Ciphers!

Gbjswjfx Fmfnfoubsz Nbui Dmvc

~~Fairview Elementary Math Club~~

https://kaplandm.github.io/FVE/

Caesar cipher

The previous slide used a Caesar cipher with +1 shift. This was used by Julius Caesar's great-nephew Augustus, the first emperor of the Roman Empire. Julius Caesar often used a +3 Caesar cipher: replace A with D, replace B with E, etc.

Who wrote the following ciphertext, Julius Caesar or Augustus? What does it say?

- Wkh glh lv fdvw.

Who wrote the following ciphertext, and what does it say?

- J gpvoe Spnf b djuz pg csjdlt boe mfgu ju b djuz pg nbscmf.

Write your own with any shift (+2, +5, etc.); see if an adult can decipher it without knowing the shift!

Rail fence cipher: encoding

This is one I learned recently. First, the sender and receiver must know the number of rows; here I use 3. To encode the message, write it out in a zig-zag in 3 rows like this:

F				V				*				H				U	
	A		R		I		W		M		T		*		L		B
		I				E				A				C			

The encrypted message takes the first row of letters (`FV*HU`), then the second (`ARIWMT*LB`), then the third (`IEAC`), ignoring blanks. Altogether, `FV*HUARIWMT*LBIEAC`.

Your turn!

1. Encode a message with 3 rows; see if an adult can decode it!
2. Encode a message with a different number of rows.

Rail fence cipher: decoding

To decode a message, make the 3-row grid, and put a little dot for each letter of the message. Then replace your dots with the letters in the message, left to right, row by row.

Example message: `IR*GEAE`

Dots:

.				.		
	.		.		.	
		.				.

Fill in the first 2 letters (`IR`) in the top rows' dots; then fill in the next 3 letters (`*GE`) in the middle row; then the last 2 (`AE`) in the bottom row:

I				R		
	*		G		E	
		A				E

Now decode `MAER*LE.L` and then another student's message.

Route cipher

To encode: write your message in a grid with 7 columns, then write out the 1st column of letters, then 2nd, etc.

T	H	I	S	*	I	S
A	N	*	E	X	A	M
P	L	E	*	C	I	P
H	E	R	*	*	*	*

$\Longrightarrow$ TAPHHNLEI*ERSE**
*XC*IAI*SMP*

To decode: write the message text column by column in a grid with 7 columns, then read it (left to right).

I*USAT**ATPTHEIIROSMN $\Longrightarrow$

I	S	*	T	H	I	S
*	A	*	P	E	R	M
U	T	A	T	I	O	N

Try it yourself: encode a message and try to decode another student's

Katakana

This table shows the (approximate) sounds corresponding to different characters from part of the katakana alphabet in Japan. The top row corresponds to vowel-only sounds; the others are the consonant sound followed by the vowel sound. For example, in row “k” column “a” the sound “ka” is encoded as カ. Note “i” is like a long E sound, and “e” is like a long A sound (and “a” is like ah).

Can you decode these English words/names?

アメリカ

ペン

カメラ

コピ

ピアノ

ラヂオ

ゼロ

	a	i	u	e	o
(none)	ア	イ	ウ	エ	オ
k	カ	キ	ク	ケ	コ
g	ガ	ギ	グ	ゲ	ゴ
s	サ	シ	ス	セ	ソ
		shi			
z	ザ	ジ	ズ	ゼ	ゾ
t	タ	チ	ツ	テ	ト
		chi	tsu		
d	ダ	ヂ	ヅ	デ	ド
n	ナ	ニ	ヌ	ネ	ノ
h	ハ	ヒ	フ	ヘ	ホ
			fu		
b	バ	ビ	ブ	ベ	ボ
p	パ	ピ	プ	ペ	ポ
m	マ	ミ	ム	メ	モ
y	ヤ		ユ		ヨ
r	ラ	リ	ル	レ	ロ
w	ワ	ヰ		ヱ	ヲ

n by itself is ン

Make your own

Make your own cipher!

Explain it to another student, and see if you can successfully send and receive a message that an adult cannot understand!