GreyCTF QRSA

mechfrog88

Please refer to `output.txt` for the value of N_a, N_b, C_a, C_b, e, D

Encryption of `FLAG`

1. Split `FLAG` by half and let

$$M_a = \texttt{int.from\_bytes(FLAG[first half], 'big')}$$
$$M_b = \texttt{int.from\_bytes(FLAG[last half], 'big')}$$

2. Set $M = M_a + M_b\sqrt{D}$
3. Find $p = p_a + p_b\sqrt{D},\ q = q_a + q_b\sqrt{D}$, where $p_a, p_b, q_a, q_b \in \mathbb{Z}$
4. Set $N = p \cdot q = N_a + N_b\sqrt{D}$
5. Define $x \equiv y \bmod N$ as $x = y + k \cdot N$ for some $k = k_a + k_b\sqrt{D}$, where $k_a, k_b \in \mathbb{Z}$
6. Set $C \equiv M^e \bmod N$, and $C = C_a + C_b\sqrt{D}$

You can assume that `FLAG` is of reasonable length and is printable ASCII text