CMI Math Circle

Synopsis for August 2 2026

1 Secret codes

In this first session of the CMI math circle, we explored the shift cipher.

We introduced the following encoding for the English alphabet to create as well as decipher our codes:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

V	W	X	Y	Z
21	22	23	24	25

Then we introduced some terminology to aid the conversation:

- ***Encryption*:** the process of converting plaintext to coded form (or ciphertext).
- ***Decryption*:** this is the opposite of encryption, that is, its the process of converting ciphertext back to plaintext so everyone can understand it.
- ***Key*:** this is the number used to perform the encryption process.

We encouraged students to try out encryption and decrytion using different shifts, and also to try and figure out the key when only the ciphertext is given (and it is known that the shift cipher was used).

1. Encrypt the plaintext 'cryptography is cool' with the key 7.
2. Encrypt the plaintext 'this is the message' with the key -5.
3. Decrypt the ciphertext 'YMNX NX JFXD' using the key -5.
4. Decrypt the ciphertext 'XYFD XFKJ JSJRD PSTBX' by working out the key.

By the end of the last exercises a number of students had figured out that there are only 25 possible shifts. Some students had worked out strategies such as:

- first figure out what English letter occurs most often and assign it to the ciphertext letter occurring most oftem
- looks at pairs of letter occurring more often in the ciphertext and try to figure them out first.

2 More secret codes

We noted that in the shift cipher, every letter was moved by adding a fixed number. Next we tried to create a cipher my multiplying each plaintext number by a fixed number. Through various small exercises, students were encouraged to figure out the differences caused by using keys such as 3 versus keys such as 2 for creating a cipher by multiplication.

Some exercises we used are listed below:

1. We begin with the key 3.

   Complete the following table.

Plaintext letter									
Plaintext number 0	1	2	3	4	5	6	7	8	9
Ciphertext number									
Ciphertext letter									

2. Encrypt the following words using the multiplication rule with key 3.

   (a) CAT
   (b) DOG
   (c) MATH
   (d) CIRCLE

3. Repeat Exercise 1 using the key 2.

Plaintext letter									
Plaintext number 0	1	2	3	4	5	6	7	8	9
Ciphertext number									
Ciphertext letter									

   What do you notice? Do any two different plaintext numbers give the same ciphertext?

4. Why is this a problem?

5. Investigate the following multiplication keys.

   For each key, decide whether every ciphertext letter appears exactly once. If it does, we can say that key is *safe*.

Key	2	3	4	5	6	7	8	9	10	11
Is it safe?										