Exercise 1

Test the limit for the Miller-Rabin-Test with fixed bases.

1. Find the smallest composite n, that passes the test for $a = 2$.
2. Find the smallest composite n, that passes the test for $a = 2$ and $a = 3$.

Exercise 2

Run the code in `fermat_factorisation.py` and factor the resulting number.

Exercise 3

Apply the quadratic sieve to find a factor of 4755.

Exercise 4

Alice and Bob used the symmetric group for their Diffie-Hellman exchange. Find the flag that was sent. The code and the observed traffic is given on Isis.