Cryptography and Number Theory

Fvb mpnbylk vba aol jvkl

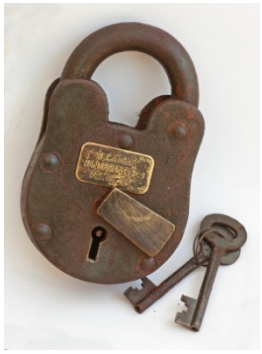
Can you read the secret message in the box above? With a little mathematical cryptography (Or a Chex secret decoder ring) we can!

Cryptography is the study of methods of converting a string of characters into an indistinguishable string that can later be converted back into the original message.

Today, this is a crucial part of much of our use of information that is passed through computers. Let's explore some of the history and motivation behind Cryptography.

How Would You Send your Message?

When Napoleon Bonaparte needed to communicate his secret battle plans, he turned to mathematicians to create a secret code that his enemies could not decrypt. His Great Paris Cipher successfully kept the Emperor's secret's safe for about a year until another mathematician broke the code.



However, before this secret code was developed, messages were transported by hand with locks and keys.

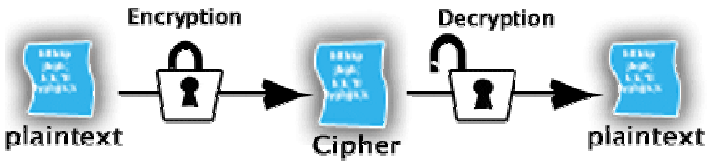
So, suppose you are Napoleon Bonaparte and you need to get a message to your general 10 miles away. How can you secure your message(s) in a way so that no one except you and the general can read it? You have locks and boxes at your disposal with which to keep the message secret.

A. Come up with a way using locks, boxes, and keys that the message can be transported and no one (including the courier) can have access to it.

B. Now suppose that you have an Ally General who you have not met before, and you want to send a secret message to them in the battle field. How could you use locks, boxes, and keys to get the message to him without anyone being able to read it in-between?

The Idea of Cryptography

The goal of cryptography is to transform a *plaintext* message into a *ciphertext* that is difficult to understand. Then there is a process to *decipher* the ciphertext to recover the original message.



So, what does math have to do with it?

Every letter (and symbol) can be represented by a number as seen in the table below.

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

We start with the original message called the plain text:

Plaintext: "Secret"
Encode the message "Secret" using numbers:

Now, we will encrypt it using a simple cipher, called a *Shift cipher*. To do this, let's **add 10** to each number and rewrite the numbers

Encryption Shift the numbers by adding 10:

Now change the numbers back into text. We call this the Cyphertext

Cyphertext:

What problem do you run into?

How can we remedy this?

Shift Cipher

For this, we need to use *modular arithmethic* using something called *congruences.*

Number Theory and Congruences

Number Theory is the study of mathematics that is mainly concerned with the properties of Integers. *Modular arithmetic*, or congruences are one of the most useful areas of Number Theory, and a key component of Cryptography.

More on Congruences

Definition. Let a, b, n be integers with $n \neq 0$. We say that

$$a \equiv b \pmod{n}$$

(read: *a is congruent to b mod n*) if $a - b$ is a multiple of n.

Another way to say this is that $a \equiv b \pmod{n}$ if a and b differ by a multiple of n. We can show this as $a = b + nk$ for some integer k (positive or negative.)

Examples

$35 \equiv 5 \pmod{10}$, $47 \equiv 1 \pmod{2}$, $-12 \equiv 3 \pmod{5}$, $5 \equiv 5 \pmod{7}$

Consider these:

Proposition. Let a, b, c, n be integers with $n \neq 0$

1. $a \equiv 0 \pmod{n}$ *if and only if* $n|a$. (that is… n divides a)
2. $a \equiv a \pmod{n}$.
3. $a \equiv b \pmod{n}$ *if and only if* $b \equiv a \pmod{n}$.
4. *If* $a \equiv b$ *and* $b \equiv c \pmod{n}$, *then* $a \equiv c \pmod{n}$

Can you verify (i.e. prove) these?

Back to the cipher: Now we can find the cyphertext from our "Secret " Message using (mod 26)

Encryption Numbers (copy from above):

Convert (mod 26):

Cyphertext:

More on Numberphile

Challenge Problem for the month:

In medieval times, the inhabitants of a remote village decided to put a number of locks on a giant chest to protect the village valuables from marauding thieves.

For additional security, the villagers created enough locks and keys so that no two people from the village had enough keys to open the chest, but amongst them any group of three people always had enough keys to open all the locks on the chest.

How many locks, and how many keys, are needed to insure that no two people can open the chest, but any three people can?