RSA - Solution

Mu Games

To find Bob and Charlie's favorite numbers it is sufficient to the private keys $(p_1, q_1), (p_2, q_2)$ given $N_1 = p_1 q_1$ and $N_2 = p_2 q_2$. Note however that Alice reused her favorite prime for both private keys so without loss of generality we can say that $p_1 = p_2 = p$. Now we can efficiently calculate p using $p = \gcd(N_1, N_2)$. After we have calculated p, we can find q_1, q_2 by dividing N_1, N_2 respectively.

We can now decrypt the cipher text using the decryption algorithm.

Note that it is not feasible in this exercise to factor N_1, N_2 using brute force because the numbers are too big.