RSA w/ Abstract Algebra

Rodolfo Lopez

May 2022

1 Introduction

The RSA algorithm was formally constructed in 1978 by MIT professors Ron Rivest, Adi Shamir, and Len Adleman (hence the acronym RSA), replacing the current, less secure National Bureau of Standards (NBS) algorithm. Their work was largely motivated by the work of the famous mathematician Leonard Euler who lived in the 18th century and also by the work of Stanford professors Diffie and Hellman who envisioned an asymmetric cryptosystem a year prior, in which each user is generated a public and private key to encode and decode some message. The key idea behind RSA is simply that it is easy to multiply two very large prime numbers but it is hard to factor that product for those two primes. There exists efficient computer algorithms to generate two very large prime numbers (say 100 digits long) as well as to multiply them together (product would be 200 digits long). However, there do not exist computer algorithms that efficiently factor that large product for those two large prime numbers. We will begin by first discussing in general terms how an asymmetric crpytosytem works. Then, we will look specifically at how the RSA algorithm works, in relation to abstract algebra.

2 Asymmetric Cryptosystem

Each user in some domain is given a unique public key function called E (for Encode) and a private key function called D (for Decode). Each user can send a message call it M to any other user in the domain. E also acts as a public address for each user in the domain.

2.1 One-Way Trapdoor Permutation

1) D and E should be inverses in order to work. It follows that, $D(E(M)) = M$ and $E(D(M)) = M$.
2) E and D should compute easily in order to be practical.
3) D should not be easily derived from E in order to be secure.

These three facts above demonstrate why E can be referred to as a one-way trapdoor permutation. One-way because it is easy to encode but hard to decode. Trying to find an M to satisfy $E(M) = C$ where C is called the cipher-text in order to guess D is unreasonable. However, via trapdoors the inverse of E, which is D, is easy to find. Lastly, E acts as a permutation since there is a bijection from M to itself. That is, every C is a potential M and every M is a potential C.

2.2 Example w/ Sender and Receiver

Consider both Rivest and Adleman (sorry Shamir) and that Rivest wants to send a message M to Adleman.

Then, we have E_R, E_A as the public encoding functions for Rivest and Adleman, respectively and D_R, D_A as the private decoding functions for Rivest and Adleman, respectively.

Rivest encodes the message M by $E_A(M) = C$ where E_A was found publicly acting as Adleman's address. Also, Adleman could respond to the message using Rivest's public address E_R.

However, now consider $D_R(M) = S$ where S is called the signature, specifically Rivest's signature. Here, S is private to Rivest.

If Rivest wants to send a message to Adleman, then he first must encode his signature using Alderman's address. $E_A(S) = E_A(D_R(M))$, the sender Rivest encodes the message using his private key, which becomes his digital signature

Thus, Adleman, the receiver, could authenticate that the message actually came from Rivest as well as deduce the message that was sent. $D_A(E_A(D_R(M))) = S$, so the sender Rivest is authenticated and $E_R(S) = E_R(D_R(M)) = M$, so the message from Rivest is deduced correctly.

Note that M cannot be forged or modified by anyone, or else $D_R(M') = S'$. However, Adleman does not know how to easily compute D_R and this would result in a different signature S'.

3 RSA

We will first cover the procedure used to generate the public and private keys. Then, we will show why it works.

3.1 Algorithm

1) Take two large prime numbers p and q.
2) Compute $n = pq$
3) Compute $\phi(n) = (p-1)(q-1)$.
4) Take e such that $gcd(e, \phi(n)) = 1$ where $1 < e < \phi(n)$.
5) Take d such that $edmod(\phi(n)) = 1$.

Encode with $C \equiv M^e(modn)$ and Decode with $M \equiv C^d(modn)$ where the Public key is (e, n) and the Private Key is (d, n). Note that $0 < M < n = pq$.

3.2 Proof

Let e, d, n be positive integers where (e, n) is the public encoding key and (d, n) is the private decoding key such that $n = pq$ where p and q are prime.

*Note that (e, n) and (d, n) should be subscripted since each user in the domain has their own unique pair of keys, however, we will work in general terms.

Also note that n is public but p and q are private to the receiver.

Let M be any integer from 0 to $n - 1$.

If the the message M is too long, then split the message and encode the pieces separately.

To encode, $C \equiv E(M) \equiv M^e(modn)$.

To decode, $M \equiv D(C) \equiv C^d(modn)$.

Now, the receiver still needs to choose a proper e and d.

Take d such that d is coprime to $(p-1)(q-1)$.

That is, $gcd(d, (p-1)(q-1)) = 1$.

Then, take e such that it is the multiplicative inverse of d.

That is, $ed \equiv 1(mod\phi(n))$.

Euler's Totient Function is defined as $\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_k})$ where $p_1, p_2, \dots, p_k$ are the unique primes dividing n. Also $\phi(1) = 1$.

This is precisely the set $(Z/n)^* = \{m \in N : 1 \leq m \leq n, gcd(m, n) = 1\}$.

We have, $(Z/n)^* \subset Z/n$ where Z/n is the set of integers mod n containing n elements. $(Z/n)^*$ is the set of units of Z/n, aka all elements have a multiplicative inverse. Equivalently, that is, all the numbers that are less than and coprime to n.

Now, we wish to show that Euler Totient Function is multiplicative for two prime numbers p and. q.

In other words, $\phi(n) = \phi(pq) = \phi(p)\phi(q)$ if $gcd(p, q) = 1$.

Consider $\phi : (Z/pq)^* \to (Z/p)^* \times (Z/q)^*$, $z \mapsto (x, y)$ where $z \in (Z/pq)^*$, $x \in (Z/p)^*$ and $y \in (Z/q)^*$

Define $\phi(z) = (zmodp, zmodq)$. Then ϕ is bijective since there exists an inverse ϕ^-1 that maps an ordered pair (x, y) to the unique solution $modpq$.

$z \equiv x(modp)$ and $z \equiv y(modq)$ from Chinese Remainder THM

Note that z is coprime to pq iff it is coprime to both p and q. So, ϕ is definitely a bijection.

We can conclude that $\phi(n) = \phi(pq) = \phi(p)\phi(q)$.

Now, for prime p, it follows that $\phi(p) = (p - 1)$ since all of the integers between 2 and $p - 1$ are coprime to p and $\phi(1) = 1$.

Since, d and $\phi(n)$ are coprime, d has a multiplicative inverse e in the set $Z/\phi(n)$.

This, would be essentially the same for the group $U(n)$ with multiplicative identity 1 and the ring $Z/\phi(n)$ with unity 1. Without going any deeper, $\phi(n)$ forms an ideal, that is a subring of the ring Z.

Recall that $ed \equiv 1(mod\phi(n))$. In other words, $ed = k\phi(n) + 1$ for some integer k.

To recap thus far, we have that

$$E(D(M)) \equiv (D(M))^e \equiv (M^d)^e(modn) = M^{ed}(modn) \equiv M^{k\phi(n)+1}(modn)$$

$$D(E(M)) \equiv (E(M))^d \equiv (M^e)^d(modn) = M^{ed}(modn) \equiv M^{k\phi(n)+1}(modn)$$

However, this should all obviously equal M.

For any M coprime to n, we have $M^{\phi(n)} \equiv 1modn$.

Since, $0 \leq M < n$, M would not be coprime to n iff M was either p or q.

That is, the chances of M happening to be p or q is extremely small, specifically of magnitude $2/n$.

So, M should most definitely be coprime to n.

Consider the congruence class of integers coprime to n, $(Z/n)^* = r_1, r_2, \ldots, r_{\phi(n)}$.

Thus, this set is reflexive, symmetric, and transitive with respect to multiplication (modn).

Suppose $M \in (Z/n)^*$. The we wish to show that multiplication by M simply permutes the set $\{Mr_1, Mr_2, \ldots, Mr_{\phi(n)}\} = (Z/n)^*$.

To look at a concrete example, consider the group $U(9)$ and let $M = 2$. Then, multiplication by 2 permutes $\{1, 2, 4, 5, 7, 8\}$ to $\{2, 4, 8, 1, 5, 7\}$. In this case, both sets are still equal and note that 5 is the inverse of 2 in $U(n)$.

Continuing the proof, we have that

$$r_1, r_2, \ldots, r_{\phi(n)} = (Mr_1)(Mr_2)\ldots(Mr_{\phi(n)})$$

$$r_1, r_2, \ldots, r_{\phi(n)} = M^{\phi(n)} r_1, r_2, \ldots, r_{\phi(n)}$$

$$1 = M^{\phi(n)}$$

The r_i's cancel since they are all have multiplicative inverses $(modn)$.

We could also show that M must be coprime to n using Lagrange's Theorem.

Recall that the set $(Z/n)^* = \{m \in N : 1 \leq m \leq n, gcd(m, n) = 1\}$ forms a group under multiplication with order $|(Z/n)^*| = \phi(n)$. This could also be referred to as the group $U(n)$.

The subgroup consisting of powers of M will have order $|M| = d$, where d is the multiplicative order of that element M. In other words, the subgroup generated by $< M >= \{1, M, M^2, \ldots, M^{d-1}\}$.

Thus, $d|\phi(n)$, we can say $dk = \phi(n)$ for some integer k by Lagrange's THM.

Because, $M^d \equiv 1(modn)$, we finally have that, $M^{\phi(n)} \equiv M^{dk} \equiv (M^d)^k \equiv 1^k \equiv 1(modn)$.

To conclude, $M^{ed} \equiv M^{k\phi(n)+1} \equiv (M^{\phi(n)})^k M \equiv 1^k M(modn) = M$

This works $\forall M$. Thus, E and D are inverse permutations acting on the finite set M where $0 < M < n = pq$.

4 References

The Chinese Remainder Theorem - University of California, Berkeley. https://math.berkeley.edu/ kmill/math55sp17/crt.pdf.

Gallian, Joseph A. "Ch. 8 External Direct Products." Contemporary Abstract Algebra, Cengage Learning, Australia ; Brazil ; Mexico ; Singapore ; United Kingdom ; United States, 2017.

The RSA Algorithm - University of Washington. https://sites.math.washington.edu/ morrow/336_09/*papers*/*Yevgeny.pdf*.