nullhat 2025: warmup

@elesquina

The task gives one RSA modulus $N = pq$, two public exponents e_1, e_2, and two ciphertexts c_1, c_2. The code shows that the same plaintext m was encrypted twice under the same N, once with e_1 and once with e_2, so $c_1 \equiv m^{e_1} \pmod N$ and $c_2 \equiv m^{e_2} \pmod N$. The important detail is that e_1 and e_2 are random primes, so $\gcd(e_1, e_2) = 1$ with overwhelming probability.

Because $\gcd(e_1, e_2) = 1$, there exist integers a, b such that $ae_1 + be_2 = 1$. Extended Euclid gives such (a, b). Then

$$m \equiv m^{ae_1+be_2} \equiv (m^{e_1})^a (m^{e_2})^b \equiv c_1^a c_2^b \pmod N.$$

If $a < 0$ (or $b < 0$), we replace c_1^a by $(c_1^{-1})^{-a}$ modulo N using a modular inverse. This yields m as an integer modulo N, which can be converted back to bytes and stripped from leading zero bytes to recover the plaintext.

The recovered plaintext contains the flag: `EliteSec{an_easy_rsa_warmup_challenge_ftw3214124124}`.