Exercises: Additive ciphers

1. Encrypt the word 'penguin' using an additive cipher with key value $b = 8$.

plaintext:	p	e	n	g	u	i	n
in numbers:	15	4	13	6	20	8	13
$p + b \mod 26$:	23	12	21	14	2	16	21
ciphertext:	X	M	V	O	C	Q	V

2. Encrypt the word 'tiger' using an additive cipher with key value $b = 13$.

plaintext:	t	i	g	e	r
in numbers:	19	8	6	4	17
$p + b \mod 26$:	6	21	19	17	4
ciphertext:	G	V	T	R	E

Note: This cipher is called ROT13 and is special because it turns the alphabet into 13 pairs. For example, T becomes G, and G become T.

3. Encrypt the word 'monkey' using an additive cipher with key value $b = 25$.

plaintext:	m	o	n	k	e	y
in numbers:	12	14	13	10	4	24
$p + b \mod 26$:	11	13	12	9	3	23
ciphertext:	L	N	M	J	D	X

Note: Adding 25 is the same as subtracting 1 because $25 \equiv -1 \mod 26$.

4. Decrypt the cipher 'JULLIN'. It was encrypted with an additive key of $b = 20$.

ciphertext:	J	U	L	L	I	N
in numbers:	9	20	11	11	8	13
$p - b \mod 26$:	15	0	17	17	14	19
plaintext:	p	a	r	r	o	t

Note: In this case it might be easier to decrypt by adding 6 than by subtracting 20.

5. Decrypt the cipher 'RUDQJH'. It was encrypted with an unknown additive key.

ciphertext:	R	U	D	Q	J	H
in numbers:	17	20	3	16	9	7
$p - b \mod 26$:	14	17	0	13	6	4
plaintext:	o	r	a	n	g	e

For this small example, brute force is the best option. By checking all the possibilities you will find that the key value was $b = 3$.