CLASSIFIED · FOR YOUR EYES ONLY

Top Secret

Codes, Ciphers, and How to Crack Them



THE ROBOT BOOK CLUB

Top Secret

Codes, Ciphers, and How to Crack Them

THE ROBOT BOOK CLUB

Copyright © 2026 Edward Benson

All rights reserved.

No part of this book may be reproduced in any form without written permission from the author, except for brief quotations in a review.

The ciphers in this book are real and every worked example and puzzle is computed exactly, so the answers in the back can never be wrong. The stories are grounded in the historical record; where a popular legend is exaggerated or a code is still unsolved, this book says so.

Published by The Robot Book Club

For the note-passers and secret-language inventors. If your teacher intercepts this book, deny everything.

How to Read the Codes in This Book

This book does two things at once: it tells you true stories about the greatest secret codes in history, and it teaches you to write and crack real codes yourself. Here is the gear you will see on the way:

CAESAR The **cipher tag** tells you which code a section is about.

The **How It Works panel** shows the actual key and a worked example — computed exactly, so it is always right.

The **Spy File** holds one surprising, true fact worth reading out loud.

A **Crack This puzzle** is a real coded message for you to solve. There are twelve, and the **answer key in the back** holds every solution.

The **cartoons** show the great moments. The moment is real; the drawing is ours.

Grab a pencil and a notebook. Read it front to back, or flip straight to the puzzles. Either way — tell no one.

The Secret War of Words

> In the summer of 1586, a spy named Thomas Phelippes sat at a desk in London, staring at a letter filled with strange, scrambled symbols. It had been smuggled out of a prison hidden inside the waterproof plug of a beer barrel. The letter belonged to Mary, Queen of Scots, and she believed the symbols were completely unreadable. But Phelippes was a master code-breaker. He didn't just read her secret plot to overthrow the English queen—he forged a fake message at the very end using her own secret alphabet, trapping her co-conspirators. Before he handed the translated letter to the queen's spymaster, Phelippes drew a tiny, chilling picture on the envelope: a hangman's gallows. Mary's unbreakable code had been broken, and it was going to cost her her life.

Hiding, Shifting, and Swapping

If you want to keep a secret, you have three options. The first is *steganography*, which is a fancy way of saying "hiding the message so nobody knows it's there." In ancient Greece, a ruler named Histiaeus supposedly shaved a servant's head, tattooed a secret message on his scalp, waited for the hair to grow back, and sent him off to start a rebellion. (Though, between you and me, memorizing the message would have been a lot faster!).

But what if the enemy intercepts your messenger? That's where *ciphers* and *codes* come in. People use the words interchangeably, but to a cryptographer, they are completely different tools. A cipher changes a message letter by letter using a strict rule. Julius Caesar protected his military orders by shifting every letter in the alphabet exactly three spaces down.

A code, on the other hand, swaps out whole words or ideas. During World War II, the US Marines worked with Navajo soldiers to build an unbreakable code based on their complex native language. A Navajo Code Talker wouldn't spell out "fighter plane"—he would say *dah-he-tih-hi*, the Navajo word for hummingbird.

The Endless Duel

The history of secret writing is an endless, high-stakes game of tug-of-war. A code-maker invents a puzzle they swear is absolutely impossible to solve. For centuries, the simple substitution cipher—like Caesar's—was the ultimate vault. Then, in 9th-century Baghdad, a brilliant scholar named Al-Kindi noticed that in almost every language, some letters are used way more often than others. In English, 'E' is everywhere. Al-Kindi realized that even if you disguise 'E' as a '#' or a 'Q', it will still show up the most. He invented "frequency analysis," and suddenly, every secret cipher in the world was blown wide open.

The code-makers struck back by inventing dizzyingly complex machines. During World War II, the German military built the Enigma, a machine that used spinning electro-mechanical rotors to change the cipher rule with every single letter typed. Press 'A' and you might get 'X'. Press 'A' again, and you get 'T'. It was designed to completely destroy frequency analysis. The code-breakers had to level up again, leading a brilliant team at Bletchley Park to build a massive, wire-filled machine called the Bombe just to fight it.

Thinking Like a Detective

So, how do you actually defeat a "perfect" cipher? You don't need to be a math genius. You just need the patience of a detective. You look for patterns, repeating symbols, and one-letter words. And when the math gets too tangled, you cheat a little by using a "crib"—a lucky guess based on human habits.

The code-breakers at Bletchley Park knew that German radio operators were creatures of habit. Every day at the exact same time, certain stations sent out a weather report. The code-breakers guessed that these intercepted messages probably started with the German word *WETTER* (weather). By lining that single guessed word up against the gibberish cipher, they could lock in a tiny piece of the puzzle, exposing the mechanical settings of the entire Enigma machine.

Secret writing isn't just for queens, generals, and spies anymore—it's the invisible digital shield that protects your text messages and online passwords today. Now, it's your turn to step into the duel. Turn the page, and get ready to crack some real codes yourself.

CHAPTER 1

Ancient Secrets

Long before computers, generals and spies were already hiding their words. Meet the very first ciphers — a sliding alphabet, a message that only makes sense wrapped around a stick, and the clever mind who invented code-breaking itself.

THIS CHAPTER TEACHES: THE CAESAR CIPHER

Caesar's Secret Shift

Julius Caesar had a massive problem. In the first century BCE, his military campaigns stretched across the world. He constantly sent runners through enemy territory carrying highly sensitive orders. If a messenger was captured, Caesar’s battle plans were ruined. He needed a way to make his letters look like complete gibberish.

His solution was brilliantly simple: he just slid the alphabet forward. Caesar chose a shift of exactly three steps. If he wanted to write an A, he counted three letters down and wrote a D. A B became an E, and a C became an F.

When he reached the end of the alphabet, he just wrapped it around like a circle. An X, Y, or Z looped back to become an A, B, or C. To read the message, his generals simply shifted every letter three spaces backward.

You might think shifting three letters is a terrible way to hide a secret. Today, it is! But back then, most of Caesar's enemies couldn't read at all. Even the few who could had never seen a substitution cipher. That simple shift was all he needed.

The Caesar Shift

SHIFT +3

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

MESSAGE

MEET ME AT THE FORUM

↓

SECRET

PHHW PH DW WKH IRUXP

Slide every letter three steps forward to hide it. Slide three steps back to read it.

SPY FILE

Did You Know?

Caesar's adopted heir, Emperor Augustus, used a shift of one. He didn't wrap his alphabet around—when he needed the last letter of the alphabet, he just wrote "AA"!



Caesar hands off a scrambled order — Rome, around 50 BC.

Puzzle Break

Grab a pencil — decode the secret message.

CRACK THIS #1

CAESAR · SHIFT 3

PHHW PH DW WKH WUHHKRXVH

Hint · *Every letter slid three steps forward. Slide it three steps back.*

ANSWER IN THE BACK OF THE BOOK

Stuck? Every solution is in the answer key at the back of the book.

How to Crush a Caesar Cipher

Julius Caesar might have conquered the ancient world, but his famous cipher has a massive, glaring weakness. If you intercept a scrambled Roman message, you don't need advanced mathematics or a captured spy to read it. You just need a little patience.

The secret to beating this code is recognizing its limit. Because there are only twenty-six letters in the alphabet, there are only twenty-five possible ways to shift them. That means there are exactly twenty-five possible keys to the entire system.

Code-breakers call this a "brute force" attack. You don't look for clever clues—you just kick the door down. Take the first scrambled word of the message and shift its letters backward by one space. If it is still gibberish, shift it by two. Then three.

Long before you test all twenty-five shifts, a normal, readable word will magically appear on your page. The Romans got away with this trick because most of their enemies couldn't read at all. Today, busting it open is the ultimate code-breaking superpower.

Only 25 Ways to Slide

SHIFT +5

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

MESSAGE

TRY EVERY SHIFT

↓

SECRET

YWD JAJWD XMNKY

A Caesar cipher has just 25 real shifts. A patient code-breaker can try them all until words appear.

SPY FILE

Did You Know?

Emperor Augustus used a shift cipher too, but his was even lazier than Caesar's. He shifted his letters by just one single space, turning every A into a B!

Puzzle Break

Grab a pencil — decode the secret message.

CRACK THIS #2

CAESAR · SHIFT 7

AOL WHZZDVYK PZ KYHNVU

Hint · *Try shifts until words appear. This one slid seven steps forward.*

ANSWER IN THE BACK OF THE BOOK

Stuck? Every solution is in the answer key at the back of the book.

The Scrambled Spartan Stick

In ancient Sparta, during the 5th-century BCE Peloponnesian War, military commanders needed to send secure messages. Instead of swapping letters for different ones, they invented a clever way to jumble the order of the letters using a wooden rod called a scytale.

A sender spiraled a long, narrow strip of leather tightly around the wooden stick, leaving no gaps. They wrote their secret message straight across the rod. When they unwound the strip, the letters transformed into a meaningless, scrambled mess.

The Roman writer Aulus Gellius noted that the unwrapped leather looked like random ink smudges because the letters were physically broken up! To read it, the receiver just wrapped the leather around an identical stick of the exact same thickness. The broken ink perfectly realigned.

While famous as history's first transposition cipher, modern historians debate its practical battlefield use. If an enemy intercepted the leather strap, they didn't need a math degree to crack it—they just had to test different-sized sticks until the letters lined up!

SPY FILE

Did You Know?

Nobody has ever found a physical ancient scytale! Our proof of how they worked comes entirely from writers who lived hundreds of years after the Spartans.



The Spartan scytale: readable only when it is wound just right.

The Polybius Fire Grid

In ancient Greece, a historian named Polybius documented a brilliantly simple way to send messages across miles of empty space. This system didn't need a messenger on horseback. It just needed a mountaintop, a sharp-eyed scout, and two fistfuls of blazing torches.

The trick is a five-by-five grid, like a checkerboard. You number the five rows down the side, and the five columns across the top, then fill the boxes with the alphabet. To send a letter, you just find its box and transmit its row and column numbers.

Instead of ink, ancient soldiers used fire. A scout held up torches on his left side for the row number, and torches on his right for the column number. By flashing these number pairs, they could spell out entire warnings from mountain to mountain.

Centuries later, this exact same mathematical grid helped captured soldiers survive. Prisoners of war realized they didn't need torches to send number pairs. They just needed a wall. They tapped out the row and column numbers, knocking secret messages right under their guards' noses.

SPY FILE

Did You Know?

The original Greek version didn't squish 'I' and 'J' into one box. It used the 24-letter Greek alphabet, leaving the final tablet with only four letters.

The Math That Broke Every Code

For hundreds of years, generals thought substitution ciphers were basically magic. If you swapped letters for new symbols, your secrets were perfectly safe! But in 9th-century Baghdad, a brilliant polymath named Al-Kindi working at the House of Wisdom shattered that illusion forever.

Al-Kindi realized that language leaves a mathematical fingerprint. Even if you disguise a written message, you cannot hide how humans actually talk. In English, the letter E is everywhere, showing up about 13 percent of the time.

He figured out that a substitution code doesn't change a letter's frequency. If a spy swaps E for a squiggly line, that squiggly line will still be the most common symbol on the page. To crack the code, you simply have to count.

Match the most common secret symbols to the most common regular letters, and the message begins to unravel. With this single realization, Al-Kindi invented the science of frequency analysis—and the modern art of code-breaking was officially born.

SPY FILE

Did You Know?

Al-Kindi's world-changing manuscript on code-breaking was completely lost to history for over a thousand years. It was finally rediscovered sitting unnoticed in an Istanbul archive in 1987!

The Disk That Scrambled Everything

In 1467 Rome, a Renaissance architect named Leon Battista Alberti had a problem. The brilliant statistical tricks invented by Al-Kindi had made old codes like the Caesar shift too easy to bust. Codebreakers just counted letters to find the secret message. Alberti needed a code that could fight back.

His solution was a brilliant mechanical gadget made of two copper plates. The outer plate held a normal alphabet, and the inner wheel held a scrambled one. By pinning them together in the center, Alberti created a code machine that could spin.

To write a message, you line up the wheels and encode a few words. But here is the genius part: right in the middle of a sentence, you spin the inner wheel to a totally new position and keep writing.

By rotating the disk, you completely change the secret alphabet mid-message. The letter 'E' might be a 'Q' in the first sentence, and an 'M' in the next. Letter counting becomes useless, making this spinning wheel a codebreaker’s worst nightmare.

The Cipher Disk

SHIFT +4

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

MESSAGE

SPIN THE WHEEL

↓

SECRET

WTMR XLI ALIIP

Turn the wheel to pick your shift. Here the wheel is set to four steps.

SPY FILE

Did You Know?

Alberti got the idea for his spinning disk in the Vatican gardens while discussing a world-changing new invention: Johannes Gutenberg's movable type printing press.

Puzzle Break

Grab a pencil — decode the secret message.

CRACK THIS #3

CAESAR · SHIFT 4

PSSO YRHIV XLI XLMVH WXEMV

Hint · *The wheel was set to four. Turn it back four to read it.*

ANSWER IN THE BACK OF THE BOOK

Stuck? Every solution is in the answer key at the back of the book.

CHAPTER 2

Codes at War

When countries fight, secrets win. This chapter is packed with the most famous codes in history — a machine that scrambled a message billions of ways, a code built from a language, dots and dashes flying through the air, and letters hidden inside little fences.

THIS CHAPTER TEACHES: PIGPEN AND MORSE CODE

The Typewriter That Lied

Imagine a typewriter that lies to you. In the 1920s through the 1940s, Germany used the Enigma machine to hide secret messages. If you typed the letter "A," electricity shot through a shifting maze of wires and lit up a totally different letter, like "G."

The secret was inside three spinning wheels called rotors. Every single time you pressed a key, the first rotor clicked forward, completely changing the maze. Press "A" three times, and it might light up as "G," then "P," then "W."

Who could solve a puzzle with billions of changing answers? A team of brilliant Polish mathematicians, including Marian Rejewski, mapped the Enigma's wiring in 1932. In 1938, they built a clacking electro-mechanical machine called the *bomba* to track the moving maze.

When World War II erupted, an ultra-secret team of British code-breakers at Bletchley Park took the baton. Mathematicians like Alan Turing and Gordon Welchman built a massive, improved machine called the Bombe to test thousands of rotor positions at once.

By searching for a "crib"—a guessed word, like "WEATHER"—the Bombe could sniff out the exact daily setting. This incredible international teamwork unraveled Germany’s deepest secrets and helped end the war.

SPY FILE

Did You Know?

Because of its spinning rotors and a complex plugboard, a standard German military Enigma machine had 158,000,000,000,000,000,000 (158 quintillion) possible settings!



Cracking the Enigma at Bletchley Park — England, 1940s.

The Code That Was Never Broken

During World War II, the U.S. Marine Corps needed a code the enemy couldn't crack. They found their answer in a brilliant group of young Navajo men. These Marines used their deeply complex, unwritten native language to build the only military code in modern history that was never broken.

The code talkers built a brilliant two-layer puzzle. The first layer was a clever alphabet. To spell out English names, they used Navajo words. For example, the letter A was "ant" and B was "bear." To spell the name Bob, they would simply say "Bear-Owl-Bear" over the radio.

The second layer was a secret dictionary of over 400 military words. A submarine became an "iron fish." A fast fighter plane became a "hummingbird." The enemy could easily listen to the radio, but all they heard were highly confusing sentences about bears, ants, and hummingbirds.

While machines took hours to unscramble messages, the Navajo code talkers could translate and send a top-secret battle command in just two and a half minutes. Thanks to their linguistic genius, thousands of lives were saved.

SPY FILE

Did You Know?

During the fierce month-long Battle of Iwo Jima, six Navajo code talkers worked around the clock, successfully sending over 800 messages with zero errors.



The Navajo code talkers send a code no enemy ever broke — 1940s.

Talking in Dots and Dashes

Imagine trying to send a text message using only a flashlight or a single radio beep. That is the genius of Morse code. It translates the entire alphabet into a rhythmic language of short signals (dots) and long signals (dashes). To keep things fast, the most common letters are shortest. "E" is just one dot!

You can send Morse code over a telegraph wire, blink it with your eyes, or flash it with a lamp. The secret to making it work is timing. A dash is exactly three times as long as a dot, and silent pauses tell the listener when letters and words end.

The most famous Morse code message in history is SOS. You have probably heard that this stands for "Save Our Souls" or "Save Our Ship." Surprisingly, that is a complete myth! Those letters don't stand for any words at all. They were chosen purely for the way they sound.

In Morse code, an "S" is three dots and an "O" is three dashes. Put together, they make an unmistakable, urgent rhythm that pierces right through crackling radio static. Check out the demo chart next to this page to see the whole alphabet—and try tapping out your own name!

Dots and Dashes

MORSE CODE

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 ––••	0 –––––	1 •––––	2 ••–––	3 •••––
4 ••••–	5 •••••	6 –••••	7 ––•••	8 –––••	9 ––––•

MESSAGE

SEND HELP NOW

↓

SECRET

••• • –• –•• / •••• • •–•• •––• / –• ––– •––

Every letter is a pattern of short and long signals. Read the chart, then read the message.

SPY FILE

Did You Know?

The first American ship to successfully call for rescue using the SOS signal was the SS *Arapahoe*, which lost power off the North Carolina coast in August 1909.

Puzzle Break

Grab a pencil — decode the secret message.

CRACK THIS #5

MORSE CODE

●●●● ● ●▬●● ●▬▬● / ●● ●●●

/ ▬●▬● ▬▬▬ ▬▬ ●● ▬● ▬▬●

Hint · *A dot is a short blink, a dash a long one. Use the Morse chart from this chapter.*

ANSWER IN THE BACK OF THE BOOK

Stuck? Every solution is in the answer key at the back of the book.

Secrets in the Pigpen

In the eighteenth century, a secretive group called the Freemasons needed a way to keep their messages hidden. Later, Union prisoners of war during the American Civil War used the exact same trick. Instead of swapping letters for other letters, they swapped letters for pictures.

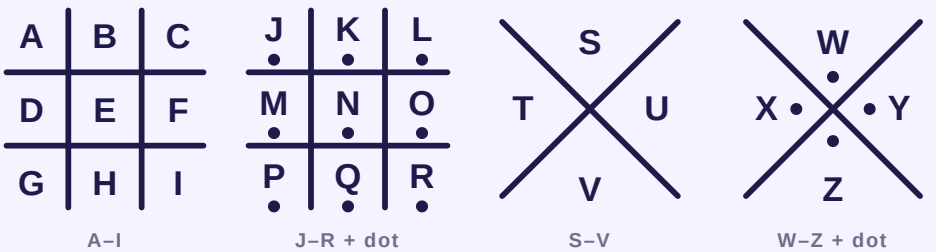
To use the pigpen cipher, you draw four grids. The first two look like big tic-tac-toe boards, and the second two look like giant X's. You drop the alphabet into the empty spaces of these grids, adding a single dot to every space in the second board and the second X.

Here is the trick: every letter becomes the shape of the "fence" around it. To write a secret message, you just draw the lines that surround your letter. If your letter lives in a dotted grid, you draw the fence and put a dot inside it.

Check out the demo grids next to this story to see how the alphabet fits inside the pens. A codebreaker just draws the blank grids, matches the shapes to the letters, and reads the hidden word!

The Pigpen Cipher

PIGPEN KEY



A–I | J–R + dot | S–V | W–Z + dot

MESSAGE

SECRET CLUB

↓

SECRET



S E C R E T C L U B

Each letter lives in its own little pen. Draw the fence around it, and add a dot for the second set.

SPY FILE

Did You Know?

In 1785, an English Freemason named Thomas Brierley had his gravestone carved with the pigpen cipher, using the secret shapes to spell out his final epitaph.



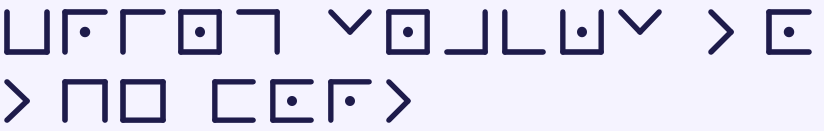
Drawing the pigpen pens by candlelight.

Puzzle Break

Grab a pencil — decode the secret message.

CRACK THIS #4

PIGPEN



Hint · *Each shape is a letter's pen from the grids. A dot means the second grid.*

ANSWER IN THE BACK OF THE BOOK

Stuck? Every solution is in the answer key at the back of the book.

The War of Waving Flags

During the Civil War, communicating across a smoky battlefield was a nightmare. U.S. Army surgeon Major Albert Myer solved this by inventing the "wig-wag" system. Signalmen waved massive flags by day and flaming torches by night. Waving left meant "1," waving right meant "2," and combinations spelled out letters.

There was just one massive problem. Myer’s brilliant assistant, E. Porter Alexander, joined the Confederate Army, while Myer fought for the Union. Both sides were using the exact same system! To stop enemies from reading their flags through spyglasses, signalmen used brass cipher disks to scramble the alphabet.

Telegraph wires weren't safe either. Enemy spies frequently climbed poles to hook their own listening gadgets directly to the cables. To protect President Abraham Lincoln’s military telegrams, the Union Army relied on a low-tech but brilliant trick called a Route Cipher.

Instead of swapping individual letters, a Route Cipher scrambles entire words. A commander wrote a message into a grid, replaced important names with fake code words, and read down the columns instead of across the rows. Anyone tapping the wire just heard a confusing jumble of out-of-order nonsense.

SPY FILE

Did You Know?

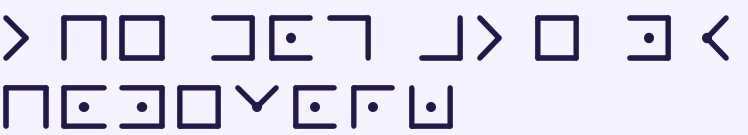
The inventor of the wig-wag system fought for the Union, but his assistant joined the Confederacy. Both sides ended up using the exact same flag signals against each other!

Puzzle Break

Grab a pencil — decode the secret message.

CRACK THIS #6

PIGPEN



Hint · *Draw the fences from the pigpen key, then read the letter inside each pen.*

ANSWER IN THE BACK OF THE BOOK

Stuck? Every solution is in the answer key at the back of the book.

Secrets the Size of a Sand Grain

Most secret codes work by scrambling a message so the enemy can't read it. But what if you hide the fact that there is a message at all? This trick is called steganography. If an enemy spy doesn't know a secret exists, they won't even try to crack it.

Movies make invisible ink look easy—just write in lemon juice and hold it over a candle! But during World War II, military censors easily busted lemon-juice spies by swabbing mail with chemical detectors. Real secret agents had to wear surgical gloves and use complex formulas that dried perfectly clear.

The ultimate hiding spot was the microdot. Perfected by German spies, an agent would type a full page of intelligence, photograph it, and use special lenses to shrink the image down to one millimeter—the size of a single grain of sand.

They printed this tiny photo on clear film, punched it out, and glued it perfectly over the period at the end of a sentence in a completely normal letter. Censors scanning the mail saw nothing but friendly chatter, missing the massive secret sitting in plain sight.

SPY FILE

Did You Know?

During the Vietnam War, the CIA successfully smuggled tiny microdot messages to prisoners of war by hiding them inside ordinary packets of Kool-Aid powder.

CHAPTER 3

Still Unbroken

Here is the honest, spine-tingling truth: some codes have never been cracked. Not by spies, not by professors, not by the world's biggest computers. Nobody knows what they say — and this chapter is careful to tell you exactly how much is really known.

THIS CHAPTER TEACHES: NOTHING NEW — THESE ARE THE MYSTERIES

UNSOLVED

The Statue That Stumped the CIA

In 1990, artist Jim Sanborn installed a giant, S-shaped copper scroll in the courtyard of CIA headquarters in Langley, Virginia. Named *Kryptos*, the curvy sculpture is covered in thousands of punched-out letters. It looks like a beautiful piece of art, but it’s actually a massive puzzle designed to tease the world's greatest spies.

The left side hides four secret messages. Codebreakers cracked the first three, known as K1, K2, and K3. Two use a Vigenère cipher, where a secret keyword changes how every single letter shifts in the alphabet. The third uses a transposition cipher, which scrambles perfectly good letters into a confusing grid.

But the final message, a 97-character section called K4, has completely stumped everyone for decades. Even the professional analysts working inside the CIA building can't figure it out. It is one of the most famous unsolved ciphers on the planet.

Sanborn wants K4 solved, so he occasionally drops hints. He revealed that certain chunks of letters translate to words like "BERLIN" and "CLOCK." But knowing a few answers isn't enough. Until someone discovers the hidden math connecting the scrambled letters to the real words, K4 remains totally unbroken.

SPY FILE

Did You Know?

Artist Jim Sanborn has given away the exact translation for 24 of K4's 97 characters, yet the world’s greatest computers still cannot figure out how to read the rest.



Kryptos: three parts solved, one still glowing in the dark.

Puzzle Break

Grab a pencil — decode the secret message.

CRACK THIS #7

MORSE CODE

▬▬ ▬▬▬ ●●●▬ ● / ●▬ ▬ / ▬●● ●▬ ●▬▬ ▬●

Hint · *Dots and dashes again: four letters, then two, then four.*

ANSWER IN THE BACK OF THE BOOK

Stuck? Every solution is in the answer key at the back of the book.

The Book No One Can Read

Deep inside a vault at Yale University sits a medieval book that makes the world's smartest codebreakers want to pull their hair out. It is filled with looping handwriting that nobody can read, surrounded by colorful drawings of impossible plants, swirling stars, and tiny women bathing in pools.

When a book dealer named Wilfrid Voynich bought it in 1912, people assumed it was a complex cipher. If you replace normal letters with your own invented shapes to write a diary, you are doing what experts think this author did. But supercomputers have spent a century trying to crack it, and nothing works.

So, what does it say? The honest truth is: we have absolutely no idea. It could be a lost human language or a brilliant code. It might also be an elaborate medieval trick, filled with gorgeous gibberish just to swindle a wealthy buyer.

Even if the words mean nothing, the object itself is not a fake. Atomic scientists tested the parchment and proved it was made between 1404 and 1438. The book is incredibly real—we just might never know its secrets.

SPY FILE

Did You Know?

Rumors claim a 13th-century philosopher named Roger Bacon wrote it. But radiocarbon dating proves the pages were made between 1404 and 1438, meaning Bacon was already long dead!



The Voynich manuscript — a whole book nobody can read.

Puzzle Break

Grab a pencil — decode the secret message.

CRACK THIS #8

CAESAR · SHIFT 5

YMJ JFLQJ MFX QFSIJI

Hint · *A five-step Caesar shift. Slide every letter back five.*

ANSWER IN THE BACK OF THE BOOK

Stuck? Every solution is in the answer key at the back of the book.

The Treasure That Never Was

In 1885, a pamphlet hit the streets of Virginia with a mind-blowing claim. A man named Thomas J. Beale had supposedly buried a massive treasure of gold, silver, and jewels worth sixty million dollars today. To find it, you just had to crack three pages of mysterious numbers.

The codes used a clever system called a book cipher. If you and a friend have the exact same book, you can hide messages using numbers. If the tenth word on the first page is "apple," writing "10" secretly stands for the letter "A."

Someone cracked the second page using the United States Declaration of Independence as the secret key. It translated into a detailed list of the buried loot! But the first page—the location—and the third page remained stubborn walls of unbroken numbers.

Treasure hunters have spent lifetimes digging for Beale's gold. But historians think the whole thing is a brilliant hoax. The letters, supposedly written in the 1820s, use the word "stampeding"—a term that didn't even appear in English print until 1832!

It is incredibly easy for a prankster to encode one message backwards to look real, and fill the other pages with meaningless, unsolvable numbers. Sometimes, an unbroken code isn't a masterpiece—it is just a spectacular joke.

SPY FILE

Did You Know?

Desperate treasure hunters have tried almost everything to find the sixty-million-dollar Beale fortune—including blowing up rocks with dynamite and hiring psychics!

UNSOLVED

The Composer's Secret Squiggles

On July 14, 1897, the famous British composer Edward Elgar sent a letter from Great Malvern, England, to his young friend Dora Penny. Elgar affectionately called her "Dorabella," and his note contained zero regular words. Instead, it was written using 87 bizarre, looping squiggles.

The cipher uses an alphabet of 24 different symbols. Each character is made of one, two, or three semicircles—looking a bit like the letter C—pointing up, down, left, right, or diagonally. It looks exactly like a substitution cipher, where each compass-pointing curve secretly stands for a letter.

For over a century, codebreakers have tried to crack it by swapping the most common squiggles for common English letters, but they only ever get total gibberish like "BLTACEIARWUN...". Because the cipher is only 87 characters long, it is mathematically too short to prove any single word translation is correct.

The coolest clue? Years earlier, Elgar scribbled these exact same semicircles next to sheet music by Franz Liszt, perfectly matching the number of printed musical notes. The Dorabella cipher might not be a written message at all, but a private, uncrackable melody meant just for a friend.

SPY FILE

Did You Know?

Elgar immortalized his friendship with Dora Penny by naming Variation 10 of his famous Enigma Variations after her.

Why Some Codes Stay Broken Forever

Sometimes, the greatest codebreakers and supercomputers in the world hit a brick wall. It is not because they aren't smart enough. It is because the strict laws of math and information say a cipher simply cannot be solved.

One reason is a missing key. If a secret message relies on a specific edition of a printed book, and that exact book is lost to history, the code becomes impossible to reverse. It is permanently locked as a random soup of numbers.

Another roadblock is a message that is simply too short. Codebreakers rely on finding patterns, which requires a lot of data. A tiny string of symbols could accurately translate into dozens of completely different sentences, leaving everyone guessing which one is real.

Finally, the simplest reason a code stays unbroken is that there is no real message hidden inside. Human brains love finding patterns in noise, but sometimes a mystery is just a clever hoax, a prank, or an artist's joke disguised as a secret.

SPY FILE

Did You Know?

A one-time pad uses a completely random key that is exactly as long as the secret message. If it is never reused, it is mathematically proven to be unbreakable.

CHAPTER 4

Make Your Own

Now it is your turn. This chapter hands you the tools to build codes your friends will actually use — a secret alphabet from a keyword, messages you can flash across a dark room, and the unwritten rules every good spy follows. Grab a notebook. Tell no one.

THIS CHAPTER TEACHES: KEYWORD SUBSTITUTION

The Secret Keyword Scramble

Shifting letters a few spaces is easy, but if you want to really scramble the alphabet, you need a key. Instead of memorizing twenty-six random letters, all you need to remember is one secret word. Let's use the word SHADOW.

To build your cipher, write your keyword first. If your word has repeating letters, cross out the extras—so APPLE becomes APLE. SHADOW has no repeating letters, so write the whole word down. These form the start of your secret alphabet.

Next, write out the rest of the alphabet in normal order right after your keyword. The only rule? You have to skip any letters you already used in your word. Once you reach the letter Z, you will have a completely scrambled row.

Check out the demo panel to see the SHADOW alphabet in action. To write a message, find your real letter in a normal alphabet and swap it for the secret letter hiding directly below it.

The SHADOW Alphabet

SECRET ALPHABET

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

MESSAGE

SPY HEADQUARTERS

↓

SECRET

QMY COSDNTSPROPQ

Write your keyword SHADOW first, then the leftover letters in order. That scrambled row is your secret alphabet.

SPY FILE

Did You Know?

Keyword ciphers have a funny weakness. Because keywords rarely use letters like V, W, X, Y, or Z, those letters usually just map to themselves at the end!



Secret HQ: build your own codes and gear.

Puzzle Break

Grab a pencil — decode the secret message.

CRACK THIS #9

SUBSTITUTION

BTSPD RCO QOAPOR POAEMO

Hint · *Use the SHADOW alphabet you just built. Match each code letter back to its plain letter.*

ANSWER IN THE BACK OF THE BOOK

Stuck? Every solution is in the answer key at the back of the book.

Talking With Flashlights

You do not need a heavy brass telegraph machine to send secret messages. If you have a flashlight, you have everything you need to talk to a friend across a dark campsite or a bedroom without making a single sound.

The trick is turning the alphabet into a code of short and long signals. Though it is called Morse code, a clever machinist named Alfred Vail actually invented the famous dot-and-dash alphabet at the Speedwell Ironworks in 1838.

Here is how to make your light readable: a quick flick on and off is a dot, and a longer, steady beam is a dash. Leave a short pause of darkness between each letter, and a longer pause between entire words.

Start by practicing the famous distress signal, SOS, because its rhythm is incredibly easy to remember. Once your eyes catch the beat, you can start flashing full sentences through the dark.

Flash It in Morse

MORSE CODE

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 −−··	0 −−−−−	1 ·−−−−	2 ··−−−	3 ···−−
4 ····−	5 ·····	6 −····	7 −−···	8 −−−··	9 −−−−·

MESSAGE

BLINK TO ME

↓

SECRET

−··· ·−·· ·· −· −·− / − −−− / −− ·

A short blink is a dot, a long blink is a dash. Now you can talk across a dark room.

SPY FILE

Did You Know?

Alfred Vail visited a newspaper office and counted their metal letters. Finding that "E" was the most used, he made it the fastest code to send: a single dot.

Puzzle Break

Grab a pencil — decode the secret message.

CRACK THIS #11

MORSE CODE

•▬ ▬••• ▬▬▬ •▬• ▬ / ▬• ▬▬▬ •▬▬

Hint · *Short blink is a dot, long blink is a dash. Two letters, then three.*

ANSWER IN THE BACK OF THE BOOK

Stuck? Every solution is in the answer key at the back of the book.

Layer Your Codes For Double Security

You built a clever keyword cipher, but there is a catch. A determined snooper with enough time can still crack a basic code just by hunting for common letters. To truly protect your secrets and buy yourself time, you need to level up.

Enter *superencipherment*, a very long word for a very smart trick: layering your codes. Instead of encrypting your secret note just once, you scramble it, and then you scramble that new message a second time.

First, run your plaintext through your keyword alphabet. Then, take that gibberish and run it through a shift cipher, sliding every letter down three spaces. The letter "E" might turn into "J", and then morph into "M".

A snooper now has to beat two puzzles at once! Just remember to use completely different rules for each layer. If you encrypt a note twice with the exact same method, mathematically, you might even accidentally decrypt it!

The MIDNIGHT Alphabet

SECRET ALPHABET

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

MESSAGE

DOUBLE THE SECRET

↓

SECRET

NLUIFG SAG RGDQGS

A second keyword, MIDNIGHT, makes a brand-new secret alphabet. Swap keys often to stay ahead of crackers.

SPY FILE

Did You Know?

The National Security Agency has a strict regulation called the Rule of Two, requiring all top-secret data to be protected by two completely independent layers of cryptography.

Puzzle Break

Grab a pencil — decode the secret message.

CRACK THIS #10

SUBSTITUTION

SQURS KL LKG IUS JLJ

Hint · *This one uses the MIDNIGHT alphabet. Line the code letters up under it.*

ANSWER IN THE BACK OF THE BOOK

Stuck? Every solution is in the answer key at the back of the book.

The Unwritten Rules of Spycraft

Even the most brilliant code is useless if someone catches you handing the note to your friend. Real operatives never swap secrets face-to-face. Instead, they use a dead drop—a pre-selected hiding spot like a hollow tree. You hide the note, leave, and your partner picks it up later.

To pull this off, you must follow the unwritten rules of tradecraft. First, agree on your hiding spot and your cipher key in person before you need them. Second, keep your messages short. Third, never, ever hide your key in the same spot as your encrypted note!

How does your partner know a message is waiting? You leave a signpost. It could be a piece of tape on your locker or a specific book on your desk. Once they see the signal, they know to check the drop spot alone.

But the absolute most important rule of operational security isn't about hiding things—it's about why you write them. Secret codes are for solving mysteries and sharing jokes. They are never for being mean or leaving classmates out. In real spycraft, kindness is your best disguise.

A Quick Caesar Recap

SHIFT +7

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

MESSAGE

TRUST YOUR TEAM

↓

SECRET

AYBZA FVBY ALHT

Even a simple seven-step Caesar shift keeps a note secret from anyone who does not know the number.

SPY FILE

Did You Know?

In 1985, traitor Aldrich Ames signaled his Russian handlers simply by drawing a chalk line over the USPS logo on a public blue mailbox in Washington, D.C.

Puzzle Break

Grab a pencil — decode the secret message.

CRACK THIS #12

SUBSTITUTION

RCO USTIR ALDO EQ KEKO

Hint · *Back to the SHADOW alphabet, and yes, spell out the number.*

ANSWER IN THE BACK OF THE BOOK

Stuck? Every solution is in the answer key at the back of the book.

The World Runs on Codes

The ciphers you've built in this chapter aren't just ancient history. From secret alphabets to layered messages and dead drops, the spycraft you just practiced is the exact foundation of our modern digital world. You are using the great-grandparents of modern computer security.

Every single time you type a password into a video game or your parents check their bank account online, invisible codes go to work. They use the very same principles of substitution and layering that you just learned, only sped up millions of times by tiny silicon chips.

Even the wealthiest tech companies face the exact same problems you do: keeping the key safe. A mathematically brilliant digital code is completely useless if someone accidentally leaves the password written on a sticky note. That is why physical spycraft still matters today.

Now it is your turn. Invent your own cipher keys, hide them well, and set up a dead drop with a friend. Keep practicing, use your codes for fun rather than being mean, and above all else—tell no one.

SPY FILE

Did You Know?

By hiding a paper cipher key under your mattress, you are practicing "key management"—the exact same physical security problem that multi-billion dollar tech companies face today!

Answer Key

No peeking until you have really tried! Here is what every **Crack This** puzzle actually said.

#1 MEET ME AT THE TREEHOUSE
CAESAR

#2 THE PASSWORD IS DRAGON
CAESAR

#3 LOOK UNDER THE THIRD STAIR
CAESAR

#4 BRING SNACKS TO THE FORT
PIGPEN

#5 HELP IS COMING
MORSE

#6 THE DOG ATE MY HOMEWORK
PIGPEN

#7 MOVE AT DAWN
MORSE

#8 THE EAGLE HAS LANDED
CAESAR

#9 GUARD THE SECRET RECIPE
KEYWORD

#10 TRUST NO ONE BUT MOM
KEYWORD

#11 ABORT NOW
MORSE

#12 THE VAULT CODE IS NINE
KEYWORD