1

$x, y \in \mathbb{Z}_{27}$
$x \mapsto x \cdot k + l \mod 27$
$y \mapsto y \cdot k + l \mod 27$
$x \cdot k + l \equiv y \cdot k + l \mod 27$
$x \cdot k \equiv y \cdot k \mod 27$
ale 27 není prvočíslo, tedy platí
$x \equiv y \mod \frac{27}{\gcd(27,k)}$
Tedy pokud například zvolíme $k = 9$, protože $27 = 3 \cdot 9$. l je libovolné, protože se vždy odečte, zvolme tedy $l = 0$.
Poté jdeme "pozpátku".
$x \equiv y \mod 3$ což například platí pro $x = 5$ a $y = 2$
Tedy poté
$x : 5 \mapsto 5 \cdot 9 \equiv 18 \mod 27$
$y : 2 \mapsto 2 \cdot 9 \equiv 18 \mod 27$
Tedy dvě různé zprávy (čísla) se zašifrují na stejné číslo. Dvojice tedy je např. $(9, 0)$. Stejně tak to funguje i pro $k = 3$

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 $I_c(x) = \sum_{i \in \mathbb{A}} (\frac{1}{26})^2$. Tato suma je konečná přes 26 prvků množiny $\mathbb{A}$ tedy $I_c(x) = 26 \cdot (\frac{1}{26})^2 = \frac{1}{26}$. Tedy pro libovolný náhodný text x platí $I_c(x) \approx \frac{1}{26}$