# Solutions — Example 5 Practice

## Problem A (easier)

Ciphertext: `URYYB JBEYQ`; shift $k = 13$ (ROT13).
Decrypt by $p \equiv c - 13 \pmod{26}$ (or apply ROT13 again):

`HELLO WORLD`

## Problem B (similar)

Ciphertext: `ZHOFRPH WR FODVV`, unknown $k$.
Guess that `WR` is `TO`. Then $W = 22$ should map to $T = 19$, so $k \equiv 22 - 19 \equiv 3$ and decryption uses $p \equiv c - 3 \pmod{26}$. Check also that `FODVV` becomes `CLASS`:

$$F(5) \to C(2),\ O(14) \to L(11),\ D(3) \to A(0),\ V(21) \to S(18),\ V(21) \to S(18).$$

Hence $k = 3$ and

`WELCOME TO CLASS`

## Problem C (harder)

Ciphertext: `YMJ VZNHP GWTBS KTC OZRUX TAJW YMJ QFED ITL`.
The trigram `YMJ` repeats and often corresponds to `THE`. If so,

$$Y(24) \to T(19) \Rightarrow k \equiv 24 - 19 \equiv 5, \quad \text{so decrypt with } p \equiv c - 5 \pmod{26}.$$

Applying $k = 5$ across the text yields:

`THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG`

---

**Takeaways.**

- Shift ciphers preserve frequency shape; a good guess (E, T, A, O) usually cracks $k$.
- Decryption rule: $p \equiv c - k \pmod{26}$; verify the guess by reading for sensible English.
- Longer texts make frequency clues stronger; short texts can be ambiguous, so test multiple hypotheses.