RSA for Programmers

Andrew DeLapo

June 2018

Introduction

RSA is named after its inventors, whose last names are Rivest, Shamir, and Adleman.

RSA is a public-key cryptosystem, which means each person involved is given a public key with which they send and receive messages.

RSA Encryption: The Big Picture

Bob wants to send Alice a secret message without the eavesdropper Eva being able to decode the message. Alice gives her public key (which everyone knows) to Bob.

Bob encrypts the message using Alice's public key, and sends it to Alice. Alice can use her private key (which only she knows) to decrypt the message.

Even if Eva is able to get Alice's public key and the encrypted message, she cannot decrypt the message without Alice's private key!

Some Math: Primes and Coprimality

A **prime number** is a number which has no integer factors (divisors) besides 1 and itself. For example, 7 and 13 are prime, but 24 is not prime. Also, 1 is not considered to be prime.

We say that two integers a and b are **coprime** (or **relatively prime**) if they share no common factors besides 1. For example, 9 and 16 are **coprime** since the factors of 9 are 1, 3, and 9, and the factors of 16 are 1, 2, 4, and 8. Another way of showing two numbers are coprime is to show that $\gcd(a, b) = 1$.

Some Math: Modular Arithmetic

Recall the "modulus" operator, which divides two numbers and returns the remainder. For example you might code

$$5 \ \% \ 2 = 1$$
$$15 \ \% \ 3 = 0$$

However, in math, we would instead write

$$5 \equiv 1 \mod 2$$
$$15 \equiv 0 \mod 3$$

The "$\equiv$" sign means "equivalent" or "congruent."

More Modular Arithmetic

When talking about modular arithmetic, we usually only use non-negative integers. For some moduli, it is possible to still have multiplicative inverses. Namely, in prime moduli, all numbers (except 0) have multiplicative inverses. For example, consider 4 in mod 7. We have

$$4 \times 2 \equiv 1 \mod 7$$

which means the multiplicative inverse of 4 in mod 7 is 2. Even without decimals, we still have cool arithmetic properties!

RSA: Encryption

Choose two (typically large) prime numbers p and q. Then let $N = pq$. Choose a number e which is less than **and** coprime to $(p-1) \times (q-1)$. Alice's public key is (N, e).

To encrypt a number x (perhaps an ASCII character), Bob uses the encryption function E,

$$E(x) = x^e \mod N \tag{1}$$

RSA: Decryption

Alice's private key is d, which is the multiplicative inverse of e mod $(p-1)(q-1)$. Since the original prime numbers p and q were never sent to Bob or anyone else, this makes d very difficult for anyone but Alice to find.

To decrypt a received number x, use the decryption function D,

$$D(x) = x^d \mod N \tag{2}$$

RSA Example: Encryption

Bob wants to send the message "abc" to Alice.

Alice randomly chooses primes $p = 7727, q = 7919$. Then $N = pq = 61,190,113$. A value of e which is coprime to $(p-1)(q-1) = 61,174,468$ is $e = 17$. Therefore her public key is $(N, e) = (61\ 190\ 113, 17)$.

Bob converts his message to ASCII in hexadecimal, giving

$$61\ 62\ 63$$

Concatenating these numbers and converting to base 10 gives the number $x = 6,382,179$.

RSA Example: Encryption Continued

Bob proceeds to encrypt his message, $x = 6,382,179$.

$$\begin{aligned} E(6,382,179) &= 6,382,179^{17} \mod 61,190,113 \\ &= 48,809,364 \mod 61,190,113 \end{aligned}$$

He sends $48,809,364$ to Alice.

RSA Example: Decryption

Alice's private key is the modular inverse of $e = 17$ in mod $61,174,468$, which is $d = 28,787,985$. She has received Bob's message, $x = 48,809,364$, and decrypts it.

$$\begin{aligned} D(48,809,364) &= 48,809,364^{28,787,985} \mod 61,190,113 \\ &= 6,382,179 \mod 61,190,113 \end{aligned}$$

She converts $6,382,179$ to hexadecimal and gets 616263, which she converts from ASCII and finds Bob's original message, "abc".

Coding Challenges

- Create a function that returns random, large prime numbers.
- Create a function that converts text to hexadecimal ASCII.
- Create a function that finds the multiplicative inverse of a number in mod n.