Problem Set 5

Due: March 6th, 5pm

1 Formal proofs

For each problem in this section, you must give a complete and rigorous proof. Your arguments should be clear, logically ordered, and written in full sentences.

In particular, state all assumptions explicitly and define all notation. Justify every nontrivial step.

1. Let p, q be prime numbers and $n = pq$. Suppose (n, e, d) is a valid RSA key triple. Prove that for *any* $M \in \mathbb{Z}_n$, $M^{ed} \equiv M \pmod{n}$.

2. ## 2 Demonstrations

For problems in this section, you still need to give complete mathematical reasoning to support your answers. I should be able to follow and understand your work, but it doesn't have to be organized into a formal proof.

3. Hey

3 Explorations

In this section, I'm looking for answers that are supported by evidence, but you don't have to prove your answers.

4. Hey