 7x^{13} \) over \( \text{GF}(11) \).

(b) Prove that whenever \( f(x) \) has degree \( \geq q \), it is equivalent to some polynomial \( \tilde{f}(x) \) with degree < \( q \).

Solution:

(a) Fermat’s Little Theorem says that for any nonzero integer \( a \) and any prime number \( q \), \( a^{q-1} \equiv 1 \mod q \). We’re allowed to multiply through by \( a \), so the theorem is equivalent to saying that \( a^q \equiv a \mod q \); note that this is true even when \( a = 0 \), since in that case we just have \( 0^q \equiv 0 \mod q \). 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 \( g(x) = 1 + 3x^{11} + 7x^{13} \mod 11 \): set \( \tilde{g}(x) = 1 + 3x + 7x^3 \).
(b) One proof uses Fermat’s Little Theorem. As a warm-up, let $d \geq q$; we’ll find a polynomial equivalent to $x^d$. For any integer, we know

\[
a^d = a^{d-q}a^q \\
\equiv a^{d-q}a \mod q \\
\equiv a^{d-q+1} \mod q.
\]

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

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

7 The CRT and Lagrange Interpolation

Let $n_1, \ldots, n_k$ be pairwise co-prime, i.e. $n_i$ and $n_j$ are co-prime for all $i \neq j$. The Chinese Remainder Theorem (CRT) tells us that there exist solutions to the following system of congruences:

\[
x \equiv a_1 \pmod{n_1} \tag{1} \\
x \equiv a_2 \pmod{n_2} \tag{2} \\
\vdots \\
x \equiv a_k \pmod{n_k} \tag{k}
\]

and all solutions are equivalent $(\mod n_1n_2\cdots n_k)$. For this problem, parts (a)-(c) will walk us through a proof of the Chinese Remainder Theorem. We will then use the CRT to revisit Lagrange interpolation.

(a) We start by proving the $k = 2$ case: Prove that we can always find an integer $x_1$ that solves (1) and (2) with $a_1 = 1, a_2 = 0$. Similarly, prove that we can always find an integer $x_2$ that solves (1) and (2) with $a_1 = 0, a_2 = 1$.

(b) Use part (a) to prove that we can always find at least one solution to (1) and (2) for any $a_1, a_2$. Furthermore, prove that all possible solutions are equivalent $(\mod n_1n_2)$.

(c) Now we can tackle the case of arbitrary $k$: Use part (b) to prove that there exists a solution $x$ to (1)-(k) and that this solution is unique $(\mod n_1n_2\cdots n_k)$.

(d) For polynomials $p_1(x), p_2(x)$ and $q(x)$ we say that $p_1(x) \equiv p_2(x) \mod q(x)$ if $p_1(x) - p_2(x)$ is of the form $q(x) \times m(x)$ for some polynomial $m(x)$.
Define the polynomials \(x - a\) and \(x - b\) to be co-prime if they have no common divisor of degree 1. Assuming that the CRT still holds when replacing \(x, a_i\) and \(n_i\) with polynomials (using the definition of co-prime polynomials just given), show that the system of congruences

\[
\begin{align*}
p(x) &\equiv y_1 \pmod{(x - x_1)} \quad (1') \\
p(x) &\equiv y_2 \pmod{(x - x_2)} \quad (2') \\
&\vdots \\
p(x) &\equiv y_k \pmod{(x - x_k)} \quad (k')
\end{align*}
\]

has a unique solution \(\pmod{(x - x_1) \cdots (x - x_k)}\) whenever the \(x_i\) are pairwise distinct. What is the connection to Lagrange interpolation?

Hint: To show that a unique solution exists, you may use the fact that the CRT has a unique solution when certain properties are satisfied.

**Solution:**

(a) Since \(\gcd(n_1, n_2) = 1\), there exist integers \(k_1, k_2\) such that \(1 = k_1n_1 + k_2n_2\). Setting \(x_1 = k_2n_2 = 1 - k_1n_1\) and \(x_2 = k_1n_1 = 1 - k_2n_2\) we obtain the two desired solutions.

(b) Using the \(x_1\) and \(x_2\) we found in Part (a), we show that \(a_1x_1 + a_2x_2 \pmod{n_1n_2}\) is a solution to the desired equivalences:

\[
\begin{align*}
 a_1x_1 + a_2x_2 &\equiv a_1 \cdot 1 + a_2 \cdot 0 \equiv a_1 \pmod{n_1} \\
 a_1x_1 + a_2x_2 &\equiv a_1 \cdot 0 + a_2 \cdot 1 \equiv a_2 \pmod{n_2}.
\end{align*}
\]

Such result is also unique. Say that we have two difference solutions \(x = c\) and \(x = c'\), which both satisfy \(x \equiv a_1 \pmod{n_1}\) and \(x \equiv a_2 \pmod{n_2}\). This would give us \(c \equiv c' \pmod{n_1}\) and \(c \equiv c' \pmod{n_2}\), which suggests that \((c - c')\) is divisible by \(n_1\) and \(n_2\). Since \(n_1\) and \(n_2\) are coprime, \(\gcd(n_1, n_2) = 1\), \((c - c')\) is divisible by \(n_1n_2\). Writing it in modular form gives us \(c \equiv c' \pmod{n_1n_2}\). Therefore, all the result is unique with respect to \(\pmod{n_1n_2}\).

(c) We use induction on \(k\). Part (b) handles the base case, \(k = 2\). For the inductive hypothesis, assume for \(k \leq l\), the system \((1)-(k)\) has a unique solution \(a \pmod{n_1 \cdots n_k}\). Now consider \(k = l + 1\), so we add the equation \(x \equiv a_{l+1} \pmod{n_{l+1}}\) to our system, resulting in

\[
\begin{align*}
x &\equiv a \pmod{n_1 \cdots n_l} \\
x &\equiv a_{l+1} \pmod{n_{l+1}}.
\end{align*}
\]

Since the \(n_i\) are pairwise coprime, \(n_1n_2 \cdots n_l\) and \(n_{l+1}\) are coprime. Part (b) tells us that there exists a unique solution \(a' \pmod{n_1 \cdots n_{l+1}}\). We conclude that \(a'\) is the unique solution to \((1)-(l+1)\), when taken \(\pmod{n_1n_2 \cdots n_{l+1}}\).

(d) We only need to check that \(q_i(x) = (x - x_i)\) and \(q_j(x) = (x - x_j)\) are coprime whenever \(x_i \neq x_j\); that is, that they don’t share a common divisor of degree 1. If \(d_i(x) = a_ix + b_i\) is a divisor of
$q_i(x)$, then $q_i(x) = q'(x)(a_i x + b_i)$ for some polynomial $q'(x)$. But since $q_i(x)$ is of degree 1, $q'(x)$ must be of degree 0 and hence a constant, so $d_i(x)$ must be a constant multiple of $q_i(x)$. Similarly, any degree 1 divisor $d_j$ of $q_j(x)$ must be a constant multiple of $q_j(x)$, and if $x_i \neq x_j$, then none of these multiples overlap, so $q_i(x)$ and $q_j(x)$ are coprime.

From our result in part (d), the congruences $(1')-(k')$ assert that we are looking for a polynomial $p(x)$ such that $p(x_i) = y_i$. The CRT then establishes the existence of $p(x)$, and that it is unique modulo a degree $k$ polynomial. That is, $p(x)$ is unique if its degree is at most $k - 1$. Lagrange interpolation finds $p(x)$.