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?