Discrete Structures Chapter 4.6 — Cryptography

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

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

Alphabet convention (zero-based).

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

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↦3+5=8 ⇒ 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.