

Exercise - Encryption



In case you get stuck anywhere, don't be afraid to ask the coaches! They are here to help and will gladly explain everything to you!

Take notes during the exercises. Even if you never look at them again, they will help you memorise things!

In this little exercise we're going to implement the Caesar Cipher in Ruby!

The Caesar Cipher is a very simple form of encryption. It is not recommended for any serious use! Here's how it works:

Input:

- Plain text (must only contain characters A-Z)
- Key (integer number)

Output:

- Encrypted text

Each letter of the alphabet gets shifted by a number of letters. E.g. for the key "1", the alphabet gets shifted by 1 letter, as seen in this table:

plain text	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	...
cipher text	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	...

For example, the input text HELLOWORLD, encrypted with key "1" would end up as IFMMPXPSME. With key "2" it would be: JGNNQYQTNF and so on.

Implement a command line tool called "caesar.rb" that allows the following interaction:

```
% ruby caesar.rb encrypt 1 HELLOWORLD
IFMMPXPSME
```

```
% ruby caesar.rb decrypt 1 IFMMPXPSME
HELLOWORLD
```

Hints

- Use Ruby's ARGV to retrieve command line arguments like "encrypt", "1" and "HELLOWORLD".
- Make sure the text to encrypt/decrypt only contains the capital letters A-Z, no spaces!
- Check that the command is either "encrypt" or "decrypt" and show an error if that's not the case.