1

Máme tedy klíče $k, l \in \mathbb{Z}_{27} \setminus \{0\}$ (těleso). Pokud by existovaly 2 zprávy a nějaká dvojice klíčů takové, že se zašifrují na stejný text, pak zobrazení $x \mapsto x \cdot k + l \mod 27$ není prosté pro libovolné x. Dokážeme, že je prosté:
$x, y \in \mathbb{Z}_{27}$
$x \mapsto x \cdot k + l \mod 27$
$y \mapsto y \cdot k + l \mod 27$
$x \cdot k + l \equiv y \cdot k + l \mod 27$
$x \cdot k \equiv y \cdot k \mod 27$ a $NSD(k, 27) = 1$ tedy krátíme
$x \equiv y \mod 27$
$x, y < 27 \rightarrow x = y$
Tedy zobrazení je prosté, tedy nemůže zašifrovat 2 různá písmena na to samé $\rightarrow$ ani text (posloupnost písmen)

2

x - nezašifrované písmeno
první část
$x \mapsto x + a \mod 256 \ (:= y)$
druhá část
$y \mapsto y \cdot c + b \mod 256 \ (:= e)$
e - zašifrované písmeno
po dosazení za y je to vlastně
$x \mapsto (x + a) \cdot c + b \mod 256 \ (:= e)$
Tedy funkci Kas lze vyjádřit vzorcem
$Kas(x, a, b, c) = x \cdot c + (a \cdot c + b) \mod 256$
Tedy to je afinní šifra, kde jeden klíč je $c \in \mathbb{Z}_{256}^*$ a druhý je $(a \cdot c + b) \in \mathbb{Z}_{256}$
Takže to je obyčejná afinní šifra, akorát s trochu jiným klíčem. Bezpečnosti to teda určitě nepomůže.

3

Mějme tedy množinu $\mathbb{A}$ velkých písmen anglické abecedy, tedy $|\mathbb{A}| = 26$. Index koincidence textu x délky n se počítá jako $I_c(x) = \sum_{i \in \mathbb{A}} \frac{f_i \cdot (f_i - 1)}{n \cdot (n-1)}$ z definice, kde f_i značí počet výskytů písmene i v textu x. Ale $\frac{f_i}{n}$ vlastně značí pravděpodobnost toho, že pokud vybereme náhodný znak z x, bude to i. Jelikož text je náhodný ze 26 znaků, potom ta pravděpodobnost je rovna $\frac{1}{26}$. Pokud uvažujeme délku text $n \to \infty$, tak je rozdíl f_i a $f_i - 1$ (i n a $n - 1$) zanedbatelný, tedy můžeme psát $I_c(x) = \sum_{i \in \mathbb{A}} \left(\frac{1}{26}\right)^2$. Tato suma je konečná přes 26 prvků množiny $\mathbb{A}$ tedy $I_c(x) = 26 \cdot \left(\frac{1}{26}\right)^2 = \frac{1}{26}$. Tedy pro libovolný náhodný text x platí $I_c(x) \approx \frac{1}{26}$