Programming Languages: FP Practicals 2-2. Caesar Cipher

Shin-Cheng Mu

Autumn 2025

1. Go to our course homepage `https://cool.ntu.edu.tw/courses/51303`. Navigate to the Modules tab.

2. Download `CaesarCipher.zip` (among materials for Week 3).

3. The main task is to define the functions below:

$$encode :: Int \to String \to String \;,$$
$$crack \;\; :: String \to Int \;,$$
$$decode :: String \to String \;,$$

such that $encode\ k\ xs$ enciphers xs using the key k, $crack\ ys$ takes a ciphered string and tries to recover the key, and $decode\ xs$ deciphers the input string (using $crack$).

4. Many auxiliary functions are currently given as "undefined". You may need to define your own auxiliary functions too.

5. This practical is adapted from a chapter in Hutton [Hut07]. For many fascinating stories about cryptography, see Singh [Sin00].

References

[Hut07] Graham Hutton. *Programming in Haskell*. Cambridge University Press, 2007.

[Sin00] Simon Singh. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Anchor, 2000.