(1) Recall that the Caesar Shift Cipher can be considered as a cipher applying modular arithmetic as follows. Let $A = 0, B = 1, \ldots Z = 25$. Suppose m is the character to be encrypted and that k is the number of positions to be shifted, then the ciphertext character c is

$$c \equiv m + k \pmod{26}.$$

An **Affine Cipher** is an encryption scheme with two parameters k and b. Suppose m is the character to be encrypted, then

$$c \equiv km + b \pmod{26}.$$

- **(a)** An Affine Cipher where $b = 0$ is called a **Decimation Cipher**. Create the encryption table for $k = 5$, $b = 0$.
- **(b)** Repeat the same for $k = 6$, $b = 0$. Can $k = 6$ be used for encryption?
- **(c)** Which values of k and b can be used in a Decimation Cipher?
- **(d)** Using the key $k = 15$, $b = 7$. Encrypt the phrase “Scytale is invented by the Spartans.”
- **(e)** If “`THE`” is encrypted to “`FLG`” using an Affine Cipher. What is the key?
- **(f)** How would you break the Affine Cipher?