Solutions for Example 2 Practice

Problem A (easier). Encrypt with $k = 4$: `MATH IS FUN`

Map to numbers (A=0):

$$\texttt{MATH IS FUN} \Rightarrow 12, 0, 19, 7,\ 8, 18,\ 5, 20, 13.$$

Add 4 mod 26:

$$12, 0, 19, 7 \mapsto 16, 4, 23, 11 \quad (\text{M} \to \text{Q},\ \text{A} \to \text{E},\ \ldots)$$

$$8, 18 \mapsto 12, 22 \qquad 5, 20, 13 \mapsto 9, 24, 17.$$

Back to letters:

$$16, 4, 23, 11,\ 12, 22,\ 9, 24, 17 \Rightarrow \boxed{\texttt{QEXL MW JYR}}.$$

Why it works: Every step is addition in $\mathbb{Z}_{26}$; wrap ensures letters stay in 0–25.

Problem B (similar). Decrypt with $k = 11$: `SPWWZ HZCWO`

Numbers for ciphertext:

$$\texttt{SPWWZ HZCWO} \Rightarrow 18, 15, 22, 22, 25,\ 7, 25, 2, 22, 14.$$

Subtract 11 (or add 15) mod 26:

$$18, 15, 22, 22, 25 \mapsto 7, 4, 11, 11, 14 \quad (\text{H,E,L,L,O})$$

$$7, 25, 2, 22, 14 \mapsto 22, 14, 17, 11, 3 \quad (\text{W,O,R,L,D}).$$

Plaintext: $\boxed{\texttt{HELLO WORLD}}$.

Problem C (harder). Unknown k: `P HT HA AOL WHYR`

Strategy (the why): Look for patterns. A one-letter word is probably `I` or `A`. Also, `AOL` famously appears when "`THE`" is shifted by $k = 7$ (since $19+7 = 26 \equiv 0 = \text{A}$, etc.).

Infer k: If `AOL` is `THE`, then the shift is $k = 7$.

Decrypt by subtracting 7:

$$\texttt{P} \mapsto \texttt{I}, \quad \texttt{HT} \mapsto \texttt{AM}, \quad \texttt{HA} \mapsto \texttt{AT}, \quad \texttt{AOL} \mapsto \texttt{THE}, \quad \texttt{WHYR} \mapsto \texttt{PARK}.$$

$\Rightarrow$ `I AM AT THE PARK`.

Key takeaways.

- Encryption: $E_k(p) = (p + k) \bmod 26$, Decryption: $D_k(c) = (c - k) \bmod 26$.
- Unknown k can be cracked with educated guesses ("`THE`", one-letter words) or brute force (only 26 options).
- Thinking in $\mathbb{Z}_{26}$ explains the wrap-around and keeps errors low.