

Homework n.2

1. Find two arbitrary prime numbers p and q between 1000 and 2000. Compute the modulus $n = pq$. Choose a public exponent e so that the private exponent d can be computed, and compute the private exponent d . Let s be your 6-digit student number. Compute:

$$\begin{aligned}y &= s^e \pmod{n} \\x &= s^d \pmod{n}\end{aligned}$$

After that, compute $y^d \pmod{n}$ and $x^e \pmod{n}$.

2. Given the same primes p and q (of Exercise 1), and $n = pq$, find all four square roots of 1 modulo n .

Solutions due: Dec 16, 2019.