Appendix R
Proof of the RSA Algorithm

William Stallings

R.1 BASIC RESULTS 2
R.2 PROOF 3

Supplement to
Cryptography and Network Security, Sixth Edition
Prentice Hall 2013
ISBN: 0133354695
http://williamstallings.com/Cryptography

The basic elements of the RSA algorithm can be summarized as follows. Given two prime numbers p and q, with $n = pq$ and a message block $M < n$, two integers e and d are chosen such that

$$M^{ed} \bmod n = M$$

We state in Section 9.2, that the preceding relationship holds if e and d are multiplicative inverses modulo $\phi(n)$, where $\phi(n)$ is the Euler totient function. It is shown in Chapter 8 that for p, q prime, $\phi(pq) = (p - 1)(q - 1)$. The relationship between e and d can be expressed as

$$ed \bmod \phi(n) = 1$$

Another way to state this is that there is an integer k such that $ed = k\phi(n) + 1$. Thus, we must show that

$$M^{k\phi(n)+1} \bmod n = M^{k(p-1)(q-1)+1} \bmod n = M \qquad \textbf{(R.1)}$$

R.1 BASIC RESULTS

Before proving Equation (R.1), we summarize some basic results. In Chapter 4, we showed that a property of modular arithmetic is the following

$$[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$$

From this, it should be easy to see that if we have $x \bmod n = 1$, then $x^2 \bmod n = 1$ and, for any integer y, we have $x^y \bmod n = 1$. Similarly, if we have $x \bmod n = 0$ for any integer y, we have $x^y \bmod n = 0$.

Another property of modular arithmetic is

$$[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$$

The other result we need is Euler's theorem, which was developed in Chapter 8. If integers a and n are relatively prime, then $a^{\phi(n)} \bmod n = 1$.

R.2 PROOF

First we show that $M^{k(p-1)(q-1)+1} \bmod p = M \bmod p$. There are two cases to consider.

Case 1: M and p are not relatively prime; that is, p divides M. In this case $M \bmod p = 0$ and therefore $M^{k(p-1)(q-1)+1} \bmod p = 0$. Thus, $M^{k(p-1)(q-1)+1} \bmod p = M \bmod p$.

Case 2: If M and p are relatively prime, by Euler's theorem, $M^{\phi(p)} \bmod p = 1$. We proceed as

$$\begin{aligned}
M^{k(p-1)(q-1)+1} \bmod p &= [(M)M^{k(p-1)(q-1)}] \bmod p \\
&= [(M)(M^{(p-1)})^{k(q-1)}] \bmod p \\
&= [(M)(M^{\phi(p)})^{k(q-1)}] \bmod p \\
&= (M \bmod p) \times [(M^{\phi(p)}) \bmod p]^{k(q-1)} \\
&= (M \bmod p) \times (1)^{k(q-1)} \qquad \text{(by Euler's theorem)} \\
&= M \bmod p
\end{aligned}$$

We now observe that

$$[M^{k(p-1)(q-1)+1} - M] \bmod p = [M^{k(p-1)(q-1)+1} \bmod p] - [M \bmod p] = 0$$

Thus, p divides $[M^{k(p-1)(q-1)+1} - M]$. By the same reasoning, we can show that q divides $[M^{k(p-1)(q-1)+1} - M]$. Because p and q are distinct primes, there must exist an integer r that satisfies

$$[M^{k(p-1)(q-1)+1} - M] = (pq)r = nr$$

Therefore, n divides $[M^{k(p-1)(q-1)+1} - M]$, and so $M^{k\phi(n)+1} \bmod n = M^{k(p-1)(q-1)+1} \bmod n = M$.