Exercises: Multiplicative and Affine ciphers

1. Encrypt the word 'tuna' using an multiplicative cipher with key value $a = 3$.

plaintext:	t	u	n	a
in numbers:	19	20	13	0
ap mod 26:	5	8	13	0
ciphertext:	F	I	N	A

   Note: Both a and n were sent to themselves. This is true for all valid key values.

2. Encrypt the word 'rabbit' using an multiplicative cipher with key value $a = 25$.

plaintext:	r	a	b	b	i	t
in numbers:	17	0	1	1	8	19
ap mod 26:	9	0	25	25	18	7
ciphertext:	J	A	Z	Z	S	H

   Note: Multiplying by 25 is a bit tricky. Since $25 \equiv -1 \mod 26$ we could simplify this by multiplying by -1 instead. For example, $(17)(25) \equiv (17)(-1) \equiv -17 \equiv 9 \mod 26$.

3. If the multiplicative encryption key is $a = 3$, what is the decryption key? Since $1 = (9)(3) + (-1)(26)$ then 9 is the decryption key of 3. (And vice versa).

4. If the multiplicative encryption key is $a = 25$, what is the decryption key?

   Since $1 = (-1)(25) + (1)(26)$ then -1 is the decryption key of 25. Or in positive terms, $25 \equiv -1 \mod 26$ is the decryption key of 25. In other words, $25 \times 25 \equiv -1 \times -1 \equiv 1 \mod 26$.

5. Encrypt the word 'zebra' using an affine cipher with multiplicative key $a = 25$ and additive key $b = 25$.

plaintext:	z	e	b	r	a
in numbers:	25	4	1	17	0
$ap \mod 26$:	-25	-4	-1	-17	0
$+b \mod 26$:	0	21	24	8	25
ciphertext:	A	V	Y	I	Z

   Note: This has the effect of reversing the alphabet, so a becomes Z, b becomes Y and so on. Historically, this is known as an Atbash cipher.

6. If the formula for affine encryption is $c \equiv ap + b \mod 26$. What is the decryption formula?

   $p \equiv a'(c + b') \mod 26$, where a' is the inverse multiplicative key and b' is the inverse additive key. Note: $p \equiv a'(c - b) \mod 26$ is also valid.