$c$ - cipher text

$p$ - plain text

$k_1, k_2$ - šifrovacie kľúče

šifrovanie: $c = k_1 \cdot p + k_2 \mod 26$

---

dešifrovanie $c = k_1 \cdot p + k_2 \mod 26$

$$c = k_1 \cdot p + k_2 \quad | + (-k_2)$$

$$c + (-k_2) = k_1 \cdot p + \underbrace{[k_2 + (-k_2)]}_{0}$$

$$c + (-k_2) = k_1 \cdot p \quad | k_1^{-1}$$

$$k_1^{-1} \cdot [c + (-k_2)] = \underbrace{[k_1^{-1} \cdot k_1]}_{1} \cdot p$$

$$p = k_1^{-1} \cdot [c + (-k_2)] =$$

$$= \underbrace{k_1^{-1}}_{k_1'} \cdot c + \underbrace{[k_1^{-1} \cdot (-k_2)]}_{k_2'}$$

---

dešifrovanie: $p = k_1' \cdot c + k_2' \mod 26$

$k_1', k_2'$ - dešifrovacie kľúče

$(-k_2)$ – opačný prvok ku $k_2$ mod 26

$k_2 + (-k_2) \equiv 0 \mod 26$

t. j. $k_2 + (-k_2) = 26$

ak $k_2 = 3$, potom $-k_2 = 23$

lebo $3 + 23 = 26 \equiv 0 \mod 26$

---

$k_1^{-1}$ – inverzný prvok ku $k_1$ mod 26

$k_1 \cdot k_1^{-1} \equiv 1 \mod 26$

napr. ak $k_1 = 5$, potom

$k_1^{-1} = 21$

lebo $5 \cdot 21 = 105 \equiv 1 \mod 26$

$105 = 104 + 1 = 4 \cdot 26 + 1$