Musa Al‘Khwarizmi
CS 3141: Prof. Kamil’s Algorithm Analysis
June 8, 2024

Overleaf Homework Template

Question 1. Write down sets in order of containment.

We pretend that equivalence classes are just numbers.

$$\mathbb{C} \supset \mathbb{R} \supset \mathbb{Q} \supset \mathbb{Z} \supset \mathbb{N} \supset \mathbb{P} \not\supset (\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}) \supset \{\varnothing\}$$

Question 2. Find roots of $x^2 - 8x = 9$.

We proceed by factoring,

$$\begin{aligned} x^2 - 8x - 9 &= 9 - 9 && \text{Subtract 9 on both sides.} \\ x^2 - x + 9x - 9 &= 0 && \text{Breaking the middle term.} \\ (x-1)(x+9) &= 0 && \text{Pulling out common } (x-1). \\ x &\in \{1, -9\} && f(x)g(x) = 0 \Rightarrow f(x) = 0 \vee g(x) = 0. \end{aligned}$$

Question 3. Figure 1 shows two cipher wheels. The left one is from Jeffrey Hoffstein, et al. [1] (pg. 3). Write a Python 3 program that uses it to encrypt: `FOUR SCORE AND SEVEN YEARS AGO`.

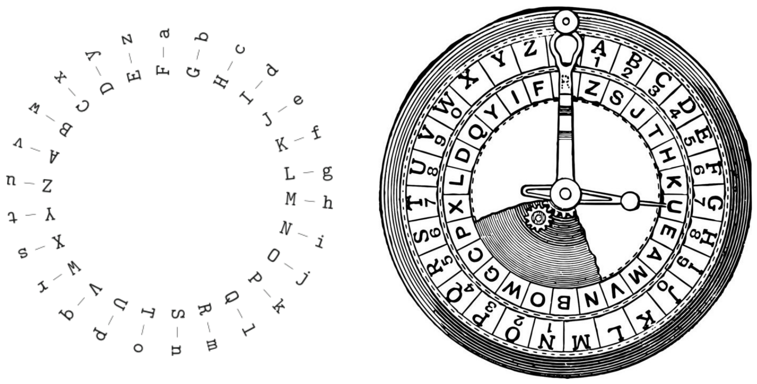

Figure 1. Cipher wheels.

The Python program is given in listing 1 and the encryption is given in table 1.

```python
def encrypt(plain):
    cipher = ''
    for c in plain:
        cipher = cipher+c if c==' ' else cipher+chr(((ord(c)-60) % 26)+65)
    return cipher
print(encrypt("FOUR SCORE AND SEVEN YEARS AGO"))
```

Listing 1. Python 3 implementing figure 1 left wheel.

Plain Text	FOUR	SCORE	AND	SEVEN	YEARS	AGO
Cipher Text	KTZW	XHTWJ	FSI	XJAJS	DJFWX	FLT

Table 1. Caesar cipher

References

[1] Jeffrey Hoffstein, Jill Pipher, Joseph H Silverman, and Joseph H Silverman. *An introduction to mathematical cryptography*, volume 1. Springer, 2008.

Bayt El-Hikmah