Exercise 1.

Let $a, b, c, d \in \mathbb{Z}$. $a$ is said to divide $b$ if (and only if) there exists some $k \in \mathbb{Z}$ such that $a \cdot k = b$. Notation: $a \mid b$. Prove the following:

(i) $a \mid b$ and $b \mid c \Rightarrow a \mid c$.
(ii) $a \mid b$ and $c \mid d \Rightarrow (ac) \mid (bd)$.
(iii) $a \mid b$ and $a \mid c \Rightarrow a \mid (xb + yc)$ $\forall x, y \in \mathbb{Z}$.

Exercise 2. Decrypt the following ciphertexts and explain your approach. The plaintext messages are in English.

a) Caesar cipher:
   sdcsxceppmsosdxzybdcmxycogfxcovfoegsdrv
   kgcgoxoondyzbydomdyebcovfocgsdrwkdrowkdsnc

b) Affine cipher:
   onhldqrttydxtlgtojkhqtjxctdc

Exercise 3. Consider an affine cipher over an alphabet with $m$ letters.

(a) Determine the number of keys for this cipher. How many keys are there if $m$ is prime? Why is it “better” to use an affine cipher with an alphabet of 23 instead of 26 letters?

(b) Show that the repeated encryption of a plaintext with two affine ciphers is not different from the encryption with one affine cipher using a different key.