Errata to "High-Speed RSA Implementation"

November 14, 2005

This note updates RSA Laboratories' Technical Note TR-201, "High-Speed RSA Implementation," by Çetin Kaya Koç, Version 2.0, November 1994.

- **Issue:** On page 4, the proof that $C^d = (M^e)^d \pmod{n}$ when $\gcd(M, n) > 1$ is incorrect. In particular, the claim that $M^{\lambda(n)} = 1 \pmod{n}$ in this case is incorrect.

- **Resolution:** Replace the text from "The exception …" through the end of the paragraph with the following:

  The exception $\gcd(M, n) > 1$ can be dealt with as follows. Let $g = \gcd(M, n)$ and let $h = n/g$. Since n is a product of distinct primes, g and h will be relatively prime. Now consider the values

  $$C_1 = (M^e)^d \bmod g \ ,$$
  $$C_2 = (M^e)^d \bmod h \ .$$

  Since M is divisible by g, we have $C_1 \equiv 0 \bmod g$.

  Since M is relatively prime to h, we can apply the general case recursively to show that $C_2 \equiv M \bmod h$.

  It follows by the Chinese Remainder Theorem that $(M^e)^d \equiv M \bmod n$.