1 Introduction

Recall that with the Diffie-Helman Protocol, at the end Alice and Bob share a string. But they have no control over this string. This is fine for some applications; however, we want a system where Bob can send Alice a message outright, not just a random string for later use. RSA (Rivest-Shamir-Adelman) is the first such publicly acknowledged protocol. Since this is Crypto there were earlier versions developed in secret.

2 The Law of Inclusion and Exclusion

If the Math Club has 10 people, and the Fashion Club has 9 people then how many people are there? You might think $10 + 9 = 19$. But there may be people in both that have been double counted. Let’s ask the question again but with more information.

If the Math Club has 10 people, and the Fashion Club has 9 people, and there are 3 people in both clubs, then how many people are there: $10 + 9 - 3 = 16$.

More generally, if $A$ and $B$ are sets then

$$|A \cup B| = |A| + |B| - |A \cap B|.$$ 

Here are some examples:

**Example 2.1** How many numbers between 1 and 91 are NOT relatively prime to 91?

Note that $91 = 13 \times 7$. Hence a number is not rel prime to 91 if it is a multiple of 7 or a multiple of 13.

Let $A$ be the set of numbers in $\{1, \ldots, 91\}$ that are multiples of 7. There are 13 of them:

$1 \times 7, 2 \times 7, \ldots, 13 \times 7$.

Let $B$ be the set of numbers in $\{1, \ldots, 91\}$ that are multiples of 13. There are 7 of them:

$1 \times 13, 2 \times 13, \ldots, 7 \times 13$.

What is $A \cap B$? How many numbers between 1 and 91 are multiples of both 7 and 13? Only 91. So there is 1 such number.

Hence the number of numbers in $\{1, \ldots, 91\}$ that are not rel prime to 91 is

$$13 + 7 - 1 = 19.$$
Example 2.2  Let $p, q$ be primes. How many numbers between 1 and $pq$ are NOT relatively prime to $pq$?

The numbers that are not rel prime to $pq$ are either multiples of $p$ or multiples of $q$. There are $q$ multiples of $p$ and there are $p$ multiples of $q$. How many are both? Just 1. Hence the number of numbers in $\{1, \ldots, pq\}$ that are not rel prime to $pq$ is

$$p + q - 1$$

So how many numbers in $\{1, \ldots, pq\}$ are rel prime to $pq$?

$$pq - (p + q - 1) = pq - p - q + 1 = (p - 1)(q - 1).$$

Definition 2.3  $\phi(n)$ is the number of elements of $\{1, \ldots, n\}$ that are rel prime to $n$. Above we showed that, if $p$ and $q$ are primes, then $\phi(pq) = (p - 1)(q - 1)$.

3 Some Number Theory that we will Need

We will need the following:

Theorem 3.1  For all $n$, for $1 \leq a \leq n - 1$, $a^{\phi(n)} \equiv 1 \pmod{n}$.

This makes doing arithmetic mod $n$ easier. If $m = L\phi(m) + L'$ then

$$a^m \pmod{n} \equiv a^{L\phi(m)+L'} \equiv (a^{\phi(m)})^L a^{L'} \equiv a^{L'} \pmod{n}$$

More succinctly

$$a^m \pmod{n} = a^m \pmod{\phi(n)} \pmod{n}$$

So if you have a very large exponent $m$ you can first mod it down mod $\phi(n)$ before doing the repeated squaring.

We will NOT prove Theorem 3.1; however, we will prove a subcase. If $p$ is prime then $\phi(p) = p - 1$. So in this case Theorem 3.1 is: for $1 \leq a \leq p - 1$, $a^{p-1} \equiv 1 \pmod{p}$. We actually prove something slightly stronger: for $0 \leq a \leq p - 1$, $a^p \equiv a \pmod{p}$.

We need a lemma.

Lemma 3.2  If $p$ is a prime and $2 \leq i \leq p - 1$ then $\binom{p}{i} \equiv 0 \pmod{p}$. 

2
Proof: The KEY is that \( \binom{p}{i} \) is an INTEGER. Written as this fraction it has a factor of \( p \) in the numerator and no factor of \( p \) in the denominator. Hence when all cancels out, that \( p \) remains. 

**Theorem 3.3** If \( p \) is prime and \( 0 \leq a \leq p - 1 \) then \( a^p \equiv a \pmod{p} \).

**Proof:** This proof is formally by induction; however, we'll just do the proof intuitively.

Fix \( p \). Let's look at \( a \)

If \( a = 0 \) then clearly \( a^0 \equiv 0 \pmod{p} \) since they are both 0.

If \( a = 1 \) then clearly \( 1^{p-1} = 1 \equiv 1 \pmod{p} \).

Let's look at \( a = 2 \)

\[
2^p \equiv (1 + 1)^p = 1 + \sum_{i=1}^{p-1} \binom{p}{i} 1^i + 1^p
\]

Every term in that summation has a factor of \( \binom{p}{i} \) in it. Note that by Lemma 3.2 all of these terms are \( \equiv 0 \pmod{p} \). Hence we get

\[
2^p \equiv (1 + 1)^p = 1 + \sum_{i=1}^{p-1} \binom{p}{i} 1^i + 1^p \equiv 1 + 1 \equiv 2 \pmod{p}.
\]

What about \( a = 3 \)?

\[
3^p \equiv (1 + 2)^p = 1 + \sum_{i=1}^{p-1} \binom{p}{i} 2^i + 2^p \equiv 1 + 2 \equiv 3 \pmod{p}.
\]

We can do this till the cows come home!

**4 RSA**

Alice will broadcast to everyone (including Bob and Eve) some numbers that will allow Bob to broadcast a message which seems hard for Eve to find— even though Alice and Bob had no secret communication. Let \( S \) be a security parameter. Alice will pick her numbers in the interval \([S, 2S]\). The larger the \( S \) is the more secure the system is.

1. Alice finds random primes \( p, q \in [S, 2S] \). Alice computes \( n = pq \). Alice finds a number \( d \in \{2, \ldots, (p - 1)(q - 1)\} \) that is relatively prime to \((p - 1)(q - 1)\). Alice privately finds \( e \) such that \( de \equiv 1 \pmod{(p - 1)(q - 1)} \). Alice broadcasts \((n, d)\).
2. Bob’s message is $m$. Bob sends $m^d \pmod{n}$.

3. Alice gets $m^d \pmod{n}$. Alice does $(m^d)^e \equiv m^{de} \pmod{n}$. Recall that $m^{de} \equiv m^{de} \pmod{(p-1)(q-1)} \equiv m \pmod{n}$. Hence Alice has $m$.

How hard is this for Alice and Bob?

Alice: Finding primes is easy, multiplying is easy, finding a $d$ rel prime to $(p-1)(q-1)$ is easy (you should think about that one), and finding $e$ such that $de \equiv 1 \pmod{(p-1)(q-1)}$ is easy. Once she gets the message from Bob, she does powering which is easy.

Bob: Bob just does powering which is easy.

Eve: She has $n$ but NOT $p,q$. She has $d$ but NOT $e$. If she could factor she would know $p,q$ and hence $(p-1)(q-1)$. She could then find $e$ such that $de \equiv 1 \pmod{(p-1)(q-1)}$. So IF Eve could factor fast then she could break RSA. The converse is NOT known. However, it is thought that RSA is hard to crack.

The version I give above is not secure for some technical reasons, but some variants of it are believed to be secure.