RSA Supplement 1

RSA Algorithm—Probability of a message not being in $Z_n^\times$

We note for $Z_n^\times$ not every $1 < m < n-1$ is in $Z_n^\times$ if n is not prime. So it seems that we can't just choose any m we want. But, consider what is the probability that a random $1 < m < n-1$ is in $Z_n^\times$, where $n = p \cdot q$? Well, that is the number of numbers, m, relatively prime to n where $1 < m < n-1$ divided by the number of integers where $1 < m < n-1$. We know this number: $\varphi(n) = (p-1)\cdot(q-1)$ and the number of numbers $1 < m < n-1$ is obviously $n-1 = p \cdot q - 1$. So the probability is

$$\frac{(p-1)\cdot(q-1)}{p\cdot q-1} = \frac{p\cdot q - q - p + 1}{p \cdot q - 1}$$

However, if p and q are large this is not a problem in practice:

$$\lim_{p\to\infty} \frac{p\cdot q - q - p + 1}{p\cdot q - 1} =$$
$$\lim_{p\to\infty} \frac{q - (q/p) - 1 + (1/p)}{q - 1/p} =$$
$$\lim_{p\to\infty} \frac{q+1}{q} = \lim_{p\to\infty} \frac{q}{q} = 1$$

The same argument holds for q. So, we only need to be concerned about the choice of m when we're working "toy" problems where p and q are not so large. Consider where p and q are of the same order say $\sim 2^{512}$. Then

$$\frac{p\cdot q - q - p + 1}{p\cdot q - 1} \approx \frac{2^{512}\cdot 2^{512} - 2^{512} - 2^{512} + 1}{2^{512}\cdot 2^{512} - 1} \approx \frac{2^{1024} - 2^{513}}{2^{1024}} = \frac{2^{513}\cdot\left(2^{511}-1\right)}{2^{513}\cdot 2^{511}} = \frac{2^{513}\cdot\left(2^{511}-1\right)}{2^{513}\cdot 2^{511}} = 1 - \frac{1}{2^{511}}$$

This is so close to 1 as to be completely immaterial. Obviously

$prob\left(m \notin Z_n^\times\right) = 1 - prob\left(m \in Z_n^\times\right) = 1 - \left(1 - \frac{1}{2^{511}}\right) = \frac{1}{2^{511}}$, which is a very small number, indeed—considering that a fair estimate of the number of atoms in the universe is on the order of 2^{262}.

Another way of considering this problem is to calculate the probability that a number is not that a random $1 < m < n-1$ is in not $Z_n^\times$:

$$\frac{(n-1)-\varphi(n)}{n-1} = \frac{(pq-1)-((p-1)\cdot(q-1))}{pq-1} = \frac{pq-1-pq+p+q-1}{pq-1} = \frac{p+q-2}{pq-1}$$

We can obtain the same result in two other ways. First, by counting the number of integers that are not relatively prime to $p \cdot q$. This is easy. The only integers that are not relatively prime to $p \cdot q$ are multiples of p and multiples of q:

$$\begin{aligned}
&\gcd(pq, p) = p \\
&\gcd(pq, 2p) = p \\
&\gcd(pq, 3p) = p \\
&\vdots \\
&\gcd(pq, (q-1)p) = p
\end{aligned}$$

and

$$\begin{aligned}
&\gcd(pq, q) = q \\
&\gcd(pq, 2q) = q \\
&\gcd(pq, 3q) = q \\
&\vdots \\
&\gcd(pq, (p-1)q) = q
\end{aligned}$$

Obviously, there are $q-1$ of the former and $p-1$ of the latter. So,

$$\frac{(p-q)+(q-1)}{pq-1} = \frac{p+q-2}{pq-1}$$

which is consistent with our previous result.

Alternatively, by inclusion-exclusion principle, the number of integers not relatively prime to $n = p \cdot q$ is

$$\frac{1}{p}+\frac{1}{q}-\frac{1}{pq} = \frac{q}{pq}+\frac{p}{pq}-\frac{1}{pq} = \frac{p+q-1}{pq}$$

But this number includes $n = p \cdot q$ and we only are concerned with numbers $x < n = p \cdot q$, so we subtract 1 from both the numerator and denominator. This leads to the same result:

$$\frac{(p+q-1)-1}{pq-1} = \frac{p+q-2}{pq-1}$$

Probably the simplest way of thinking about this is that the only numbers $1 < m < n-1$ that are not relatively prime to n are those that have a common divisor with p or with q, since $n = p \cdot q$. Which numbers have a common divisor with p?

$$p, 2p, 3p, 4p, 5p, \cdots, qp = n$$

There are obviously q of these numbers. So, the probability of a random m being one of these numbers is $q/n = q/pq = 1/p$. Similarly, which numbers have a common divisor with q?

$$q, 2q, 3q, 4q, 5q, \cdots, pq = n$$

There are, obviously, p of these numbers. So, the probability of a random m being one of these numbers is $p/n = p/pq = 1/q$.

Therefore the probability that a number has a common divisor with $n = p \cdot q$ is

$$\frac{1}{p} + \frac{1}{q}$$

But, remember that we need to exclude those numbers that have a common divisor with p and q, according to the inclusion-exclusion principle. Multiplying the previous probabilities

$$\frac{1}{p} \cdot \frac{1}{q} = \frac{1}{pq}$$

Subtracting that from the previous result gives us

$$\frac{1}{p} + \frac{1}{q} - \frac{1}{pq}$$

Again, this is the same result.