

③

$$h) n = 2881 = 43 \cdot 67$$

$$\ell = 3 \text{ sau } 5 \text{ sau } 10$$

$$\phi(n) = 42 \cdot 66 = 2772$$

$$1 < \ell < \phi(n) \text{ și } \gcd(\ell, \phi(n)) = 1$$

$$\begin{array}{l} - \gcd(3, 2772) = 3 \times \\ - \gcd(5, 2772) = 1 \checkmark \quad \left| \Rightarrow \boxed{\ell = 5} \right. \\ - \gcd(10, 2772) = 2 \times \end{array} \quad P_k = (2881, 5)$$

$$c) \ell = 13$$

$$d = 851 \text{ sau } 853 \text{ sau } 856$$

$$de \equiv 1 \pmod{\phi(n)}$$

$$- 851 \cdot 13 \equiv 1 \pmod{2772}$$

$$11063 \equiv 1 \pmod{2772}$$

$$(2772 \cdot 3) + 2747 \equiv 1 \pmod{2772} \oplus (2747 \neq 1)$$

$$- 853 \cdot 13 \equiv 1 \pmod{2772}$$

$$11089 \equiv 1 \pmod{2772}$$

$$(9 \cdot 2772) + 1 \equiv 1 \pmod{2772} \oplus \Rightarrow \boxed{d = 853}$$

$$S_k = (2881, 853)$$

④ - sistem afim

$$c \equiv am + b \pmod{31}$$

$$a = ?$$

$$\begin{array}{l} 1 \leq a < n \\ \gcd(a, n) = 1 \\ 31 \text{ este prim} \end{array} \quad \Rightarrow a \in \{1, 2, \dots, 30\}$$

$$\begin{cases} 22 \equiv 10a + b \pmod{31} \\ 3 \equiv 12a + b \pmod{31} \end{cases} \Rightarrow \begin{cases} 22 - 10a \equiv b \pmod{31} \\ 3 \equiv 12a + b \pmod{31} \end{cases} =$$

$$\Rightarrow 3 \equiv 12a + 22 - 10a \pmod{31}$$

$$3 \equiv 2a + 22 \pmod{31}$$

$$-19 \equiv 2a \pmod{31} \quad (\text{se adaugă } 31 \text{ pentru ca } >$$

$$12 \equiv 2a \pmod{31}$$

$$6 \equiv a \pmod{31} \Rightarrow \boxed{a = 6}$$

$$3 \equiv 12 \cdot 6 + b \pmod{31}$$

$$3 \equiv 72 + b \pmod{31}$$

$$-69 \equiv b \pmod{31}$$

$$24 \equiv b \pmod{31} \Rightarrow \boxed{b = 24}$$

