Problem of the Week
Problem A and Solution
Secret Message

Problem

Andrea wants to send secret messages to her friends. She creates a grid and fills it with the letters of the alphabet in order. She uses letters to identify the columns of the grid and numbers to identify the rows of the grid. Then she sends a message by using the positions of the letters and spaces in the grid.

To make it harder for people to decode her messages, she uses different sized grids for different messages, and sometimes she leaves some blank spaces at the beginning of the grid. For example, this is a grid with 8 columns and 3 blank spaces at the beginning:

	A	B	C	D	E	F	G	H
1				a	b	c	d	e
2	f	g	h	i	j	k	l	m
3	n	o	p	q	r	s	t	u
4	v	w	x	y	z			

A) Using the grid above, decode the message: `H2D1G3C2C1D2F3F4A2H3A3`

B) Without seeing the particular grid Andrea uses, she can still send her friends secret messages that they can decode if they know how many columns are in the grid and how many blank spaces are at the beginning of the grid. We call this kind of information the key. So for the grid above, the key is 83.

If the key is 62, the grid would have six columns and two blank spaces at the beginning. How do you encode the message: **this is secret** using the key 62?

C) Decode the message `D1D4A6B4A5A4C2D4B1B4D2A6` using the key 51.

Solution

A) The decoded message is: **math is fun**

B) Here is the grid that matches the key 62:

	A	B	C	D	E	F
1			a	b	c	d
2	e	f	g	h	i	j
3	k	l	m	n	o	p
4	q	r	s	t	u	v
5	w	x	y	z		

We could use any of `A1`, `B1`, `E5`, or `F5` for the spaces in the message. The letters can only be encoded in one way. So here is one solution for the encoding of **this is secret**: `D4D2E2C4A1E2C4B1C4A2E1B4A2D4`.

C) Here is the grid that matches the key 51:

	A	B	C	D	E
1		a	b	c	d
2	e	f	g	h	i
3	j	k	l	m	n
4	o	p	q	r	s
5	t	u	v	w	x
6	y	z			

So the decoded message is: **cryptography**

Teacher's Notes

Cryptography is the study of encoding private data. It is a practice that goes back thousands of years. In most cryptographic schemes, encoding and decoding a message requires a *key*. One of the trickiest parts of sending secret messages is that both the sender and the receiver need to know a key in order to encode and decode the message. The question becomes how do you transmit the key without someone finding out what it is.

Today, most data online is secured using *public key encryption*. In this case, the receiver has two keys: a public key and a private key. The receiver provides the sender with a public key that the sender uses to encode the message. However, without the private key, it would be almost impossible to decode the message - even for the sender.

Here is one way to think of public key cryptography. If I want you to be able to send me a secret message, I can send you a box with an open (public) lock. You can put the message in the box and lock it. After it is locked, nobody except the person with a (private) key can read the message. Now you can safely send me a secret message.