

Break the Code

Getting into Cryptography



What is encryption?

Encryption is like a secret code that keeps information safe and private when we need to send it to other people.

It is used to protect sensitive information, like passwords, credit card numbers, or personal messages.

Can you think of other examples of sensitive information that needs to be encrypted?







28cQmF#%B2WG^LJ What is encryption? ol@5v*1

In computer terms, encryption works in a similar way.

Instead of a treasure box, we use *algorithms* to scramble the message into a secret code.

This code looks like a jumbled mess of letters and numbers.



What is cryptography? J MPWF UIF DPMPVS CMVF (a message in code)

cryptogram

How can we decrypt this cryptogram?



J MPWF UIF DPMPVS CMVF I LOVE THE COLOUR BLUE

A	В	С	D	E	F	G	Н		J	K	L	Μ	Ν	0	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z
В	С	D	Е	F	G	Н	I	J	K	L	Μ	N	0	Ρ	Q	R	S	Т	U	V	W	X	Y	Ζ	A



To encrypt messages, you need a cipher and a key.

9&QMF#%B2w

a scrambling procedure that jumbles up the information the (secret) information needed to unscramble the information



Caesar Cipher





Can you figure out this secret message? The key is **3**.

OHPRQV





Can you figure out this secret message? The key is **3**.

LEMONS





Can you figure out this secret message? The key is **3**.

LEMONS

A	В	С	D	E	F	G	Н		J	κ	L	М	N	0	Ρ	Q	R	S	т	U	V	W	Х	Y	Ζ
D	Е	F	G	H	I	J	K	L	Μ	Ν	0	Ρ	Q	R	S	Т	U	V	W	Х	Y	Ζ	А	В	С



Now you try!

- Follow the worksheet or create a cryptogram of your own.
- Ask a friend to decode your message.
- Don't forget to give them your key
- Don't forget to remove spaces and punctuation so they don't guess it right away ⁽³⁾



Decoding without a Key

There are over *400 septillion* ways to encrypt messages using the Caesar Cipher.

It's a lot easier to decode these kinds of messages, even if you don't know the key:

- Trying out all of the possible options (brute force)
- Looking for common words or letters (frequency analysis)



----- (The word you want to encode.)

														PLA	INT	EXT	r													
			Α	В	С	D	Ε	F	G	Η	T	J	K	L	Μ	Ν	0	Ρ	Q	R	S	Т	U	V	W	X	Y	Ζ		
1		Α	Α	В	С	D	E	F	G	Н	Т	J	K	L	М	Ν	0	Р	Q	R	S	Т	U	۷	W	Х	Y	Ζ		1
2		В	Ζ	Α	В	С	D	Ε	F	G	Н	Ι	J	Κ	L	Μ	Ν	0	Р	Q	R	S	Т	U	۷	W	X	Υ		1
3		С	Y	Ζ	Α	В	С	D	Ε	F	G	Η	Ι	J	K	L	Μ	Ν	0	Р	Q	R	S	Т	U	۷	W	X		1
4		D	Х	Y	Ζ	Α	В	C	D	E	F	G	Н	Ι	J	К	L	Μ	Ν	0	Р	Q	R	S	Т	U	V	W		1
5		Ε	W	X	Y	Ζ	Α	В	С	D	Ε	F	G	Η	Ι	J	K	L	Μ	Ν	0	Р	Q	R	S	Τ	U	V		ENCODED TE
6		F	V	W	Х	Y	Z	Α	В	C	D	Ε	F	G	Н	1	J	K	L	Μ	Ν	0	Р	Q	R	S	Т	U		
7		G	U	V	W	Х	Y	Z	Α	В	С	D	E	F	G	Η	Ι	J	K	L	Μ	Ν	0	Р	Q	R	S	Τ		1
8		Η	Т	U	V	W	X	Y	Ζ	Α	В	С	D	E	F	G	Н	Ι	J	K	L	М	Ν	0	Р	Q	R	S		1
9		1	S	Т	U	V	W	X	Y	Ζ	Α	В	С	D	E	F	G	Η	I	J	K	L	Μ	Ν	0	Р	Q	R		
10		J	R	S	Τ	U	V	W	Х	Y	Ζ	Α	В	С	D	E	F	G	Н	Ι	J	K	L	Μ	Ν	0	Р	Q		1
11		К	Q	R	S	Т	U	V	W	Х	Y	Ζ	Α	В	C	D	E	F	G	Η	Ι	J	K	L	Μ	Ν	0	Ρ		
12	KΕ	L	Р	Q	R	S	T	U	V	W	Х	Y	Ζ	Α	В	С	D	E	F	G	Η	Ι	J	K	L	Μ	Ν	0		
13		Μ	0	P	Q	R	S	T	U	V	W	Х	Y	Z	Α	B	C	D	E	F	G	Η	Ι	J	K	L	M	Ν		
14		Ν	Ν	0	Р	Q	R	S	Т	U	V	W	X	Y	Z	Α	B	С	D	E	F	G	Н		J	K	L	Μ		
15		0	Μ	N	0	Р	Q	R	S	Т	U	V	W	X	Y	Z	Α	В	C	D	E	F	G	Η	Ι	J	K	L		
16		Ρ	L	Μ	N	0	P	Q	R	S	Т	U	V	W	X	Y	Z	Α	B	C	D	E	F	G	Н	1	J	K	_	
17		Q	K	L	M	N	0	P	Q	R	S	Т	U	V	W	X	Y	Z	Α	B	C	D	E	F	G	H	Ι	J		
18		R	J	K	L	Μ	N	0	Р	Q	R	S	T	U	V	W	X	Y	Z	Α	B	C	D	E	F	G	H	Ι		
19		S	Ι	J	K	L	M	N	0	P	Q	R	S	T	U	V	W	X	Y	Z	Α	B	C	D	E	F	G	Η		
20		Т	Н		J	K	L	Μ	N	0	Р	Q	R	S	Т	U	V	W	X	Y	Ζ	Α	В	C	D	E	F	G		1
21		U	G	H	I	J	K	L	M	N	0	Ρ	Q	R	S	Т	U	V	W	X	Y	Z	Α	B	С	D	E	F		1
22		V	F	G	Η	1	J	K	L	Μ	N	0	P	Q	R	S	T	U	V	W	X	Y	Ζ	Α	B	C	D	E		1
23		W	E	F	G	Η		J	K	L	M	Ν	0	Р	Q	R	S	Т	U	V	W	X	Y	Ζ	Α	B	C	D		1
24		X	D	E	F	G	H		J	K	L	Μ	N	0	P	Q	R	S	T	U	V	W	Х	Y	Ζ	Α	B	C		I I
25		Y	C	D	E	F	G	Η		J	K	L	M	N	0	Р	Q	R	S	T	U	V	W	X	Y	Z	A	B		I I
26	1	Ζ	B	C	D	E	F	G	H		J	K	L	Μ	Ν	0	Р	Q	R	S	T	U	V	W	Х	Y	Z	Α		1



													PLA	INT	EXT												
		Α	В	С	D	Ε	F	G	Н	I	J	K	L	Μ	Ν	0	Ρ	Q	R	S	Т	U	۷	W	X	Y	Ζ
	Α	Α	В	С	D	Ε	F	G	Η	Т	J	Κ	L	Μ	Ν	0	Р	Q	R	S	Т	U	۷	W	Х	Y	Ζ
	В	Ζ	А	В	С	D	Ε	F	G	Н	Ι	J	Κ	L	Μ	Ν	0	Р	Q	R	S	Т	U	۷	W	Х	Y
	С	Υ	Ζ	Α	В	С	D	Ε	F	G	Η	Т	J	Κ	L	Μ	Ν	0	Р	Q	R	S	Т	U	۷	W	Х
	D	Х	Y	Ζ	Α	В	С	D	Ε	F	G	Η	Ι	J	K	L	Μ	Ν	0	Р	Q	R	S	T	U	۷	W
	Ε	W	Х	Y	Ζ	Α	В	С	D	Ε	F	G	Η	Ι	J	K	L	Μ	Ν	0	Р	Q	R	S	Τ	U	V
	F	۷	W	Х	Y	Ζ	Α	В	С	D	Ε	F	G	Η	Ι	J	K	L	Μ	Ν	0	Р	Q	R	S	Τ	U
	G	U	۷	W	X	Y	Ζ	Α	В	С	D	Ε	F	G	Η		J	K	L	Μ	Ν	0	Р	Q	R	S	Τ
	Η	Τ	U	V	W	Х	Y	Ζ	Α	В	С	D	E	F	G	Η	1	J	K	L	Μ	Ν	0	Р	Q	R	S
	1	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	1	J	K	L	M	N	0	Р	Q	R
	J	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	1	J	K	L	M	N	0	P	Q
	K	Q	R	S		U	V	W	X	Y	Z	A	B	C	D	E	F	G	Н		J	K	L	M	N	0	P
Ψ		P	Q	K	5		U	V	VV	X	Y	Z	A	B		D	E		U F	Н	<u>/</u> _	J	K	L	IVI	N	0
			۲ 0	Q	ĸ	5		U	V	W	X	Y	Z	A	B		D	E		G	H	1	J	K	L		N
		IN N/I	N	P	Q D	ĸ	С С	۱ د	U T	V	VV	X \\\/	Y	Z V	A 7	B	C D	C	E		G	н		J	K	L	
	Р			N	P 0	Q D		D D	۱ د	т	V	vv	^ \//	T V	Z V	A 7			0		г с	G C	п С	L L	1	N 1	Ľ
	г О	ĸ		M	N		D	0	R	s	т		VV	~ W/	Y	V	A 7	٨	R	C	L D	F	F	G	Ч	J	N I
	R		ĸ		M	N	0	P	0	R	S	т	V U	V	w	ı x	γ	7	Δ	B	C	D	F	F	G	ч Н	1
	S	1	1	K	1	M	N	0	P	0	R	S	т	Ŭ	V	w	X	γ	7	Δ	B	C	D	F	F	G	H
	т	H	1	J	ĸ	L	M	N		P	0	R	S	T	U	v	W	X	Y	7	A	B	C	D	Ē	F	G
	U	G	H	-	J	K	L	M	N	0	P	Q	R	S	T	U	V	W	X	Y	Z	A	В	C	D	E	F
	v	F	G	Η	Τ	J	К	L	М	N	0	P	Q	R	S	Т	U	٧	W	Х	Y	Ζ	Α	В	С	D	Ε
	W	Ε	F	G	Н	T	J	Κ	L	М	Ν	0	Ρ	Q	R	S	Т	U	۷	W	Х	Y	Ζ	Α	В	С	D
	X	D	Ε	F	G	Η	Ι	J	Κ	L	М	Ν	0	Р	Q	R	S	Т	U	V	W	Х	Y	Ζ	Α	В	С
	Y	С	D	Ε	F	G	Η	T	J	Κ	L	М	Ν	0	Р	Q	R	S	Т	U	۷	W	Х	Y	Ζ	Α	В
	Ζ	В	С	D	Ε	F	G	Η	T	J	Κ	L	Μ	Ν	0	Р	Q	R	S	Т	U	۷	W	Х	Y	Ζ	А





Encode "SOUND" using the key "L"

S	0	U	Ν	D
н	D	J	С	S









Vigenère Cipher: Polyalphabetic Cipher

Encode "ISLAND" using the key "ORANGE"

	S	L	А	Ν	D
0	R	A	Ν	G	Е
U	В	L	N	Н	Z

													PLA	INT	EXT												
		Α	В	С	D	E	F	G	Η	I	J	К		М	Ν	0	Ρ	Q	R	S	Т	U	۷	W	X	Y	Ζ
	Α	А	В	С	D	Ε	F	G	Н	Т	J	K	L	Μ	Ν	0	Р	Q	R	S	Т	U	V	W	Х	Y	Ζ
	В	Ζ	Α	В	С	D	Ε	F	G	Η	Т	J	K	L	Μ	Ν	0	Р	Q	R	S	Τ	U	۷	W	Х	Υ
	С	Y	Ζ	Α	B	C	D	E	F	G	Η	1	J	K	L	Μ	N	0	Р	Q	R	S	Τ	U	V	W	X
	D	X	Y	Z	A	B	C	D	E	F	G	H	1	J	K	L	M	N	0	P	Q	R	S	T	U	V	W
	E	W	X	Y	2	A	В	C	D	E	F	G	H	1	J	K	L	IVI	N	0	P	Q	R	5		U	V
	F	V	W	X	Y	Z	A	B		D	E	F	G	H		J	K	L	IVI	N	0 N	P	Q	K	5	l c	U
	Ч	T		VV	×	T Y	V	7	Δ	R	C	D	F	E	G	Ц	J		K		M	N	P 0	Q D	K O	D D	S
	п 1	S	Т		V	∧ ₩	X	V	A 7	Δ	R	C	D	F	F	G	н	1		K		M	N	г 0	P		B
		R	S	т	V U	V	w	ı x	Y	7	Δ	R	C	D	F	F	G	H	1	I I	ĸ		M	N	0	P	0
	ĸ	0	R	S	Т	U	V	w	X	Ŷ	7	A	B	C	D	F	F	G	H	1		K	1	M	N	0	P
Ł	L	P	Q	R	S	T	·U	v	W	X	Y	Z	A	B	C	D	Ē	F	G	H	1	J	K	L	M	N	0
₹ I	м	0	P	Q	R	S	Т	U	V	W	Х	Y	Ζ	Α	В	С	D	E	F	G	Н	1	J	Κ	L	Μ	Ν
	N	N	0	Р	Q	R	S	Т	U	V	W	Х	Y	Ζ	А	В	С	D	Ε	F	G	Η	Ι	J	К	L	Μ
	0	Μ	Ν	0	Р	Q	R	S	Т	U	V	W	Х	Y	Ζ	А	В	С	D	Ε	F	G	Н	Ι	J	Κ	L
	Ρ	L	Μ	Ν	0	Р	Q	R	S	T	U	۷	W	Х	Y	Ζ	Α	В	С	D	Ε	F	G	Η	Ι	J	Κ
	Q	К	L	Μ	Ν	0	Р	Q	R	S	Т	U	۷	W	Х	Y	Ζ	Α	В	С	D	Ε	F	G	Η	Ι	J
	R	J	Κ	L	Μ	Ν	0	Р	Q	R	S	Τ	U	۷	W	Х	Y	Ζ	Α	В	C	D	Ε	F	G	Η	Т
	S		J	Κ	L	Μ	Ν	0	Р	Q	R	S	Τ	U	V	W	Х	Y	Ζ	A	В	С	D	Ε	F	G	Η
	Τ	Η	1	J	К	L	Μ	Ν	0	Р	Q	R	S	Τ	U	V	W	Χ	Y	Ζ	Α	B	C	D	Ε	F	G
	U	G	H	1	J	K	L	M	N	0	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	С	D	E	F
	V	F	G	H	1	1	K	L	M	N	0	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	W	E	F	G	H	1	J	K	L	M	N	0	P	Q	R	5		U	V	W	X	Y	Z	A	В	C	D
	X	D	E	F	G	H	1	J	K	L	IVI	IN N	0 N	P 0	Q	K	5 D	l c	U	V	W	X	Y	Z	A 7	B	
	T 7			E	F	G	H		1	K	Ľ	IVI	IN M	N	P	Q D	ĸ	D	l c	U T	V	VV V		Y	Z V	A 7	В
i	2	В	C	υ	E	F	0	н	1	1	ĸ	L	IVI	IN	0	۲	ų	к	3		U	V	vv	^	T	2	А



How to Decode using a Vigenère Cipher

Decode "QKHMN" using the key "MOUSE"

Q	K	Н	Μ	Ν
Μ	0	U	S	Е
С	Y	В	E	R

				-									PLA	INT	EXT												
		Α	В	С	D	Е	F	G	Η	Т	J	K	L	Μ	Ν	0	Ρ	Q	R	S	Т	U	۷	W	X	Y	Ζ
	Α	Α	В	C	D	Ε	F	G	Η	Т	J	Κ	L	Μ	Ν	0	Р	Q	R	S	Τ	U	۷	W	Х	Y	Ζ
	В	Ζ	Α	В	С	D	Ε	F	G	Η	Ι	J	K	L	Μ	Ν	0	Р	Q	R	S	Τ	U	۷	W	X	Υ
	С	Y	Ζ	A	B	С	D	E	F	G	Η	Ι	J	K	L	Μ	Ν	0	Р	Q	R	S	Τ	U	V	W	X
	D	Х	Y	Z	A	B	C	D	E	F	G	H	1	J	K	L	M	N	0	Р	Q	R	S	T	U	V	W
	E	W	X	Y	L	A	B	C	D	E	F	G	H	-	J	K	L	M	N	0	P	Q	R	S		U	V
	F	V	W	X	Y	Z	A	В		D	E	F	G	H	1	J	K	L	IM	N	0	P	Q	R	5		U
	G	U	V	VV	X	Y	Z	A 7	B	D	0	E	F	G	H	I U	J	K	L	IVI	IN M	U N	P	Q	ĸ	5 D	I C
		۱ د	T	V	VV	×	T V	۷ ۷	A 7	D	R R	C	D	F	E	п С	Ц	1	N I	ĸ		M	N	r O	Q D	R	э Р
	÷	R	۱ ۲	т	V U	V	^ W	X	Z V	7	Δ	R	C	D	F	F	G	ч Н	1	N I	ĸ		M	N	F O	P	0
	ĸ	0	R	S	Т	U	V	W	X	Y	7	Δ	B	C	D	F	F	G	ч Н	1	1	K	1	M	N	0	P
Ł	L	P	0	R	S	Т	·U	v	W	X	Y	7	A	B	C	D	F	F	G	·	1	J	K	1	M	N	
Ŧ	М	0	P	Q	R	S	Т	U	V	W	X	Y	Ζ	Α	В	С	D	E	F	G	Η		J	K	L	M	Ν
	Ν	Ν	0	Ρ	Q	R	S	Т	U	۷	W	Х	Y	Ζ	Α	В	С	D	Ε	F	G	Н	Т	J	Κ	L	Μ
	0	Μ	Ν	0	Р	Q	R	S	Т	U	۷	W	Х	Y	Ζ	А	В	С	D	Ε	F	G	Н	Τ	J	К	L
	Ρ	L	Μ	Ν	0	Р	Q	R	S	Т	U	۷	W	Х	Y	Ζ	Α	В	С	D	Ε	F	G	Н	Т	J	Κ
	Q	Κ	L	Μ	Ν	0	Р	Q	R	S	Т	U	۷	W	Х	Y	Ζ	Α	В	С	D	Ε	F	G	Н		J
	R	J	Κ	L	Μ	Ν	0	Р	Q	R	S	Τ	U	۷	W	Х	Y	Ζ	А	В	С	D	Ε	F	G	Н	Т
	S	Т	J	К	L	Μ	Ν	0	Р	Q	R	S	Т	U	۷	W	Х	Y	Ζ	Α	В	С	D	E	F	G	Η
	Т	Η		J	K	L	Μ	Ν	0	Р	Q	R	S	Τ	U	V	W	Х	Y	Ζ	Α	В	С	D	E	F	G
	U	G	H	1	J	K	L	M	N	0	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
	V	F	G	H		J	K	L	M	N	0	P	Q	R	S	1	U	V	W	X	Y	Z	A	B	C	D	E
	W	E	F	G	H	1	J	K	L	IVI	N	U N	P	Q	K	5		U	V	W	X	Y	Z	A	B		D
	X		E	F	G	H		J	K	L	IVI	IN NA	N	P	Q	ĸ	D D	l c	U	V	VV	X W/	Y	Z V	A 7	В	
	T 7		0	E	F	G	H	I	J	K	L V	IVI	IN NA	N	P 0	Q D	ĸ	<u>р</u>	C I	U	V	VV V	X W	Y	Z V	A	В
i	2	В	C	U	E	F	G	Н	I	J	ĸ	L	IVI	IN	U	۲	ų	К	2		U	V	vv	X	Y	Z	Α



Encrypting Famous Quotes

- Take a movie quote and turn it into a polyalphabetic cipher code using the Vigenère Cipher.
- 2. Write it on your worksheet and see if your partner can crack the code!
- 3. Can you guess what movie the quote is from?





Transposition Ciphers

A method of encryption where the **positions** of the letters are changed, rather than changing the letters to hide the original message.

						Plair	ntext									T	ransp	oositio	on ma	itrix 1	а	<i>a</i>						Т	ransp	ositi	on ma	itrix 1	b			
	I,	Ρ,	U,	L.	L.	E.	D,	T.	H.	E .,	L,	E ₁₂	P,	E.	R.	M	U,12	T ₁₀	Α,	Τ.,	I.	0.	N.	S.	Α,	E.	I,	M.	N.	0.	Ρ,	R.	S,	Τ,,	Τ.,	U ₁₂
١	1,,	E.,	R.	Α.	N.	D.,	Α.,	C.	T.	22	V.	A.	Ŀ	P.	U,	L.	L.	Е.	D,	Τ.	H.	E ₁₀	L.	E 12	D,	P.	H.	L.	L.	E ₁₀	I,	U,	E ₁₂	Ε.	T.	L.
	Γ	E.	D	A	S	E.	C.	B	E.	T.	M	E	۷.,	Е,	R.	Α.	N,	D	A .,	C.	T.	12	V.	A.	Α.,	Ε.	T.	A	V.	122	۷.,	R.	A .,	D .,	C.	Ν.,
		Ц	Δ.	N		9	M		N	V	E		T ₂₅	E.	D	A.	S.	E.	C	R.	Ε.	T.	M.	E.	Cat	E.	E .,	A.	Mas	T _{at}	T ₅	D ₂₇	E	E	R.	S.
	37		~»	140	-	0.						14	C ,,,	H.	A.	N.	L	S.	M.	U.	N.	۷.	Ε.	L	M.	H.	N.	N.	Ε.	V .	C .,	A .,	L	S.	U.	L
2		50	N.,	G.	53	H.	E.	C.	0,,	N.	C.	Eto	L.		Nat	G	T.	Hs	E.	C.	0,,	N.	C.	E.	Ε.	١.,	0,,	G.	C.	N.	L.	Nst	E	H"	C.	Τ.
/	4 .,	L	E.	D.	P	A.	S.	S	A.	G.	E	B ₇₂	A.	L	E.	D"	Ρ.	A.	S.	S.	A.	G.	E "	B	S.	L.	A.	D.	E	G.	A.	E.	\mathbf{B}_n	A.	S.	P
	E 73	H ₇₄	75	N ₇₈	D,	A 78	N,,,	0.	L	D _{s2}	B	O ₅	Е"	H,	75	N ₇₅	D,	A ₇₈	N.	0	L.	D.	B	O "	N ₇	H.	L.	N.,	B.	D.	Е,	75	0.	A .,	0	D"
(⊃	K.	C.	A.	S.	E.							O.	K.	C.	A.	S.,	E.								K.		Ass			0.	C _{\$7}		Е.,		S
1				Т	ransp	oositi	on ma	atrix 2	2a							Т	rans	positio	on ma	ıtrix 2	b.									Ciphe	ertext					
	J.	I.	G.	S.	ransp A,	oositi W.	on ma	atrix 2	2a Z .,	Z ₁₂	L.	E.	Α,	E.	G.	T L	ransı J.	oositio L.	n ma	trix 2	ь U,	W.	Ζ.,	Z ₁₂	Е.,	T.	N	V.	U,	Cipho E.,	ertext	D.,,	1.	A	Е.	C.
	J. D,	I. A.	G. C.	S.	ransp A, E.	oositi W. S.	on ma P7 N3	atrix 2 U, P,	2a Z.,, E.,	Z ₁₂	L. H.	E.	A , E,	E.	G. C.	I.	J _s	L.	n ma P, N,	itrix 2 S ₆ M.	U.	W	Z.,	Z12 E3	E.	T.	N ₇₀	V.	U,	Cipho E.	ertext C ₂	D"	I	A	En T	C,
	J. D,	I. A.	G. C.,	S. M.	A, E.s	W. S.	on ma P7 N ₂	atrix 2 U, P, O.	Za Za Ea	Z.12 E.25	L. H.	E ₂	A, E.,	E ₂	G. C.	I. A.	ransı J. D,	H.	P, P, N,	ntrix 2 S₀ M₀ H.	ь U. Р.	W. S.,	Z., E.,	Z ₁₂ E ₂ s	E. C.	Т. Н.	N ₇₆	V C	U. K.	Ciphe E G.	ertext C ₂₀ I ₂₂	D,7 E,73	I E	A E	E,, T,,	C., A.,
	J. D,	I. A., H.,	G, C, K,	S. M. H.	Tansp A, E, T,	W ₁₀ S _{e7} E ₃₃	on ma P, N,,	U, P, O,	Z., E., A.,	Z ₁₂ E ₂₅ L ₅₁	L. H. L.	E ₂ I ₂ A ₄	A. E.s T.a	E ₂ Iss Ato	G, C, K,	I. A., H.,	Transp J. D. L.	L. L. L.	P7 P7 N70 N40	Ma Ma Ha	U, P, O,	W.(S., E.s	Z., E., A.,	Z ₁₂ E ₂₈	E C. H.	Ta Ha	N,, N,, E,,	V C A	U. K.	Ciphe E G A.,	C ₂₀	D,7 E,13 D,7	I., E., L.,	A.o E.o	E ₇₁ T ₅₃ B ₆₅	C., A., L.,
	J. D,	I. A., H., N.,	G, C,, K,,	S. M. H. D.	Tansp A, Ess Tan N ₇₀	Ser Es	on ma P, N, N, L,	U, P, O, V,2a	Za Za Ea Aa	Z 12 E 25 L 11 E 47	L. H. C.	Ez Is As En	A, E., T,,		G, C,, K,,	I. A., H.	Transp J. D. L. A.	L. L. C.	P7 N77 N18 L111	Hrix 2 Sa Ma Ha Da	U, P, O, V,	W. S. E. A.	Z E A		E.s C.r H.r. E.z	T. H. N.	N ₇ , N ₁ , E ₁₀	V., C., A.,	U, K., A.,	Cipho E G. A. C.	C ₂ C ₂ I ₂ I ₄	D,7 E,73 D,7 I,75	I E L S	A. E. A.	E ₇₁ T ₅₅ B ₅₅	C., A., L., N.,
•		I. A.,, H.,, E.,	G. C. K. G.	S. M. H. D.	ransı A. E. T. N.	W. S. E.s A.	on ma P, N,, N,, G,,	U., P., O., V., D.,	Za Z., E., M. I,	Z ₁₂ E ₂₅ L ₅₁ E ₄₇		E. I.s A.s E.n C.z	A. E.s T.z N.s		G. C. G. I.	I. A., H., E.,	ransı J. D. L. A. B.	C _s	n ma P, N. N. L. G.	Itrix 2 Sa Ma Ha Da Ta	eb U, P, O, , V, , D,	W.(S., E., A.,	Z., E., A., M.	Z ₁₂ E ₂ L ₁₁ V ₁₂	E.s C.a H.r. E.12 L.1	T. H. N. A.	N,, N,, E,, S,,	V C A H	U. K. A. L.	Cipho E G A C M	C _a I _z I _u T _z	D, E, D, I, D,	I E L S T	A., E., A., L, O.,	E ₇₁ T ₅₅ B ₅₅ N ₇₉	C. A. L. N.
		I. A.,, H., E., A.,	G. C. K. G. L. E.	S. M. H. D. T.	ransp A, E, T, N, V, U,	W. S. E. A. N.	on ma P, N, N, G, D,	 U. P. O. V. D. A. 	22 Z., Z., Z., J., M., I., N.,	Z 12 E 16 E 17 V 13 E 16	L. H. L. C. T. I.		A. E.s T. N. V.		G. C. K. G. L.	I. A., H., E., A.,	Tansp J. D. L. A. B. S.		P7 P7 N20 N20 N20 N20 N20 N20 N20 N20 N20 N20	itrix 2 S. M. H. D. T. O.	U, P, 0, V,	W. S. E. A. N.	Z., E., A., M., I.	Z.:2 E.s L.: E.s V.: E.s	E C H E P	T. H. N. A. G.	N ₇ , N ₁ , E ₁ , S ₂ , D ₂ ,	V., C., A., H., O,	U, K, A, L, U,	Ciphe E. G. A. C. M.	E	D,7 E,73 D,7 I,5 D,4 C,4	I E.s L S T.s	A E. A L. O	E., T., B., N.,	C., A., L., N., T.
		I. A., H., E., A., A.,	G. C. K. G. L2 E. F. 7	5. M. H. D. T.	A, E.s T ₂ , N, U, E.s	W, S, E, A, B, B, 2	on ma P, N,, N,, L,, D,, O,,	U., U., P., O., V., V., D., D., E.,	2a Z.,, E.,, M., M., N.,	Z.;2 E.;5 L.;1 E.;7 V.;3 E.;5	L. H. C. T. S.		A. E., T., N., V., E.,		G., C., K., G., I., E.,	I. A., H., E., A.,	iransp Js D7 Ls Ass Bs Ls Es 2		P, P, N, N, C, D,	Itrix 2 S. M. H. D. T. S. C. S.	25 U, P, O,, V,, D, A, F,	W.« S., E., A., R., B.,	Z., E., A., M., I. N.,	Z.2 E.3 L.1 E.2 V.3 E.5	E C H E P	T., H., N., G., P.	N.,, N.,, E.,, S.,, D.,,	V C A H O V	U, K. A. L. D.	Ciphe E G A., C., M A.,	C ₂ L ₂ L ₄ T ₂ H, E,	D.7 E.7 D.7 I.8 C.6	I E S S.,		E ₇ T ₅ B ₅ N ₇ L ₁	C. A. L. N. T. N.
, 		I. A., H., N., C. , A., A.,	G, C, K, G, I 2 E, E, E,	5. M. H. D. T. 0. 1. T.	A, E, T, N, V, E, o C,	Www Ser Ess Aw Ns Brz Rs	on ma P, N, , L,, G, , O,,	atrix 2 U. P. O V D A E. C	Za Z., A., M., I, N., S.,	Z,12 E,25 E,27 V,13 E,27 E,25 O,27	L. H. C. T. S. L.	E: I A E C C H N	A, E.s T. N. V. U. E. C.		G, C, K, G, E, E,	Т	ransı J. D, L. A. B. S. L., C. C. A.	L, H, L, C, T, S, L,	P, N., N., C, D, O,	Itrix 2 S. M. H. D. T. S. C. S. L. T.	ь U. P. 0. V. С.	W. S. E. A. N. B. R. B. Z.	Z., E., A., M., I. N., D., S.,	Z., E., L., E., E., O.,	E.s C.e H.r E.	T., H., A., G., P., B.,	N.,, E.,, S.,, D.,, R.,,	V., C., A., H., O., S.,	U, K, A, L, U, E,	Ciphe E. G. A., C. M. A., A.,	C ₂ I ₂ I ₄ T ₂ H, E, M ₃	D,, E,, D, L, C,, I,	I.a E.a I.a S.a T.a S.a N.a	A., E., A., C., D.,	E,, T,, B,, N,, I,, A,, S,,	C., A., L., N., T.

https://en.wikipedia.org/wiki/Transposition_cipher



Rail-Fence Ciphers

A rail-fence cipher rearranges the letters of a message into a zig zag pattern along a set number of "rails" or lines.

R		I		F		Ν		Е		I		Н		R
	A		L		Е		С		С		Ρ		Е	

RIFNEIHRALECCPE



Rail Fence Cipher

Let's try to encrypt FRENCHFRIES together



Rail Fence Cipher

FRENCHFRIES

F		Е		С		F		Ι		S
	R		Ν		Н		R		Е	

FECFIS RNHRE

or **FECFISRNHRE** to be a little more tricky



Rail Fence Cipher

Three Rails

F				С				Ι		
	R		Ν		Н		R		Е	
		Е				F				S

FCIRNHREEFS

or FCI RNHRE EFS



How would we decrypt this using a Rail Fence Cipher?

PNUNETIHEGISAFS

- **1.** Count the number of letters in the code (15)
- 2. Create a grid: the number of rows correspond with the key (2 in this case), and the number of columns correspond with the letters in the code (15).



Decrypting using Rail Fence

3. Fill in the grid by **skipping a space** between each letter. **PNUNETIHEGISAFS**

Р		Ν		U		Ν		Е		Т		Ι		Н
	Е		G		I		S		А		F		S	

PENGUINS EAT FISH



More Decrypting using Rail Fence

Unscramble this! They key is 2.

EEHNSRSCOLPATAEOOL



More Decrypting using Rail Fence

Unscramble this!

Ε		Ε		Η		Ν		S		R		S		С		0	
	L		Ρ		A		Т		A		Ε		0		0		L

ELEPHANTS ARE SO COOL



Create your own secret codes!

- 1. Working in pairs, write a secret message that you would like to send to another pair.
- 2. Create your own code to encrypt your message.
- 3. Share the code and key so that they can decipher the message.



Dual Defence: Creating a Stronger Code

Combine the 2 methods we just learned to make a really strong code.

- What kind of key would you need to provide?
- How would you make this super difficult to crack?



Other types of ciphers

Pigpen Ciphers

> JIFUV >ND VIE> X marks the spot

$$D \xrightarrow{A}_{C} B E \xrightarrow{H}_{G} F M \xrightarrow{V}_{K} L \xrightarrow{N}_{K} R \xrightarrow{O}_{V} P V \xrightarrow{S}_{U} T Z \xrightarrow{V}_{V} R$$

https://en.wikipedia.org/wiki/Pigpen_cipher



https://www.cachesleuth.com/scytale.html

ADFGVX Cipher

	_	_	_	_		_
	Α	D	F	G	۷	X
Α	1	4	7	R	Ε	G
D	1	M	Ν	Т	А	В
F	С	D	F	н	J	К
G	L	0	Ρ	Q	S	U
۷	۷	W	Х	Y	Ζ	0
х	2	3	5	6	8	9

https://crypto.interactivemaths.com/adfgvx-cipher.html



Making it work in the real world.

- The individual techniques may seem outdated, but learning about them is important for understanding the basics of cryptography and how more advanced modern ciphers work.
- Today, the combination of Transposition and Substitution ciphers do most of the work in today's encryption technology.



Thank you!