On the Decryption Exponent of RSA

D. R. Stinson

Recall that the setting for the RSA cryptosystem is $\mathbb{Z}_n$, where $n = pq$, and p and q are distinct odd primes. In this situation, $\phi(n) = (p-1)(q-1)$. The encryption exponent b is chosen such that $\gcd(b, \phi(n)) = 1$, and the decryption exponent is defined to be

$$a = b^{-1} \bmod \phi(n).$$

Then the encryption function is $e_K(x) = x^b \bmod n$ and the decryption function is $d_K(y) = y^a \bmod n$.

In this note, we show that it is not necessary that $a \equiv b^{-1} \bmod \phi(n)$ — sometimes a smaller value can be used as the encryption exponent. (Thanks to Mike Wiener for pointing this out to me.)

We need the concept of the *exponent* of a (multiplicative) group G, which is defined to be the smallest positive integer λ such that $x^\lambda = 1$ for all $x \in G$. We know that $x^{|G|} = 1$ for all $x \in G$, so certainly the integer λ exists and is finite. (In fact, it is not hard to prove that λ divides $|G|$.) Now, if a and b are any two integers such that $ab \equiv 1 \bmod \lambda$, then it is not hard to show that $x^{ab} = x$ for all $x \in G$.

In the case of ${\mathbb{Z}_n}^*$, where $n = pq$ and p and q are distinct odd primes, it can be shown that

$$\lambda = \lambda(n) = \frac{(p-1)(q-1)}{\gcd(p-1, q-1)}.$$

So, suppose that we define

$$a' = b^{-1} \bmod \lambda(n).$$

By the remark above, $x^{a'b} = x$ for all $x \in {\mathbb{Z}_n}^*$. In fact, it is also true that $x^{a'b} = x$ for all $x \in \mathbb{Z}_n \backslash {\mathbb{Z}_n}^*$, so we can use a' as the decryption exponent instead of a, if we wish.

Here is a small example to illustrate. Suppose $p = 13$ and $q = 17$, so $n = 221$. Then $\phi(n) = 192$ and $\lambda(n) = 48$. Suppose the encryption exponent is $b = 37$. Then we have $a = 37^{-1} \bmod 192 = 109$, while $a' = 37^{-1} \bmod 48 = 13$.