



Problem 1. «RSA signature»

We want to sign the message M using the RSA-signature. As usually, let $N = p \cdot q$ be the RSA-modulus, where p and q are two big primes. Let e be the RSA-public exponent and d be the RSA-secret exponent satisfying that $e \cdot d = 1 \pmod{(p-1)(q-1)}$. The desired signature is given by

$$S = M^d \pmod{N}.$$

Suppose that the attacker knows the value

$$M_p := M^{d_p} \pmod{p},$$

but he doesn't know the value

$$M_q := M^{d_q} \pmod{q},$$

where

$$d_p := d \pmod{p-1}, \quad d_q := d \pmod{q-1}.$$

If the attacker knows the modulus N (but not p and q), the public exponent e (but not d), and the original message M , what secret signature parameters can he calculate? Justify the answer.

