

## SECRET CODES

Last time we talked about error-detecting codes. These were codes that added some additional information to a “message” (like the UPC information) in such a way that certain types of copying errors would be detected.

Today we want to look at a different kind of code called a secret code. Now we want to encode messages in such a way that only the intended recipients can figure out the message. The study of secret codes is called *cryptology*. Obviously this is tremendously important for electronic financial transactions (we don’t want anyone else to have access to our money at the ATM) and for national security (we can’t have enemies eavesdropping on our war plans). In fact, the National Security Agency of the United States is the single largest employer of mathematicians in the country, and one of the main things they study is code-making and code-breaking.

Many of the coding schemes use modular arithmetic. Let’s look at two of them.

### Secret Key Cryptography & the Caesar Cipher

Let’s start out with an old coding scheme. It is said that this scheme was used by Julius Caesar to code messages to his generals so that if the messenger were overtaken, the message would remain secret. Of course, the general knew the scheme and could recover the message if the messenger made the trip alive.

Here is the scheme. First the message is converted from letters to numbers using the following table.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

1. Convert the message “I LOVE MATH!” into its 9-number code. Notice that the blanks and punctuation are ignored.

Next, some number (Caesar reportedly used 3) was added to each number in the code. (Of course, we should work mod 26 – why?) This number (3 for Caesar) is called the **encoding key**.

2. Convert the 9-number code into a new 9-number code by adding 3 (mod 26) to each of the 9 numbers.

Finally, the numeric encoding was converted back to a letter encoding (using the table again).

3. Convert the 9-number code into a new 9-number code by adding 3 (mod 26) to each of the 9 numbers.

4. It is possible to describe this process without using any numbers. Explain how to encode “I LOVE MATH!” without using any numbers.

5. MORE MESSAGES. Encode each of these messages using a Caesar cipher with encoding key 3.

- a) “HELLO”
- b) “GO KNIGHTS!”
- c) “TO INFINITY AND BEYOND!”

Now redo them with an encoding key of 9.

OK, we're half done. We can *encode* messages. But how does the recipient decode them? You can probably figure this one out.

6. Decode the following messages:

- a) FRUUHFW
- b) BRX JRW LW
- c) LWLVJRRG
- d) QJAMNA FRCQXDC TNH

## Public Key Cryptography & RSA

In the Caesar cipher, once you know the encoding key, it is easy to figure out how to decode.

7. Describe how to decode if the encoding key ( $e$ ) is a) 3, b) 7, c) 9.

8. If your method for decoding involved subtraction (or going backwards), try to find another (equivalent method) that uses addition (or going forwards).

So decoding and encoding are the same thing (but with different keys)! The problem is that once someone knows the encoding key ( $e$ ), they can easily figure out the decoding key ( $d$ ). This has some big disadvantages. In particular, how does the sender tell the recipient what key to use? (If you send it with the messenger, you might as well let the messenger know the message.)

Now we want to find a system such that knowing  $e$  is not enough to figure out  $d$ . That way, we can receive messages by posting our encoding key ( $e$ ) in a directory. Anyone who wants to send a message can simply encode it with our **public key**. Of course, we keep the decoding key a secret and use it to decode the message. We call this the **private key**.

Let's suppose we want to send numbers as messages (that saves us the conversion back and forth to letters, but we could do that if we needed to.) Our directory would look like this:

<u>Name</u>	<u>modulus</u>	<u>public key</u>	<u>private key</u>
John Q Public	26	5	only John knows
Jan Doe	65	5	only Jane knows
Sam I Am	21	7	only Sam knows

To send Jane a message, we work mod 65 and encode with  $e = 5$ . Of course, we can't use the Caesar cipher, because then everyone would know how to decode, and we only want Jane to be able to decode. So what can we do?

RSA is one particular system that is amazingly like the Caesar cipher. The biggest difference is that we will use multiplication (actually exponentiation) instead of addition. So here is the scheme.

To send a message to Jane we take our number (let's call it  $M$  for message) and raise it to the power 5 (mod 65). So to send Jane the number 10, we code it as

$$10^5 \pmod{65} \equiv 100000 \pmod{65} \equiv 30 \pmod{65}$$



## Solutions

**4** I LOVE MATH = L ORYH PDWK

**5** Here are the solutions using keys of 3, 6, and 9 to encode:

- HELLO: KHOOR, NKRRU, QNUUX
- GO KNIGHTS: JR NQLJKWV, MU QTOMNZY, PX TWRPQCB
- TO INFINITY AND BEYOND: WR LQILQLWB DQG EHBRQG, CX RWORWRCH JWM KN-HXWM, ZU OTLOTOZE GTJ HKEUTJ,

**6** CORRECT, YOU GOT IT, ITISGOOD, HARDER WTHOUT KEY ( $e = 9$ )

**9**  $2^5 = 32 \equiv 32 \pmod{65}$ ,  $3^5 = 243 \equiv 48 \pmod{65}$ ,  $4^5 = 1024 \equiv 49 \pmod{65}$ ,  $10^5 = 100000 \equiv 30 \pmod{65}$ ,

**10**  $30^{25}$  means multiply  $30 \times 30 \times 30 \cdots \times 30$ . (That's twenty-five 30's multiplied together.) We can do this in five groups of 5 30's:

$$\begin{aligned} 30^{25} &= (30 \times 30 \times 30 \times 30 \times 30) \times (30 \times 30 \times 30 \times 30 \times 30) \times (30 \times 30 \times 30 \times 30 \times 30) \\ &\quad \times (30 \times 30 \times 30 \times 30 \times 30) \times (30 \times 30 \times 30 \times 30 \times 30) \\ &= 30^5 \times 30^5 \times 30^5 \times 30^5 \times 30^5 \\ &= (30^5)^5 \end{aligned}$$