AN ALGEBRAIC PROOF OF RSA ENCRYPTION AND DECRYPTION

Recall that RSA works as follows. A wants B to communicate with A, but without E understanding the transmitted message. To do so:

- A broadcasts "RSA method, encryption exponent e, modulus N," where $N = pq$, p and q are large primes, and $\gcd(e, \phi(N)) = 1$. (Here, $\phi(N)$ indicates the number of integers between 0 and N that are relatively prime to N.)
- B encrypts a message m by computing $c = m^e$, and broadcasts c.
- A decrypts c by computing $c^d = (m^e)^d$, modulo N. (Here, d is the Bézout coefficient of e in the linear combination $ed + t\phi(N) = 1$.)

So RSA successfully encrypts and decrupts if $m^{ed} \equiv m \pmod{N}$. To show this, we proceed through several claims.

Definition. Let $\mathbb{Z}_n^*$ be the subset of $\mathbb{Z}_n$ whose elements are relatively prime to n.

Example. $\mathbb{Z}_{35}^* = \{1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34\}$. Observe that $\phi(N) = 24 = (5-1) \times (7-1)$, where $35 = 5 \times 7$.

Claim 1. Every $a \in \mathbb{Z}_n^*$ has a multiplicative inverse $s \in \mathbb{Z}_n^*$; that is, $as \equiv 1 \pmod{n}$.

Proof. Let $a \in \mathbb{Z}_n^*$. By Theorem 1.35 in the text, there exist $s, t \in \mathbb{Z}$ such that $as + nt = 1$. Rewrite as $n(-t) = as - 1$. By definition of divisibility, $n \mid (as - 1)$. By definition of congruence, $as \equiv 1 \pmod{n}$. That is, s is a multiplicative inverse of a. In addition, the linear combination $as + nt = 1$ shows that $\gcd(s, n) = 1$, so $s \in \mathbb{Z}_n^*$, as claimed. $\square$

Example (continued). It is easy to verify that the multiplicative inverse of 18 in $\mathbb{Z}_{35}^*$ is 2.

Claim 2. For every $a \in \mathbb{Z}_n^*$, the set $S = \{ab : b \in \mathbb{Z}_n^*\}$ has $\phi(n)$ distinct elements. In fact, $S = \mathbb{Z}_n^*$.

Proof. Let $a \in \mathbb{Z}_n^*$ and compute S. For each $b \in \mathbb{Z}_n^*$, we have $\gcd(a, n) = \gcd(b, n) = 1$; by Exercise 1 below, $\gcd(ab, n) = 1$. Hence each $ab \in S$ is also an element of $\mathbb{Z}_n^*$, and $S \subseteq \mathbb{Z}_n^*$. Since $\mathbb{Z}_n^*$ has $\phi(n)$ elements, the only way S can have fewer is if $ab = ac$ for distinct $b, c \in \mathbb{Z}_n^*$. By way of contradiction, assume that such b and c exist. By Claim 1, a has a multiplicative inverse $s \in \mathbb{Z}_n^*$. Multiply both sides of our congruence by s, and we see that

$$s(ab) \equiv s(ac) \quad \Longrightarrow \quad (sa)b = (sa)c \quad \Longrightarrow \quad 1 \cdot b \equiv 1 \cdot c \quad \Longrightarrow \quad b \equiv c\,.$$

However, we chose $b, c \in \mathbb{Z}_n^*$ to be distinct, so we have a contradiction. It must be that S has $\phi(n)$ distinct elements, and since we knew $S \subseteq \mathbb{Z}_n^*$ we actually have $S = \mathbb{Z}_n^*$. $\square$

Example (continued). Let $a = 13$. Then the set S of Claim 2 is

$$S = \{13, 26, 4, 17, 8, 34, 12, 3, 16, 29, 33, 11, 24, 2, 6, 19, 32, 23, 1, 27, 18, 31, 9, 22\}\ .$$

This is precisely $\mathbb{Z}_{35}^*$.

Claim 3. For every $a \in \mathbb{Z}_n^*$, there is some $k \in \mathbb{N}^+$ such that $a^k \equiv 1 \pmod n$, and for the smallest such k there are k distinct powers of a, modulo n.

Proof. Let $a \in \mathbb{Z}_n^*$ and let $T = \{a, a^2, a^3, \ldots\}$. By Exercise 2 below, for each a^k we have $\gcd\left(a^k, n\right) = 1$. Each $a^k \in T$ is thus an element of $\mathbb{Z}_n^*$, so $T \subseteq \mathbb{Z}_n^*$. Now, $\mathbb{Z}_n^*$ is a finite set; to be precise, it has $\phi(n)$ elements. That forces T to be a finite set; there must be distinct $i, j \in \mathbb{N}$ such that $a^i \equiv a^j \pmod n$. Without loss of generality, $i < k$. Since $a^i \in \mathbb{Z}_n^*$, Claim 1 tells us it has a multiplicative inverse $b \in \mathbb{Z}_n^*$. Multiply both sides of the congruence by b, we see that

$$a^i b \equiv a^j b \quad \Longrightarrow \quad a^i b \equiv \left(a^{j-i} \cdot a^i\right) b \quad \Longrightarrow \quad a^i b \equiv a^{j-i}\left(a^i b\right) \quad \Longrightarrow \quad 1 \equiv a^{j-i}\,.$$

Recall that $i < j$, so $j - i \in \mathbb{N}^+$ and $k = j - i$ satisfies $a^k \equiv 1$.

By the Well-Ordering Property, we can identify a smallest positive k such that $a^k \equiv 1$. To show that there are k distinct powers of a, modulo n, suppose that $a^i \equiv a^j$, where $0 < i \leq j \leq k$. As before, $1 \equiv a^{j-i}$. We chose k to be the smallest positive integer such that $a^k \equiv 1$, and $j - i < k$, so $j - i$ cannot be positive. Instead, $j - i = 0$, which means $i = j$. In other words, $a^i \equiv a^j$ only if $i = j$. So the powers a, a^2, … a^k must all be distinct. □

Corollary. *For any $a \in \mathbb{Z}_{35}^*$, a's inverse is a power of itself.*

Example (continued)**.** Let $a = 13$. The set T computed in the proof of Claim 3 is

$$T = \{13, 29, 27, 1\}\ .$$

So $a^4 \equiv 1$. Notice that $|T| = 4$, a divisor of $\phi(35)$. Also, $13^3 \equiv 27$ is the multiplicative inverse of 13.

Let's do another. Let $a = 26$. The set T computed in the proof of Claim 3 is

$$T = \{26, 11, 6, 16, 31, 1\}\ .$$

So $a^6 \equiv 1$. Again, we notice that $|T| = 6$, a divisor of $\phi(35)$. Also, $26^5 \equiv 31$ is the multiplicative inverse of 26.

Notice that if $26^2 \equiv 26^4$, then we would have $1 \equiv 26^2$, but we already saw that $k = 6$ is the smallest positive number such that $26^k \equiv 1$.

Claim 4. For every $a \in \mathbb{Z}_n^*$, the number of distinct powers of a in $\mathbb{Z}_n^*$ is a divisor of $\phi(n)$.

Proof. Let a, k, and T be as in the proof of Claim 3. Define $U_1, U_2, \ldots$ iteratively as follows:

- $U_1 = T$, and
- for $i = 1, 2, \ldots$,
  - if $U_1 \cup \cdots \cup U_i = \mathbb{Z}_n^*$, then stop;
  - otherwise, choose $b_i \in \mathbb{Z}_n^*$ that is not in $U_1 \cup \cdots \cup U_i$, and let $U_{i+1} = \left\{ab_i, a^2 b_i, \ldots, a^k b_i\right\}$.

We proceed through several subclaims.

Subclaim 1. The sequence of U_i's is finite.

Subproof. Each U_{i+1} is defined using an element of $\mathbb{Z}_n^* \backslash (U_1 \cup \cdots U_i)$. As $\mathbb{Z}_n^*$ has finitely many elements, we can create a new set with an element not already taken only finitely many times.

Let U_{last} be the last one generated.

Subclaim 2. $\mathbb{Z}_n^* = U_1 \cup \cdots U_{\text{last}}$.

Subproof. Were this not the case, the iteration would continue beyond U_{last}.

Subclaim 3. If $i \neq j$, then $U_i \cap U_j = \emptyset$.

Subproof. By way of contradiction, assume $i \neq j$ and $U_i \cap U_j \neq \emptyset$. Let $c \in U_i \cap U_j$. By construction, there exist $b_{i-1}, b_{j-1} \in \mathbb{Z}_n^*$ and $\ell, m \in \mathbb{N}^+$ such that $c \equiv a^\ell b_{i-1} \equiv a^m b_{j-1}$. Without loss of generality, suppose $i < j$. By construction of the U's, we cannot have $b_{j-1} \in U_i$, as that would contradict the choice of b_{j-1}, which cannot be in $U_1 \cup \cdots \cup U_{j-1}$, and U_i would be among them. However, $b_{j-1} \equiv a^{\ell-m} b_{i-1}$. If $\ell - m \geq 0$, then $b_{j-1} \in U_i$, a contradiction, so we must have $\ell - m < 0$. By Exercise 3 below, we know that $b_{j-1} \equiv a^{k+(\ell-m)} b_{i-1}$. In this case $k + (\ell - m) > 0$, and again $b_{j-1} \in U_i$, a contradiction. Hence $U_i \cap U_j = \emptyset$.

Subclaim 4. For each $i = 1, 2, \ldots$ we have $|U_i| = |T|$.

Subproof. For $U_1 = T$ this is true by definition. Any other U_i is constructed by multiplying $a^j b_{i-1}$ for some $b_{i-1} \in \mathbb{Z}_n^*$ and some $j = 1, 2, \ldots, k$. By Claim 2, $a^j b_{i-1} \neq a^\ell b_{i-1}$ if $1 \leq j, \ell \leq k$ and $j \neq \ell$. □

Subclaim 2 tells us that the elements of $\mathbb{Z}_n^*$ are all contained among the U's, which by Subclaim 3 have no common elements, and by Subclaim 4 are the same size. This is the basic model of division, so each $|U_i|$ divides $|\mathbb{Z}_n^*|$. In particular $|T| = |U_1|$ divides $|\mathbb{Z}_n^*| = \phi(n)$, and $|T|$ is the number of distinct powers of a. □

Example (continued)**.** Earlier we showed that in $\mathbb{Z}_{35}^*$, with $a = 13$ we have $U_1 = T = \{13, 29, 27, 1\}$. Clearly $\mathbb{Z}_{35}^* \neq U_1$; let $b_1 = 2 \in \mathbb{Z}_{35}^* \setminus U_1$. Then

$$U_2 = \{13 \times 2, 29 \times 2, 27 \times 1, 1 \times 2\} = \{26, 3, 34, 2\} \ .$$

Notice that $U_1 \cap U_2 = \emptyset$. Again, $Z_{35}^* \neq U_1 \cup U_2$; let $b_2 = 3 \in \mathbb{Z}_{35}^* \setminus (U_1 \cup U_2)$. Then

$$U_3 = \{13 \times 3, 29 \times 3, 27 \times 3, 1 \times 3\} = \{4, 17, 11, 3\} \ .$$

Notice that $U_1 \cap U_3 = U_2 \cap U_3 = \emptyset$. Again, $Z_{35}^* \neq U_1 \cup U_2 \cup U_3$; let $b_3 = 6 \in \mathbb{Z}_{35}^* \setminus (U_1 \cup U_2 \cup U_3)$. Then

$$U_4 = \{13 \times 6, 29 \times 6, 27 \times 6, 1 \times 6\} = \{8, 34, 22, 6\} \ .$$

Notice that $U_1 \cap U_4 = U_2 \cap U_4 = U_3 \cap U_4 = \emptyset$. Again, $Z_{35}^* \neq U_1 \cup U_2 \cup U_3 \cup U_4$; continuing in this fashion, we choose and construct

$$b_4 = 9 \text{ and } U_5 = \{12, 16, 33, 9\}$$
$$b_5 = 18 \text{ and } U_6 = \{24, 32, 31, 18\} \ .$$

The iteration has ended, illustrating Subclaim 1. We have $\mathbb{Z}_{35}^* = U_1 \cup \cdots \cup U_6$, illustrating Subclaim 2. The U's are disjoint, illustrating Subclaim 3. ("Disjoint" means their intersection is empty.) The U's all have $|T| = 4$ elements, illustrating Subclaim 4. In fact,

$$\phi(35) = 24 = 6 \times 4 = (\text{number of } U\text{'s}) \times |T| \ .$$

Claim 5 (Euler's Theorem)**.** For any $a \in \mathbb{Z}_n^*$, $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof. By Claim 3, there is some $k \in \mathbb{N}^+$ such that $a^k \equiv 1 \pmod{n}$, and the smallest such k is the number of distinct powers of a in $\{a, a^2, \ldots\}$. By Claim 4, $k \mid \phi(n)$. Choose $q \in \mathbb{N}$ such that $kq = \phi(n)$. By substitution,

$$a^{\phi(n)} = a^{kq} = \left(a^k\right)^q \equiv 1^q = 1 \ .$$

□

Example (continued)**.** Previously we saw that $13^4 \equiv 1 \pmod{35}$. Since $4 \times 6 = 24$,

$$13^{\phi(35)} = 13^{24} = 13^{4\times 6} = \left(13^4\right)^6 \equiv 1^6 = 1 \ .$$

Claim 6. The final step of the RSA algorithm deciphers B's message.

Proof. As explained at the beginning, we need to show that $m^{ed} \equiv m \pmod{N}$. By construction, $ed + t\phi(N) = 1$. Without loss of generality, we may assume d is positive and t is negative. Rewrite the equation as $ed = 1 - t\phi(N)$. Let $u = -t > 0$ and we have $ed = 1 + u\phi(N)$. By substitution into the congruence,

$$m^{ed} = m^{1+u\phi(N)} = m^1 \times m^{u\phi(N)} = m \times \left(m^{\phi(N)}\right)^u = m \times 1^u = m \ .$$

□

Example. This time we encrypt and decrypt the word DOGS a little more realistically.

Pair the word's letters as DO and GS. Transform DO into the number $3 \times 26 + 14 = 92$ and transform GS into the number $6 \times 26 + 18 = 174$. Let

$$p = 23 \text{ and } q = 31 \qquad \Longrightarrow \qquad N = pq = 713 \quad \text{and} \quad \phi(N) = (23-1) \times (31-1) = 660 \ .$$

Choose $e = 511$; it is easy to verify that $\gcd(511, 660) = 1$ via the Euclidean algorithm. The encryption is then

$$\begin{aligned} \text{DO: } 92^{511} &\equiv 92^{1+2+4+8+16+32+64+128+256} \equiv 92 \\ \text{GS: } 174^{511} &\equiv 50 \ . \end{aligned}$$

B thus broadcasts 92 and 50 to A.

To decrypt, A determines the decryption exponent $d = 31$ using the Euclidean algorithm, then computes

$$\begin{aligned} 92^{31} &\equiv 92 \\ 50^{31} &\equiv 174 \ . \end{aligned}$$

A then transforms the numbers back into letters by dividing by 26:

$$\begin{aligned} 92 &= 3 \times 26 + 14 \\ 174 &= 6 \times 26 + 18 \ . \end{aligned}$$

Observe that $3, 14, 6, 18$ are precisely the numbers corresponding to D, O, G, S.

Exercises

Exercise 1. Show that if $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$, then $\gcd(ab, n) = 1$.

Exercise 2. Show that if $\gcd(a, n) = 1$, then $\gcd\left(a^k, n\right) = 1$.

Exercise 3. Show that if $T = \left\{a, a^2, \ldots, a^k\right\}$ is a complete list of distinct powers of a modulo n, then $x \equiv a^k x \pmod{n}$.

Exercise 4. For $\mathbb{Z}_{35}^*$ and $a = 13$ compute the sets $U_1, U_2, \ldots\ U_{\text{last}}$ of Claim 4.

Exercise 5. Use the Euclidean algorithm to verify that 31 is the decryption exponent for $N = 713$ and $e = 511$.