Exercise 1. Show that the following language is in P:

$$\texttt{RELATIVELY-PRIME} = \{\langle x, y\rangle \mid x \texttt{ and } y \texttt{ are integers, } gcd(x, y) = 1\}$$

Exercise 2. A Caesar cipher is a simplified encryption protocol in which all letters are shifted $0 < k < 26$ positions *mod* 26, e.g. when $k = 3$:

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
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

To use this encryption method, look up the substitution for each letter, like this:

SMITH COLLEGE→ VPLWK FROOHJH

Show that this encryption scheme can be broken in $O(n)$ where n is the length of the message.

Exercise 3. Consider the language:

$$VERTEX - COVER = \{\langle G, k\rangle \mid G \texttt{ is a graph that has a vertex cover of size } k\}$$

where a **vertex cover** is a set of k vertices such that every edge in the graph touches at least one of the vertices.

(a) Draw a diagram of a graph on 10 vertices with an **vertex cover** of size 5.

(b) Prove that $VERTEX - COVER$ is NP-complete.

Exercise 4. Consider the language:

$$SET - COVER = \{\langle U, S, k\rangle \mid U \texttt{ is a set of elements } \{1, 2, ..., n\} \texttt{ (the "universe"), } S \texttt{ is a set of } m \texttt{ subsets where } \bigcup S = U, \texttt{ and } S \texttt{ contains a set cover of size } k\}$$

where a **set cover** is a set of k subsets $\in S$ such that every element in U is contained in at least one of the selected subsets.

(a) Draw a diagram of a universe with 10 elements, partitioned into 5 subsets with a **set cover** of size 3.

(b) Prove that $SET - COVER$ is NP-complete.

References
