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: **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 4 5 5 12 20 12 15 9 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: **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:

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