Discrete Structures   Chapter 4.6 — Cryptography

Example 1 (Student Worksheet): Caesar Cipher, shift $k = 3$

Learning goals. Practice converting letters $\leftrightarrow$ numbers, computing $(p + k) \bmod 26$, and translating back.

Alphabet convention (zero-based).

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

We work in $\mathbb{Z}_{26}$ (mod 26). Spaces and punctuation are carried through unchanged; we use uppercase.

Encryption rule. For plaintext number $p \in \{0, \ldots, 25\}$ and shift k, the ciphertext number is

$$c \equiv p + k \pmod{26}.$$

For this worksheet we use $\boxed{k = 3}$ (the classic "Caesar +3").

Fast tips (use 'em shamelessly):

- Add 3 quickly by doing *+1, +2, +3* as you scan, or use the wrap trick: adding 3 to $24, 25$ wraps to $1, 2$.
- Decrypting a +3 cipher is the same as *adding* -3, i.e., adding 23 mod 26.
- Common wrap cases: 24+3 $\to$ 1 (Y$\to$B), 25+3 $\to$ 2 (Z$\to$C).

Guided task. Encrypt the message:

`MEET YOU IN THE PARK`

Step 1 — Letters $\to$ numbers (A=0,...,Z=25). Fill the *plaintext numbers* p under each letter.

M E E T Y O U I N T H E P A R K

(write numbers p here)

Step 2 — Add the shift $k = 3$ mod 26. Compute $c \equiv p + 3 \pmod{26}$ for each position and write the results:

Step 3 — Numbers $\to$ letters. Translate each c back to letters to form the ciphertext:

Neatness check. Your ciphertext should be readable in groups (keep the spaces from the original). If you decrypt with -3 you should land back on `MEET YOU IN THE PARK`.

Quick reference table (optional). If you like a visual:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Practice (still Caesar, but you drive):

P1. Encrypt (easy). Use $k = 5$ to encrypt:

`DOGS AND CATS`

Hint: D=3 so D$\mapsto$3+5=8 $\Rightarrow$ I. Keep spaces.

P2. Decrypt (easy). The ciphertext below was made with a $k = 5$ Caesar. Recover the plaintext.

`YMNX NX FQ YJXY`

Tip: Decrypt by adding -5 (or $+21$) mod 26.

P3. Crack the shift (harder). The message below is a Caesar cipher with *unknown* k:

`L ORYH PDWKP`

Clues: Try common words; guess that "`PDWKP`" might be "`MATH?`" or "`MATHS?`". Also, a one-letter word is often `A` or `I`. Determine k and decrypt.

Reflection. In one sentence: why does "mod 26" make the Caesar cipher *wrap* from Z back to A?

Example 1: Caesar Cipher ($k = 3$)

Question. Encrypt the message `MEET YOU IN THE PARK` using the Caesar cipher with shift $k = 3$.

Step 1 — Letters → numbers.

We use zero-based numbering: A=0, B=1, ..., Z=25.

$$\text{MEET YOU IN THE PARK} \quad \Rightarrow \quad 12, 4, 4, 19,\ 24, 14, 20,\ 8, 13,\ 19, 7, 4,\ 15, 0, 17, 10$$

Step 2 — Apply $f(p) = (p + 3) \bmod 26$.

Add 3 to each number, wrapping around if the result exceeds 25:

$$(12 + 3) = 15,\ (4 + 3) = 7,\ (4 + 3) = 7,\ (19 + 3) = 22,$$

$$(24 + 3) = 27 \equiv 1,\ (14 + 3) = 17,\ (20 + 3) = 23,$$

$$(8 + 3) = 11,\ (13 + 3) = 16,\ (19 + 3) = 22,\ (7 + 3) = 10,\ (4 + 3) = 7,$$

$$(15 + 3) = 18,\ (0 + 3) = 3,\ (17 + 3) = 20,\ (10 + 3) = 13.$$

Step 3 — Numbers → letters.

Convert the ciphertext numbers back to letters:

$$15, 7, 7, 22,\ 1, 17, 23,\ 11, 16,\ 22, 10, 7,\ 18, 3, 20, 13$$

$$\Rightarrow \text{PHHW BRX LQ WKH SDUN}$$

Final Answer. The encrypted message is:

$$\boxed{\texttt{PHHW BRX LQ WKH SDUN}}$$

(Translation: "MEET YOU IN THE PARK" shifted +3.)

Quick Reflection. The Caesar cipher uses modular arithmetic in $\mathbb{Z}_{26}$ so letters "wrap around" after Z. The function $f(p) = (p + k) \bmod 26$ keeps all results in 0–25.

—

Practice Solutions

P1 — Encrypt (easy). Use $k = 5$ to encrypt: `DOGS AND CATS`.

Step 1 — Convert to numbers:

$$3, 14, 6, 18,\ 0, 13, 3,\ 2, 0, 19, 18$$

Step 2 — Add 5 mod 26:

$$8, 19, 11, 23,\ 5, 18, 8,\ 7, 5, 24, 23$$

Step 3 — Back to letters:

$$\boxed{\texttt{ITLX FSI HFYX}}$$

—

P2 — Decrypt (easy). Decrypt `YMNX NX FQ YJXY` that was made with $k = 5$.

We reverse the shift: $c - 5 \pmod{26}$.

$$\text{Y} = 24 \to 19 = \text{T},\ \text{M} = 12 \to 7 = \text{H},\ \text{N} = 13 \to 8 = \text{I},\ \text{X} = 23 \to 18 = \text{S}$$
$$\Rightarrow \boxed{\texttt{THIS IS AN TEST}}$$

So the message is "THIS IS AN TEST." (It should probably read "THIS IS A TEST.")

—

P3 — Crack the shift (harder). Ciphertext: `L ORYH PDWKP!`

Try guessing common English patterns.

`ORYH` looks like "LOVE," and the one-letter word "L" likely corresponds to "I."

That suggests a shift of $k = 3$ backward (since L $\to$ I is -3).

Decrypting with $k = 3$:

$$\texttt{L ORYH PDWKP!} \Rightarrow \boxed{\texttt{I LOVE MATH!}}$$

—

Summary of Key Takeaways

- The Caesar cipher is modular addition in $\mathbb{Z}_{26}$.
- Encryption: $E_k(p) = (p + k) \bmod 26$
- Decryption: $D_k(c) = (c - k) \bmod 26$
- If you can add or subtract mod 26, you can encrypt or decrypt.
- This cipher is historically important but easily broken by frequency analysis or brute force (26 possibilities).

Going Deeper. You can extend this same math to more complex ciphers:

$$f(p) = (a \cdot p + b) \bmod 26$$

where a must have a multiplicative inverse mod 26. This leads directly into the *Affine Cipher*—our next example.

Example 2 (Worksheet) — Shift Cipher with $k = 11$

Goal. Encrypt the message `STOP GLOBAL WARMING` using Caesar's shift cipher with $k = 11$.

Big idea (the "why"):

We model letters as numbers in $\mathbb{Z}_{26}$ so that a shift is just *modular addition*. This keeps us in the alphabet and gives the wrap-around from Z back to A.

$$\mathrm{A} = 0,\ \mathrm{B} = 1,\ \ldots,\ \mathrm{Z} = 25 \qquad\qquad E_k(p) = (p + k) \bmod 26.$$

For this example, $k = 11$.

Step 1 — Normalize and map letters → numbers

We use uppercase and keep spaces. Convert each letter of `STOP GLOBAL WARMING` to its number:

$$\underbrace{\texttt{STOP}}_{18\ 19\ 14\ 15} \quad \underbrace{\texttt{GLOBAL}}_{6\ 11\ 14\ 1\ 0\ 11} \quad \underbrace{\texttt{WARMING}}_{22\ 0\ 17\ 12\ 8\ 13\ 6}.$$

Step 2 — Apply the shift $k = 11$ (add 11 mod 26)

Compute $c \equiv p + 11 \pmod{26}$ for each number. Do the wrap when you go past 25.

$$\begin{aligned} \texttt{STOP}: &\quad 18, 19, 14, 15 \mapsto 3, 4, 25, 0 \\ \texttt{GLOBAL}: &\quad 6, 11, 14, 1, 0, 11 \mapsto 17, 22, 25, 12, 11, 22 \\ \texttt{WARMING}: &\quad 22, 0, 17, 12, 8, 13, 6 \mapsto 7, 11, 2, 23, 19, 24, 17. \end{aligned}$$

Step 3 — Map numbers → letters and keep spaces

$$3, 4, 25, 0 \ \mid 17, 22, 25, 12, 11, 22 \ \mid 7, 11, 2, 23, 19, 24, 17 \quad \Rightarrow \quad \boxed{\texttt{DEZA RWZMLW HLCXTYR}}$$

Helpful tips & common pitfalls

- **A=0, not 1.** Off-by-one mistakes are the #1 bug.
- **Wrap cleanly:** if $p + k \geq 26$, subtract 26 (i.e., reduce mod 26).

- **Spaces/punctuation** pass through unchanged; only letters get shifted.
- **Decrypting** with $k = 11$ is the same as adding -11 (or $+15$) mod 26.

Practice (your turn!)

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

Why: smaller shift, shorter phrase—perfect confidence builder.

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

Tip: subtract 11 mod 26 or add 15.

Problem C (harder). Unknown k. Decrypt the Caesar ciphertext: `P HT HA AOL WHYR`
Hints: a one-letter word is often `I` or `A`. The block `AOL` frequently shows up when "`THE`" is encrypted with $k = 7$.

Reflection. In one sentence: explain why modular arithmetic guarantees a valid letter after every shift.

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:

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

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

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:

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

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

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 $19+7 = 26 \equiv 0 = \mathrm{A}$, etc.).

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

Decrypt by subtracting 7:

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

$$\Rightarrow \boxed{\texttt{I AM AT THE PARK}}.$$

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.

Caesar Cipher Decryption

Student Worksheet

Understanding Decryption

Previously, we learned how to **encrypt** messages using the Caesar cipher. Now we'll learn to **decrypt** them—convert the secret message back to the original!

The key insight: **Decryption is the reverse of encryption.**

- **Encryption:** We shifted letters *forward* by k positions using $f(p) = (p + k) \bmod 26$
- **Decryption:** We shift letters *backward* by k positions using $f(p) = (p - k) \bmod 26$

Key Concept: Negative Numbers and Mod

When we subtract and get a negative number, we need to "wrap around" the other direction. For example, if we try to go back 7 from the letter E (position 4), we get $4 - 7 = -3$.
To handle this, we compute: $-3 \bmod 26 = 23$ (which is the letter X).
Quick trick: If you get a negative number, just add 26 to make it positive!

$$-3 + 26 = 23$$

Example 3: Worked Solution

Question: Decrypt the ciphertext message "LEWLYPLUJL PZ H NYLHA HSOHOLY" that was encrypted with the shift cipher with shift $k = 7$.

Solution:

Step 1: Convert letters to numbers

We use our standard A=0, B=1, C=2, ..., Z=25 system. Let's convert the ciphertext:

- **LEWLYPLUJL:** L=11, E=4, W=22, L=11, Y=24, P=15, L=11, U=20, J=9, L=11
- **PZ:** P=15, Z=25

- **H:** H=7
- **NYLHA:** N=13, Y=24, L=11, H=7, A=0
- **HSOHOLY:** A=0, L=11, H=7, O=14, L=11, Y=24

Our number sequence is:

$$11 \quad 4 \quad 22 \quad 11 \quad 24 \quad 15 \quad 11 \quad 20 \quad 9 \quad 11$$

15 25 7 13 24 11 7 0 0 11 7 9 14 11 24

Step 2: Apply the decryption function
We apply $f(p) = (p-7) \bmod 26$ to shift backward by 7. Let's work through each number:

$$\begin{aligned}
f(11) &= (11-7) \bmod 26 = 4 \bmod 26 = 4 \\
f(4) &= (4-7) \bmod 26 = -3 \bmod 26 = 23 \quad (\text{add } 26\text{: } -3+26=23) \\
f(22) &= (22-7) \bmod 26 = 15 \bmod 26 = 15 \\
f(11) &= (11-7) \bmod 26 = 4 \bmod 26 = 4 \\
f(24) &= (24-7) \bmod 26 = 17 \bmod 26 = 17 \\
f(15) &= (15-7) \bmod 26 = 8 \bmod 26 = 8 \\
f(11) &= (11-7) \bmod 26 = 4 \bmod 26 = 4 \\
f(20) &= (20-7) \bmod 26 = 13 \bmod 26 = 13 \\
f(9) &= (9-7) \bmod 26 = 2 \bmod 26 = 2 \\
f(11) &= (11-7) \bmod 26 = 4 \bmod 26 = 4
\end{aligned}$$

Continuing for the remaining letters:

$$f(15) = 8, \quad f(25) = 18, \quad f(7) = 0$$
$$f(13) = 6, \quad f(24) = 17, \quad f(11) = 4, \quad f(7) = 0, \quad f(0) = 19$$
$$f(0) = 19, \quad f(11) = 4, \quad f(7) = 0, \quad f(9) = 2, \quad f(14) = 7, \quad f(11) = 4, \quad f(24) = 17$$

Our decrypted numbers are:

$$4 \quad 23 \quad 15 \quad 4 \quad 17 \quad 8 \quad 4 \quad 13 \quad 2 \quad 4$$

8 18 0 6 17 4 0 19 19 4 0 2 7 4 17

Pro Tip: Handling Negative Results

Whenever $(p - k)$ gives you a negative number:

1. Notice it's negative
2. Add 26 to make it positive
3. That's your answer!

Example: $(4 - 7) = -3$, so $-3 + 26 = 23$

Step 3: Convert numbers back to letters
Using A=0, B=1, ..., Z=25:

- 4=E, 23=X, 15=P, 4=E, 17=R, 8=I, 4=E, 13=N, 2=C, 4=E
- 8=I, 18=S
- 0=A
- 6=G, 17=R, 4=E, 0=A, 19=T
- 19=T, 4=E, 0=A, 2=C, 7=H, 4=E, 17=R

Final Answer: The decrypted message is $\boxed{\textbf{EXPERIENCE IS A GREAT TEACHER}}$

Why This Works

If someone encrypted a message by shifting forward 7, we decrypt by shifting backward 7. It's like walking 7 steps forward, then 7 steps back—you end up where you started!

Practice Problems

Problem A (Easier Warm-up)

Decrypt the ciphertext "**FDW**" that was encrypted with shift $k = 3$.

Hint: This is a short message. Remember to subtract 3 from each letter's position. If you get negative numbers, add 26!

Problem B (Standard Practice)

Decrypt the ciphertext "**MJQQT BTWQI**" that was encrypted with shift $k = 5$.

Hint: You encrypted this message in the previous worksheet! Now decrypt it to get back the original message.

Problem C (Challenge)

Decrypt the ciphertext "**EJKKR ZRUOJ**" that was encrypted with shift $k = 5$.

Challenge: Some of these letters will give negative results when you subtract 5. Practice your wrapping-around skills!

Caesar Cipher Decryption
Teacher Solutions Manual

Problem A Solution: Decrypt "CAT" with shift $k = 3$

Step 1: Convert letters to numbers

$$\begin{aligned} \text{F} &= 5 \\ \text{D} &= 3 \\ \text{W} &= 22 \end{aligned}$$

Number sequence: 5 3 22

Step 2: Apply decryption function $f(p) = (p - 3) \bmod 26$

$$\begin{aligned} f(5) &= (5-3) \bmod 26 = 2 \bmod 26 = 2 \\ f(3) &= (3-3) \bmod 26 = 0 \bmod 26 = 0 \\ f(22) &= (22-3) \bmod 26 = 19 \bmod 26 = 19 \end{aligned}$$

Decrypted numbers: 2 0 19

Step 3: Convert back to letters

$$\begin{aligned} 2 &= \text{C} \\ 0 &= \text{A} \\ 19 &= \text{T} \end{aligned}$$

Answer: $\boxed{\textbf{CAT}}$

Teaching Note

This is the easiest problem because: (1) short message, (2) all results are positive (no negative numbers to handle), and (3) it's the reverse of Problem A from the encryption worksheet. Students can verify their answer by re-encrypting CAT with $k = 3$ to get FDW.

Problem B Solution: Decrypt "MJQQT BTWQI" with shift $k = 5$

Step 1: Convert letters to numbers

Breaking down by word:

- **MJQQT:** M=12, J=9, Q=16, Q=16, T=19
- **BTWQI:** B=1, T=19, W=22, Q=16, I=8

Number sequence:

$$12 \quad 9 \quad 16 \quad 16 \quad 19 \qquad 1 \quad 19 \quad 22 \quad 16 \quad 8$$

Step 2: Apply decryption function $f(p) = (p - 5) \bmod 26$

$$\begin{aligned}
f(12) &= (12 - 5) \bmod 26 = 7 \bmod 26 = 7 \\
f(9) &= (9 - 5) \bmod 26 = 4 \bmod 26 = 4 \\
f(16) &= (16 - 5) \bmod 26 = 11 \bmod 26 = 11 \\
f(16) &= (16 - 5) \bmod 26 = 11 \bmod 26 = 11 \\
f(19) &= (19 - 5) \bmod 26 = 14 \bmod 26 = 14 \\
f(1) &= (1 - 5) \bmod 26 = -4 \bmod 26 = 22 \quad (-4 + 26 = 22) \\
f(19) &= (19 - 5) \bmod 26 = 14 \bmod 26 = 14 \\
f(22) &= (22 - 5) \bmod 26 = 17 \bmod 26 = 17 \\
f(16) &= (16 - 5) \bmod 26 = 11 \bmod 26 = 11 \\
f(8) &= (8 - 5) \bmod 26 = 3 \bmod 26 = 3
\end{aligned}$$

Decrypted numbers:

$$7 \quad 4 \quad 11 \quad 11 \quad 14 \qquad 22 \quad 14 \quad 17 \quad 11 \quad 3$$

Step 3: Convert back to letters

- 7=H, 4=E, 11=L, 11=L, 14=O
- 22=W, 14=O, 17=R, 11=L, 3=D

Answer: $\boxed{\textbf{HELLO WORLD}}$

Teaching Note

This problem introduces negative numbers! When we decrypt B (position 1) with shift 5, we get: $1 - 5 = -4$.
To handle negative results in modular arithmetic: $-4 \bmod 26 = 22$
Students can calculate this by adding 26: $-4 + 26 = 22$, which corresponds to the letter W.
Connection: Students encrypted "HELLO WORLD" in the previous worksheet and got "MJQQT BTWQI". Now they're decrypting it back—reinforcing the inverse relationship between encryption and decryption.

Problem C Solution: Decrypt "EJKKR ZRUOJ" with shift $k = 5$

Step 1: Convert letters to numbers

Breaking down by word:

- **EJKKR:** E=4, J=9, K=10, K=10, R=17
- **ZRUOJ:** Z=25, R=17, U=20, O=14, J=9

Number sequence:

$$4 \quad 9 \quad 10 \quad 10 \quad 17 \qquad 25 \quad 17 \quad 20 \quad 14 \quad 9$$

Step 2: Apply decryption function $f(p) = (p - 5) \bmod 26$

$$\begin{aligned}
f(4) &= (4 - 5) \bmod 26 = -1 \bmod 26 = 25 \quad (-1 + 26 = 25) \\
f(9) &= (9 - 5) \bmod 26 = 4 \bmod 26 = 4 \\
f(10) &= (10 - 5) \bmod 26 = 5 \bmod 26 = 5 \\
f(10) &= (10 - 5) \bmod 26 = 5 \bmod 26 = 5 \\
f(17) &= (17 - 5) \bmod 26 = 12 \bmod 26 = 12 \\
f(25) &= (25 - 5) \bmod 26 = 20 \bmod 26 = 20 \\
f(17) &= (17 - 5) \bmod 26 = 12 \bmod 26 = 12 \\
f(20) &= (20 - 5) \bmod 26 = 15 \bmod 26 = 15 \\
f(14) &= (14 - 5) \bmod 26 = 9 \bmod 26 = 9 \\
f(9) &= (9 - 5) \bmod 26 = 4 \bmod 26 = 4
\end{aligned}$$

Decrypted numbers:

$$25 \quad 4 \quad 5 \quad 5 \quad 12 \qquad 20 \quad 12 \quad 15 \quad 9 \quad 4$$

Step 3: Convert back to letters

- 25=Z, 4=E, 5=F, 5=F, 12=M
- 20=U, 12=M, 15=P, 9=I, 4=E

Answer: $\boxed{\textbf{ZEFFM UMPIE}}$

Teaching Note

This is the *challenge* problem because it starts with E (position 4), which requires wrapping around when decrypted.

When we compute $f(4) = (4 - 5) = -1$, we need to wrap around to the *end* of the alphabet:

$$-1 \bmod 26 = 25 \text{ (the letter Z)}$$

Students can think of it this way: going back 1 from A brings you to Z (the last letter).

Mathematically: $-1 + 26 = 25$

Multiple negative cases: This problem is harder because it has multiple instances where students need to handle negative results, giving them more practice with this crucial concept.

Pattern recognition: Students might notice that letters early in the alphabet (A, B, C, D, E) will always produce negative results when the shift is larger than their position number.

Common Student Errors to Watch For

1. **Forgetting to handle negative numbers:** Students might write $4 - 5 = -1$ and stop there, not realizing they need to add 26. Watch for students who leave negative numbers in their final answer.

2. **Adding instead of subtracting:** Some students confuse encryption and decryption, using $(p + k)$ instead of $(p - k)$.

3. **Incorrect negative arithmetic:** Students might compute $-4 + 26$ incorrectly. Emphasize: start at 26, count backward 4.

4. **Off-by-one errors with A=0:** Remind students that A=0, not A=1. When they decrypt to position 0, that's the letter A.

5. **Not checking their work:** Students can verify decryption by re-encrypting their answer with the same shift—they should get back the original ciphertext.

Extension Activity

Have students encrypt a message with one shift value, then decrypt it with the same shift value to verify they get back the original message. This reinforces the inverse relationship:

$$\text{Message} \xrightarrow{+k} \text{Ciphertext} \xrightarrow{-k} \text{Message}$$

Example 4 — Affine Cipher Warm-Up

Goal. Determine which letter replaces `K` when the encryption function

$$f(p) = (7p + 3) \bmod 26$$

is used.

Big idea (the why):

The affine cipher multiplies the plaintext value by a "stretch" factor and then shifts it. It combines multiplication and addition inside modular arithmetic.

$$\text{Encryption: } E(p) = (ap + b) \bmod 26 \qquad \text{Decryption: } D(c) = a^{-1}(c - b) \bmod 26.$$

The constants a and b are keys. a must be coprime to 26 so that a^{-1} exists.

Step 1 — Convert letter K to a number

$$K \to 10$$

Step 2 — Apply the function $f(p) = (7p + 3) \bmod 26$

$$f(10) = (7 \cdot 10 + 3) \bmod 26 = 73 \bmod 26 = 21.$$

Step 3 — Convert number 21 back to a letter

$$21 \to V$$

Result: K is encrypted as V.

Why it works:

Multiplying by 7 mixes up the order of letters more effectively than a simple shift, yet because 7 and 26 are coprime, every letter still maps to exactly one output.

Practice (your turn!)

Problem A (easier). Using $f(p) = (3p + 1) \bmod 26$, find what letter replaces `C`. *Hint:* $C = 2$.

Problem B (similar). Using $f(p) = (5p + 7) \bmod 26$, find what letter replaces `H`. *Hint:* compute carefully, mod 26.

Problem C (harder). Encrypt the word `DOG` using $f(p) = (11p + 8) \bmod 26$. Write each step clearly: letter → number → formula → result → letter.

Reflection. Why must a be coprime with 26 for this cipher to be reversible?

Solutions — Example 4 Affine Cipher

Example Walk-Through

$K \to 10,\ f(p) = (7p+3) \bmod 26.$

$$f(10) = (7 \cdot 10 + 3) \bmod 26 = 73 \bmod 26 = 21.$$

21 corresponds to V. $\boxed{K \to V}$

—

Problem A

$C = 2.$

$$f(2) = (3 \cdot 2 + 1) \bmod 26 = 7.$$

$7 \to H.$ $\boxed{C \to H}$

Problem B

$H = 7.$

$$f(7) = (5 \cdot 7 + 7) \bmod 26 = 42 \bmod 26 = 16.$$

$16 \to Q.$ $\boxed{H \to Q}$

Problem C

Encrypt `DOG` with $f(p) = (11p + 8) \bmod 26$.

$$\begin{array}{rcrcl} D & = & 3 & \Rightarrow & (11 \cdot 3 + 8) \bmod 26 = 41 \bmod 26 = 15 \to P \\ O & = & 14 & \Rightarrow & (11 \cdot 14 + 8) \bmod 26 = 162 \bmod 26 = 6 \to G \\ G & = & 6 & \Rightarrow & (11 \cdot 6 + 8) \bmod 26 = 74 \bmod 26 = 22 \to W \end{array}$$

$\boxed{\texttt{DOG} \to \texttt{PGW}}$

Reflection Answer

If a shares a factor with 26, then some letters collapse to the same output (no unique inverse), making decryption impossible. Only when $\gcd(a, 26) = 1$ does the cipher remain bijective and reversible.

Example 2 (Worksheet) — Shift Cipher with $k = 11$

Goal. Encrypt the message `STOP GLOBAL WARMING` using Caesar's shift cipher with $k = 11$.

Big idea (the "why"):

We model letters as numbers in $\mathbb{Z}_{26}$ so that a shift is just *modular addition*. This keeps us in the alphabet and gives the wrap-around from Z back to A.

$$\text{A} = 0,\ \text{B} = 1,\ \ldots,\ \text{Z} = 25 \qquad\qquad E_k(p) = (p + k) \bmod 26.$$

For this example, $k = 11$.

Step 1 — Normalize and map letters → numbers

We use uppercase and keep spaces. Convert each letter of `STOP GLOBAL WARMING` to its number:

$$\underbrace{\texttt{STOP}}_{18\ 19\ 14\ 15} \quad \underbrace{\texttt{GLOBAL}}_{6\ 11\ 14\ 1\ 0\ 11} \quad \underbrace{\texttt{WARMING}}_{22\ 0\ 17\ 12\ 8\ 13\ 6}.$$

Step 2 — Apply the shift $k = 11$ (add 11 mod 26)

Compute $c \equiv p + 11 \pmod{26}$ for each number. Do the wrap when you go past 25.

$$\begin{aligned} \texttt{STOP}: &\quad 18, 19, 14, 15 \mapsto 3, 4, 25, 0 \\ \texttt{GLOBAL}: &\quad 6, 11, 14, 1, 0, 11 \mapsto 17, 22, 25, 12, 11, 22 \\ \texttt{WARMING}: &\quad 22, 0, 17, 12, 8, 13, 6 \mapsto 7, 11, 2, 23, 19, 24, 17. \end{aligned}$$

Step 3 — Map numbers → letters and keep spaces

$$3, 4, 25, 0 \ \mid 17, 22, 25, 12, 11, 22 \ \mid 7, 11, 2, 23, 19, 24, 17 \quad \Rightarrow \quad \boxed{\texttt{DEZA RWZMLW HLCXTYR}}$$

Helpful tips & common pitfalls

- **A=0, not 1.** Off-by-one mistakes are the 1 bug.
- **Wrap cleanly:** if $p + k \geq 26$, subtract 26 (i.e., reduce mod 26).

- **Spaces/punctuation** pass through unchanged; only letters get shifted.
- **Decrypting** with $k = 11$ is the same as adding -11 (or $+15$) mod 26.

Practice (your turn!)

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

Why: smaller shift, shorter phrase—perfect confidence builder.

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

Tip: subtract 11 mod 26 or add 15.

Problem C (harder). Unknown k. Decrypt the Caesar ciphertext: `P HT HA AOL WHYR`
Hints: a one-letter word is often `I` or `A`. The block `AOL` frequently shows up when "`THE`" is encrypted with $k = 7$.

Reflection. In one sentence: explain why modular arithmetic guarantees a valid letter after every shift.