Solutions — Example 4 Affine Cipher

Example Walk-Through

$K \to 10,\ f(p) = (7p + 3) \bmod 26.$

$$f(10) = (7 \cdot 10 + 3) \bmod 26 = 73 \bmod 26 = 21.$$

21 corresponds to V. $\boxed{K \to V}$

—

Problem A

$C = 2.$

$$f(2) = (3 \cdot 2 + 1) \bmod 26 = 7.$$

$7 \to H$. $\boxed{C \to H}$

Problem B

$H = 7.$

$$f(7) = (5 \cdot 7 + 7) \bmod 26 = 42 \bmod 26 = 16.$$

$16 \to Q$. $\boxed{H \to Q}$

Problem C

Encrypt `DOG` with $f(p) = (11p + 8) \bmod 26$.

$$\begin{array}{rclcl} D & = & 3 & \Rightarrow & (11 \cdot 3 + 8) \bmod 26 = 41 \bmod 26 = 15 \to P \\ O & = & 14 & \Rightarrow & (11 \cdot 14 + 8) \bmod 26 = 162 \bmod 26 = 6 \to G \\ G & = & 6 & \Rightarrow & (11 \cdot 6 + 8) \bmod 26 = 74 \bmod 26 = 22 \to W \end{array}$$

$\boxed{\texttt{DOG} \to \texttt{PGW}}$

Reflection Answer

If a shares a factor with 26, then some letters collapse to the same output (no unique inverse), making decryption impossible. Only when $\gcd(a, 26) = 1$ does the cipher remain bijective and reversible.