



SCHOOL OF CIPHER

Breaking Codes

How every cipher in booklet one falls, and what to do when there is nothing there

BOOKLET 5 OF 5

Free to copy for home and classroom use
schoolofcipher.com

Counting letters	3
The shape of a word	4
Trying every key	5
Guessing one word	6
What am I looking at?	7
Codes that were never there	8
Answers	9
About this booklet	10



Counting letters

The oldest way to break a cipher, written down by al-Kindi in Baghdad in the ninth century. No key, no cleverness, just a tally.

How often each letter turns up in English

E is far ahead of everything. Then T, A, O, I, N, S, H, R. At the other end, J, Q, X and Z are almost never used.

Count the letters in this message

ZXG SYythG CZVGZZGE DH ZXG CGZZGE G

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
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Write your count under each letter. Which cipher letter turns up most?

Now guess

If the commonest cipher letter is really E, write E under it everywhere it appears and see what the message starts to look like.

Why this beats trying every key. A scrambled alphabet has more keys than there are atoms in a room, and no amount of trying will get through them. This gets through in ten minutes with a pencil, because the cipher hides which letter is which but does nothing to hide how often each one appears.



The shape of a word

You do not need to know which letters they are. Label them in the order they first appear: the first new letter is A, the second B, and a repeat keeps the label it had.

Work out the shape of each word

NOON	LETTER	
THAT	SEES	
COOKIE	DEED	
THERE	BOOK	

Which English words could these be?

A cipher word shaped A B B A, four letters:

A cipher word shaped A B B C D E, six letters:

Long words are a gift. Almost nothing in English has the shape of LETTER, so a six letter cipher word with that shape has very few candidates. This is why code-breakers look for the longest word first.



Trying every key

A shift cipher has exactly twenty five wrong keys and one right one. So do not be clever. Try them all.

Shift this back, one at a time, until it turns into English

XLI KSPH MW MR XLI SPH QMPP

- | | |
|----------|----------|
| 1 _____ | 14 _____ |
| 2 _____ | 15 _____ |
| 3 _____ | 16 _____ |
| 4 _____ | 17 _____ |
| 5 _____ | 18 _____ |
| 6 _____ | 19 _____ |
| 7 _____ | 20 _____ |
| 8 _____ | 21 _____ |
| 9 _____ | 22 _____ |
| 10 _____ | 23 _____ |
| 11 _____ | 24 _____ |
| 12 _____ | 25 _____ |
| 13 _____ | |

Where brute force stops working. Add one letter to a key and the number of keys does not go up by one, it multiplies. A five letter key word gives about twelve million. A scrambled alphabet gives four hundred million million million million, and a computer trying a billion a second would still be going when the sun burns out.



Guessing one word

A guessed piece of message is called a crib. It does not have to be much: a station that always opens the same way, a letter that starts Dear Sir.

Every message from this station begins with the word WEATHER

FNJQCQNA ANYXAC LUNJA BTRNB

Line WEATHER up under the first seven letters. What shift turns F into W?

Now use that shift on the whole message.

Make a crib on purpose

The Americans suspected the code group AF meant Midway, so they had Midway broadcast in clear that its water plant had broken. Japan duly reported that AF was short of water, and a guess became a certainty.

Which is why real ciphers avoid predictable openings. No fixed greeting, no message beginning the same way twice. A cipher is only as strong as the most guessable thing inside it.



What am I looking at?

A code-breaker's first question is never which cipher. It is what kind of thing is this.

Four questions, in order

1. **Letters or numbers?** Numbers in pairs, all between one and five, means a square: Polybius or tap code.
2. **How many different symbols?** Two means Bacon or binary. Five means ADFGX. Twenty six means an ordinary alphabet cipher. More than twenty six means several symbols per letter.
3. **Do the letter counts look like English?** If E, T and A are still commonest, the letters were **moved**, not replaced: a transposition. If the counts are flat, something is fighting the counting attack.
4. **Are the word lengths normal?** Groups of four or five mean the sender hid the word breaks on purpose.

Say what each of these probably is

44 23 15 32 11 34

AABBB ABAAA AAABB AABAA

MEMT NGTX ETEO IHQZ

3141592653589793238462643

The hardest answer a code-breaker can give is that there is nothing there. The last line is pi. It looks exactly like a code and it is not one.



Codes that were never there

Take any long piece of text and read every seventh letter. Then every eighth. Then every ninth. You will find words. You will always find words.

Try it on this

QWERTYUIOPASDFGHJKLZXCVBNMQAZWSXEDCRFVTGBYHNUJMIKOLPMNBVCXZLKJHGFDSAPOIUYTREWQ

Every third letter:

Every fifth letter:

Every seventh letter:

What it means when you find one

Nothing. There are seventy eight letters here and dozens of spacings to try, which is hundreds of chances for a short word to appear. Something always does.

People have claimed for centuries that messages are hidden in Shakespeare, and that skipping letters through religious texts reveals prophecies. The same trick finds the same kinds of words in novels, in phone books and on this page.

The rule that protects you. Fix the rule before you look, and then keep it. If you are allowed to change the rule until something appears, you will always make something appear, and it will mean nothing. Wherever somebody shows you a pattern, ask: did they decide what counted before they started looking?

Sheet 1, counting

The message is a simple substitution of THE COMMONEST LETTER IS THE LETTER E. G stands for E and appears most often, which is the way in.

Sheet 2, word shapes

NOON is ABBA. THAT is ABCA. COOKIE is ABBCDE. THERE is ABCDC. LETTER is ABCCBD. SEES is ABBA. DEED is ABBA. BOOK is ABBC.

Sheet 3, brute force

A shift of four backwards gives THE GOLD IS IN THE OLD MILL.

Sheet 4, the crib

F to W is nine places back. The message reads WEATHER REPORT CLEAR SKIES.

Sheet 5, identification

Numbers in pairs between one and five: Polybius or tap code. Two symbols in groups of five: Bacon. Ordinary letters in groups of four with normal letter counts: a transposition. And the last one is pi, which is not a code at all.

Sheet 6

There is no correct answer, and that is the answer. Whatever a child finds, ask them how many spacings they tried before they found it.



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