Cookie Lover: RSA Signature Forgery

November 14, 2023

1 Introduction

In this RSA signature forgery challenge, we want to forge a signature for the message *"I love cookies."*. Naturally, we only have access to the public RSA key, but do not know the secret key d. Further, we have access to an oracle that will sign any message for us (using the secret key d) - *with the exception* of strings containing the string "cookie" or control characters.

2 The Solution

What we need to do is find a factorization of the message (in its integer representation) so that each of the factors conforms to the oracle's constraints. Since RSA is multiplicative, we can then multiply the individual signatures together to get the signature for "I love cookies." E.g., say $m = a \cdot b \cdot c$, i.e., we can factor our message into the three factors a, b, and c (which aren't necessarily prime). Then $a^d \cdot b^d \cdot c^d = (a \cdot b \cdot c)^d = m^d$.

I went about this by firstly factoring the message into its prime factors using code found on the internet (`pollard_rho.py`), then determining which of these factors fulfill the oracle's criteria for messages it is willing to sign. Subsequently, I computed all subsets of these valid factors to find one whose product was equal to the message. I had all elements of this subset signed by the oracle, multiplied the results together and thus successfully forged my signature. Lit!