RSA-CRT Fault Attack

Let (e, N) be the RSA public key and $(p, q, |d|_p, |d|_q, |q^{-1}|_p)$ the RSA private key for use with Chinese Remainder Theorem (CRT). Furthermore, assume that the signer produced a faulty signature f, whereby the fault affected only the partial signature modulo p (i.e. s_1 according to the RFC), and later discovered that the signature was invalid and recomputed the signature s, this time without errors.

We know from PKCS #1 that there exist s_1, s_2 s.t. $s = s_2 + q \cdot \left|(s_1 - s_2) \cdot |q^{-1}|_p\right|_p$ and similarly some f_1 exists s.t. $f = s_2 + q \cdot \left|(f_1 - s_2) \cdot |q^{-1}|_p\right|_p$.

From that follows that $s - f = q \cdot \left|(s_1 - f_1) \cdot |q^{-1}|_p\right|_p$, which means q divides $s - f$.

Since q is prime, it follows that $q = \gcd(s - f, N)$.

References:

- https://crypto.stanford.edu/~dabo/abstracts/faults.html

⟲ Revision #1
★ Created 13 December 2024 11:56:28 by Annatar
✎ Updated 18 December 2024 21:49:33 by Annatar