Exercise 1. Factorize $n = 33$ given non-trivial square roots of unity 10 and 23.

Exercise 2. Factorize $n = 1457$. Suppose you have learned that 1457 is a probable prime to base 187, and a strong pseudoprime to base 187.

Exercise 3. Factorize RSA modulus $n = 2491$, given that $e = 3$ and $d = 1595$.

Exercise 4. Show that textbook RSA is not secure against chosen plaintext attack. The IND-CPA game is defined as follows

1. The challenger generates a new key pair PK, SK and publishes PK to the adversary, the challenger retains SK.
2. The adversary may perform a polynomially bounded number of calls to the encryption oracle or other operations.
3. Eventually, the adversary submits two distinct plaintexts M_0 and M_1 to the challenger.
4. The chellenger selects a bit $b \in \{0, 1\}$ uniformly at random, and sends the challenge ciphertext $C = E(PK, M_b)$ back to the adversary.
5. The adversary is free to perform any number of additional computations.
6. Finally, the adversary outputs a guess for the value b.

A cryptosystem is indistinguishable under chosen plaintext attack (is IND-CPA secure) if every probabilistic polynomial time adversary has only a negligible advantage over random guessing.

Exercise 5. Use homomorphic properties of RSA to show that textbook RSA is not secure against adaptive chosen ciphertext attack (CCA2). The IND-CCA2 game is defined as follows.

1. The challenger generates a new key pair PK, SK and publishes PK to the adversary, the challenger retains SK.
2. The adversary may perform any number calls to the encryption or decryption oracles, or other operations.
3. Eventually, the adversary submits two distinct chosen plaintexts M_0 and M_1 to the challenger.
4. The challenger selects a bit $b \in \{0, 1\}$ uniformly at random, and sends the challenge ciphertext $C = E(PK, M_b)$ back to the adversary.
5. The adversary is free to perform any number of additional computations, calls to the encryption and decryption oracles, but may not submit the challenge ciphertext C to the decryption oracle.
6. Finally, the adversary outputs a guess for the value b.

The plaintext RSA is homomorphic w.r.t. multiplication, meaning that

$$\begin{cases} C_1 = m_1^e \bmod n \\ C_2 = m_2^e \bmod n \end{cases} \Longrightarrow C_1 \times C_2 = m_1^e \cdot m_2^e \bmod n = (m_1 m_2)^e \bmod n \ .$$