NSUCRYPTO2024

Problem 1: RSA Signature

October 21, 2024

Solution:

The attacker can calculate p, q, and d as follows:
Since the attacker knows M_p, e, and N, they can calculate the value:

$$M_p^e \equiv M^{d_p \cdot e} \pmod{p}$$

Given that $e \cdot d_p \equiv 1 \pmod{p-1}$, we know that:

$$M_p^e \equiv M \pmod{p} \Rightarrow M_p^e = M + k \cdot p \quad \text{for some} \quad k \in \mathbb{Z}$$

Since the attacker also knows the value of M, they can recover p by calculating:

$$\gcd(N, M_p^e - M)$$

This has a high probability of yielding the value of p when $M_p \not\equiv M_q$.
Once p is known, the attacker can compute:

$$q = \frac{N}{p}$$

With p and q known, the attacker can now compute $\varphi(N) = (p-1)(q-1)$, and from there, the private exponent d can be calculated by:

$$d \equiv e^{-1} \pmod{\varphi(N)}$$

Please refer to the solution script for more details on NSUCRYPTO2024 Problem 1.