SCHOOL OF CIPHER

Ciphers

Nine ways to scramble a message so nobody else can read it

BOOKLET 1 OF 5

WHAT IS INSIDE

Contents

FOR GROWN-UPS

How to use these sheets

Every sheet is one cipher. Pick one, do it, and stop. There is no order to follow and nothing is a prerequisite.

What works, from doing this with children

1. **Let them encode first.** Writing a message of their own is where the rule sticks. Decoding somebody else's comes second.
2. **Swap and decode.** The arguments about who made the mistake are the lesson, not an interruption to it.
3. **Let them be wrong for a while.** The moment a child spots their own error is worth more than being told.
4. **Finish with the puzzle strip.** A short win at the end matters.

A good order, if you want one

Pigpen first: it looks like magic and needs no arithmetic. Then the shift cipher, then rail fence, then whatever they are drawn to.

> **Answers are on the last sheet.** Consider not handing it out. A child who checks the answer stops thinking; a child who cannot check keeps going.

SHEET 1

Pigpen

Every letter lives in a pen. The shape of the walls around it is the letter, and a dot means the second grid.

A	B	C
D	E	F
G	H	I

no dots

J	K	L
M	N	O
P	Q	R

with a dot

S T U V go in an X shape without dots, W X Y Z in an X shape with dots.

Write your name in pigpen

Now a message nobody else should read

Why it feels like magic: the page stops looking like writing at all. That is the whole trick, and it is why children remember this one.

SHEET 2

The shift cipher

Slide the whole alphabet along by a secret number. Julius Caesar used a shift of three.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Fill the bottom row in with your shift, then use it.

Encode with a shift of 5

```
MEET ME BY THE GATE
```

Decode. The shift is 7.

```
AOL KVN HAL TF OVTLDVYR
```

Break it without the key. There are only twenty five shifts. Try them all: one of them will be English. That is called brute force, and it is the reason this cipher never lasted.

SHEET 3

Rail fence

Write the message zig-zagging down two rails, then read the top rail followed by the bottom rail.

Encode BRING THE MAP

Top rail first, then the bottom rail:

Decode. Two rails.

```
TEDGSNH IHOSITEE
```

Notice what did not change. Count the letters: exactly the same ones are there, in a different order. That makes this a transposition, and it means counting letters will never break it.

SHEET 4

Key word columns

Write the message in rows under a key word. Number the key word's letters in alphabet order, then read the columns out in that order.

Key word: JANET

J	A	N	E	T

A is 1, E is 2, J is 3, N is 4, T is 5. Write the message across the rows, then read down column 1, then column 2, and so on.

Try it with

```
THE PASSWORD IS PENGUIN
```

Change the key word and the whole cipher changes. Nothing to carry, nothing to lose: the key lives in your head.

SHEET 5

Polybius squares

Every letter becomes two numbers: which row, then which column. I and J share a cell.

A	B	C	D	E
F	G	H	I	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

Row numbers down the side, column numbers across the top, both starting at 1.

Encode

```
LOOK UNDER THE DESK
```

Decode

```
44 23 15 22 34 31 14 23 11 44
```

The same square, knocked on a wall, is the tap code that prisoners of war used to talk through the walls of their cells. Two counts of taps, one letter.

SHEET 6

Key word alphabet

Write a key word with any repeated letters removed, then finish the alphabet, skipping every letter you have already used.

Key word: THURSDAY

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

The top row is the message letter. Fill in the bottom row and it is your cipher letter.

Encode

```
NOBODY EXPECTS THE CODE BREAKER
```

A whole scrambled alphabet from one word you can remember. That is the point: nothing to carry, and you can rebuild it from memory anywhere.

SHEET 7

Atbash

The alphabet backwards. A pairs with Z, B with Y, and so on to the middle. There is no key at all.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Encode

```
MEET ME AT THE OLD OAK
```

Decode

```
GSVIV RH MLGSRMT GL IVNVNYVI
```

Doing it twice brings the message back. Encoding and decoding are the same job, which means there is no key to forget and none to steal. It is also why anybody who has seen it once can read it forever.

SHEET 8

Playfair

Letters travel in pairs. Build the square from a key word, then work each pair through three rules.

Key word: MONARCHY

The three rules

1. **Same row:** each letter steps one to the right, wrapping round the end.
2. **Same column:** each letter steps one down, wrapping round the bottom.
3. **A rectangle:** each letter slides across to the other corner, staying in its own row.

Split into pairs, then encode

```
MEET ME AT NOON
```

A double letter breaks the rules, so push an X between them. And because it works on pairs, counting single letters tells a code-breaker nothing at all.

SHEET 9

Bacon's cipher

Every letter becomes five units of two kinds, A and B. Then those units can be carried by anything that comes in two forms.

A AAAAA · B AAAAB · C AAABA · D AAABB · E AABAA · F AABAB · G AABBA · H AABBB · I ABAAA · J ABAAB · K ABABA · L ABABB · M ABBAA
N ABBAB · O ABBBA · P ABBBB · Q BAAAA · R BAAAB · S BAABA · T BAABB · U BABAA · V BABAB · W BABBA · X BABBB · Y BBAAA · Z BBAAB

Turn this into units

HIDE

Now hide them

Write an ordinary sentence with one word for every unit. Underline the words that stand for B and leave the A words plain. Somebody reading it sees a sentence.

Three hundred years later the same idea got two new names: nought and one.

FOR GROWN-UPS

Answers

Sheet 2, shift cipher

Encode with 5: RJJY RJ GD YMJ LFYJ
Decode with 7: THE DOG ATE MY HOMEWORK

Sheet 3, rail fence

BRING THE MAP becomes BIGHMP RNTEA
TEDGSNH IHOSITEE decodes to THE HIDDEN GHOSTS (two rails)

Sheet 4, key word columns

Key JANET numbers as A1 E2 J3 N4 T5.
THE PASSWORD IS PENGUIN becomes HSIG POPI TSDN EWSU AREN

Sheet 5, Polybius

LOOK UNDER THE DESK becomes
31 34 34 25 45 33 14 15 42 44 23 15 14 15 43 25
44 23 15 22 34 31 14 23 11 44 decodes to THE GOLD THAT

Sheet 6, key word alphabet

THURSDAY gives T H U R S D A Y B C E F G I J K L M N O P Q V W X Z
NOBODY EXPECTS THE CODE BREAKER becomes IJHJ RXSW KSUO NOYS UJRS HMST ESM

Sheet 7, Atbash

MEET ME AT THE OLD OAK becomes NVVG NV ZG GSV LOW LZP
GSVIV RH MLGSRMT GL IVNVNYVI decodes to THERE IS NOTHING TO REMEMBER

Sheet 8, Playfair

With MONARCHY: MEET ME AT NOON becomes CL KL CL RS AN NA

Sheet 9, Bacon

HIDE becomes AABBB ABAAA AAABB AABAA

If an answer here disagrees with a child's working, check the child's first. These were generated by machine and checked, but the interesting conversations start when somebody thinks the answer sheet is wrong.

CREDITS

About this booklet

School of Cipher is a free set of lessons, animations and worksheets about codes, ciphers, signals and hiding messages, for code-breakers roughly aged seven to eleven.

How this was made. The writing, worksheets, diagrams and animations in this booklet were produced by **Claude**, an AI assistant made by Anthropic, working from a person's prompting, direction and curation. A human chose what the project should be, what belonged in it, what to cut, what was wrong, and what to keep. The AI did the drafting and the building.

Facts have been checked where checking was possible, and where a source could not be confirmed the claim was left out rather than guessed at. If you find a mistake, it is worth telling us: on a site about code-breaking, being corrected is the point.

Sources and further reading

Codes, Ciphers and Secret Writing by Martin Gardner is where this project started, and several of the earliest ciphers here follow his explanations.

Historical details have been drawn from public reference sources, museum material and the published records of the organisations named in the text.

Using this booklet

- Print at **100 per cent**, not fit to page, or any template will come out the wrong size.
- Photocopy freely for a class, a club or a family. No permission needed.
- Every sheet works on its own. There is no need to go in order.

schoolofcipher.com · free forever · no accounts, no tracking, no ads