Exercises: General substitution ciphers

1. Below is cipher A, written as two rows:

plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
ciphertext	Q	J	L	H	K	Z	X	G	Y	W	C	N	B	U	F	T	D	I	E	P	A	O	S	V	R	M

   Use cipher A to encrypt the word 'pelican'.

   TKNYLQU (correction to video solution)

2. Use cipher A above to decrypt the cipher message 'FEPIYLG'.

   ostrich

3. Below is cipher B, written as two rows:

plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
ciphertext	A	D	B	M	S	T	Y	F	C	N	V	E	R	H	G	O	W	J	X	I	U	Z	K	P	L	Q

   We are going to encrypt a word twice. Encrypt the word 'shark' using cipher A followed by cipher B.

   SYWCB

4. The cipher message 'DTUSOVC' was encrypted twice, using cipher A followed by cipher B. What is the message?

   monster

5. In the course we saw there were $26! \approx 4 \times 10^{26}$ possible general substitution ciphers.

   There are currently 7.8 billion people in the word (7,800,000,000).

   There are 31,536,000 seconds in a year.

   If everyone in the world checked one possibility per second, how long would it take to check every possible cipher?

   The number of ciphers checked per person $= \frac{26!}{7{,}800{,}000{,}000} = 51,704,033,477,769,953.$

   Time in years $= \frac{51{,}704{,}033{,}477{,}769{,}953}{31{,}536{,}000} = 1,639,524,146.$

   It would take the world approximately 1.6 billion years to check them all.