Example 7 (Worksheet) — Shift Ciphers as a Cryptosystem

Goal. Describe the family of shift ciphers in the formal language of a cryptosystem.

The Big Idea: What's a Cryptosystem?

A **cryptosystem** is a mathematical framework describing how messages are encrypted and decrypted. Formally, it's written as a 5-tuple:

$$(\mathcal{P},\ \mathcal{C},\ \mathcal{K},\ \mathcal{E},\ \mathcal{D})$$

where each symbol represents a part of the encryption ecosystem:

- $\mathcal{P}$ – the set of possible *plaintexts*
- $\mathcal{C}$ – the set of possible *ciphertexts*
- $\mathcal{K}$ – the *keyspace*, all keys that can be used
- $\mathcal{E}$ – the set of *encryption functions*
- $\mathcal{D}$ – the set of *decryption functions*

The golden rule of any cryptosystem is:

$$D_k(E_k(p)) = p \quad \text{for every plaintext } p.$$

That means: decrypting an encrypted message must always give you back the original.

Step 1 — Translate the Language of Letters into Math

Each letter of the alphabet is assigned a number in $\mathbb{Z}_{26}$ (the integers 0–25 mod 26).

$$\mathrm{A} = 0,\ \mathrm{B} = 1,\ \ldots,\ \mathrm{Z} = 25$$

A message like `HELLO` becomes $[7, 4, 11, 11, 14]$.

Step 2 — Define the Shift Cipher Functions

To encrypt, we *add* a fixed key k mod 26:

$$E_k(p) = (p + k) \bmod 26.$$

To decrypt, we *subtract* the same k mod 26:

$$D_k(c) = (c - k) \bmod 26.$$

Step 3 — Describe the Family of Shift Ciphers as a Cryptosystem

Putting it all together:

$$\begin{aligned}
\mathcal{P} &= \mathcal{C} = \text{all strings of elements in } \mathbb{Z}_{26},\\
\mathcal{K} &= \mathbb{Z}_{26},\\
\mathcal{E} &= \{\, E_k(p) = (p + k) \bmod 26 \mid k \in \mathbb{Z}_{26} \,\},\\
\mathcal{D} &= \{\, D_k(c) = (c - k) \bmod 26 \mid k \in \mathbb{Z}_{26} \,\}.
\end{aligned}$$

This means each possible shift k defines one member of the family of shift ciphers.

Step 4 — Check the "Undo" Property

To verify that encryption and decryption work as a matched pair:

$$D_k(E_k(p)) = (p + k - k) \bmod 26 = p.$$

So every message can be perfectly recovered.

Tips & Common Pitfalls

- Don't confuse the "keyspace" $\mathcal{K}$ with a single key k. The keyspace is the entire set of possible shifts.
- Forgetting to take mod 26 is a very common mistake.
- A shift cipher is *not secure* — only 26 possible keys! We study it to understand the structure of more complex systems.

Practice — Your Turn!

Problem A (Easier). For a shift cipher with $k = 5$, write down $E_k(p)$ and $D_k(c)$. Explain in your own words what "mod 26" ensures.

Problem B (Similar). Let $p = 19$ (the letter T) and $k = 7$. Compute $E_k(p)$ and translate it back into a letter. Then apply D_k to check that you get back T.

Problem C (Harder). Write the complete 5-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ for a system that works on uppercase English letters and digits (0–9). What changes?

Reflection. How does writing cryptography in formal notation help us build new systems in the future?