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:

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

$$15 \quad 25 \qquad 7 \qquad 13 \quad 24 \quad 11 \quad 7 \quad 0 \qquad \begin{matrix} 0 \\ 24 \end{matrix} \quad 11 \quad 7 \quad 9 \quad 14 \quad 11$$

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:

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

Our decrypted numbers are:

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

$$8 \quad 18 \qquad 0 \qquad 6 \quad 17 \quad 4 \quad 0 \quad 19 \qquad 19 \quad 4 \quad 0 \quad 2 \quad 7 \quad 4 \quad 17$$

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 **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!