1. Given a public exponent e, find suitable prime factors p and q of an RSA modulus.

2. Given primes $p = 37, q = 31$, and a public exponent $e = 5$, find the corresponding RSA private exponent d or explain why it doesn't exist.

3. Given a public exponent $e = 3$, find two suitable prime numbers p and q between 1000 and 2000. Compute modulus $n = pq$ and private exponent d. Let m be your 6-digit student code. Perform encryption, decryption, signature and signature verification operations on m.

4. Given the same primes p and q as in the previous task, find all four square roots of 1 modulo $n = pq$.

5. Consider a modification to the RSA signature scheme, where instead of performing computations in a composite order ring $\mathbb{Z}_{pq}$, we work in a prime order ring $\mathbb{Z}_n$, where n is a sufficiently large prime. The modified scheme works as follows.

   (a) For a fixed value of a public exponent e, Alice selects a sufficiently large prime n, which is her public key, and calulates her private exponent d.

   (b) Alice distributes her signature $s = m^d \bmod n$ on message m.

   This modified signature scheme is not secure against passive adversary Carol. It is sufficient for Carol to obtain one single sample of Alice's signature, so that Carol is able to create an arbitrary amount of fake signatures on behalf of Alice. How can Carol do that?