Exercises: Vigenère ciphers

1. Encrypt the word 'hippopotamus' using a Vigenère cipher with key word '**MAGIC**'.

   Keyword: **M A G I C M A G I C M A**

   Plaintext: h i p p o p o t a m u s

   Ciphertext: T I V X Q B O Z I O G S

   Note: This can be completed using the Vigenère table or the formula $c_i \equiv p_i + k_i \mod 26$.

2. Decrypt the cipertext 'PZRFHETQRHZ' using a Vigenère cipher with key word '**LONDON**'.

   Keyword: **L O N D O N L O N D O**

   Plaintext: e l e c t r i c e e l

   Ciphertext: P Z R F H E T Q R H Z

   Note: This can be completed using the Vigenère table or the formula $p_i \equiv c_i - k_i \mod 26$.

3. The phrase 'mountain goat' was encrypted using a Vigenère cipher and produced the ciphertext 'EIJRKMIAYIPX'. What was the key word?

   Keyword: **S U P E R M A N S U P E**

   Plaintext: m o u n t a i n g o a t

   Ciphertext: E I J R K M I A Y I P X

   Note: This can be completed using the Vigenère table or the formula $k_i \equiv c_i - p_i \mod 26$.

4. We can make the key of a Vigenère cipher longer by repeating two keywords separately. A combined key is then made by adding the letters of the two keywords together.

   In other words, the letters of two keywords k' and k'' make a combined key $k = k' + k'' \mod 26$.

   Here is an example that uses the keywords **JAMES** and **BOND**.

Keyword 1:	**J**	**A**	**M**	**E**	**S**	**J**	**A**	**M**	**E**	**S**	**J**	**A**	**M**	**E**	**S**	**J**
Keyword 2:	**B**	**O**	**N**	**D**	**B**	**O**	**N**	**D**	**B**	**O**	**N**	**D**	**B**	**O**	**N**	**D**
Combined Key :	K	O	Z	H	T	X	N	P	F	G	W	D	N	S	F	M
Plaintext:	s	h	a	k	e	n	n	o	t	s	t	i	r	r	e	d
Ciphertext:	C	V	Z	R	X	K	A	D	Y	Y	P	L	E	J	J	P

   (a) Complete the combined key, using $k = k' + k'' \mod 26$.

   (b) Encrypt the message using the combined key.

   (c) What is the length of the combined key?

   20, lowest common multiple of 5 and 4.

   (d) Show that encrypting a plaintext with k is equivalent to encrypting it twice with k' and k''.

$$c_i = p_i + k_i = p_i + (k'_i + k''_i) = (p_i + k'_i) + k''_i \mod m$$