

General Setting

Better add `tools.py` to your Python path, or just copy it into every single folder.


For every task:

- in `setup.py` you find the source code
- this code was executed, generating the corresponding output
- file `secret.py` and all private keys were removed

Exercise 1

Find the secret flag for each cipher in `secret_parameters`, where some additional information about the private key is given.

Exercise 2

1. Find a method, how we can decrypt every message, if we are given $d_p := d \bmod (p - 1)$ and the public key (n, e) .
2.  **Bonus:** Can you also break the secret key, if you are given $q^{-1} \bmod p$?

Remark. Recall, that d_p and $q^{-1} \bmod p$ are two of the secret values we can use to faster decrypt messages via CRT.

Exercise 3

Find the rather small messages in `small_message_small_exponent`, that were encrypted with $e = 3$. For some parts you probably need Sagemath.

If you find a way without Sagemath, post it!

Exercise 4

Find the secret message, that was sent to 20 people in the code for `hastad`.

Exercise 5

Slide 54 suggests solving the root in the integers via bisection. What are reasons against using faster methods like Newton- or Secant-Method?

Exercise 6 (Bonus)

Compute a small addition chain for $n = 2^{127} - 3$.