# Caesar Cipher

The Caesar cipher *(or Caesar code)* is a **monoalphabetic substitution** cipher, where each letter is replaced by another letter located a little further in the alphabet *(therefore shifted but always the same for given cipher message).*

The shift distance is chosen by a number called the offset, which can be right *(A to B)* or left *(B to A)*.

For every shift to the right *(of +N*), there is an equivalent shift to the left *(of 26-N)* because the alphabet rotates on itself, the Caesar code is therefore sometimes called a **rotation cipher**.

One clue: ‘e’ is the most common character in English language.

Puzzle #1

Encrypted: Gurer’f ab fvyire ohyyrg va plorefrphevgl; bayl ynlrerq qrsrafr jbexf.

Puzzle #2

Encrypted: Vhfxulwb xvhg wr eh dq lqfrqyhqlhqfh; qrz lw’v hvvhqwldo.

**PigPen Cipher**

What is the PigPen cipher? The Pig Pen Cipher, also known as the Freemason Cipher *(or masonic alphabet)*, is an encryption system that was historically used by some members of Freemasonry to protect their communications.

It is based on a special arrangement of letters in a grid *(cross or grid like*[*tic tac toe*](https://www.dcode.fr/tic-tac-toe-cipher)*)* in order to use 26 symbols to represent the letters of the alphabet by substitution.

A screenshot of a puzzle

AI-generated content may be incorrect.

PigPen Puzzle #1

char(87)char(65)char(78)char(84)   char(84)char(79)   char(75)char(69)char(69)char(80)   char(89)char(79)char(85)char(82)   char(79)char(78)char(76)char(73)char(78)char(69)   char(80)char(82)char(73)char(86)char(65)char(67)char(89)   char(83)char(84)char(65)char(89)   char(79)char(70)char(70)   char(84)char(72)char(69)   char(73)char(78)char(84)char(69)char(82)char(78)char(69)char(84)

Puzzle #2

char(72)char(85)char(65)char(78)char(83)   char(65)char(82)char(69)   char(84)char(72)char(69)   char(87)char(69)char(65)char(75)char(69)char(83)char(84)   char(76)char(73)char(78)char(75)   char(73)char(78)   char(65)char(78)char(89)   char(83)char(69)char(67)char(85)char(82)char(73)char(84)char(89)   char(67)char(72)char(65)char(73)char(78)

Rail Fence Cipher

What is Rail Fence cipher? The Rail Fence *(or zig-zag)* cipher is a transposition cipher that involves writing text in a wave pattern across multiple lines and reading it line by line to obtain the encrypted message.

How to encrypt using Rail Fence cipher? The Rail Fence cipher follows these steps:

— Define a number of levels N *(or rows or floors),* this number is sometimes called the cipher key.

— Write the message following a sawtooth pattern *(alternating up and down)* along a path of N levels/floors.

Example: Encode DCODEZIGZAG with N=3:

|  |
| --- |
| D---E---Z-- |
| -C-D-Z-G-A- |
| --O---I---G |

— Read the message line by line to obtain the encrypted text.

Example: The encrypted message is DEZCDZGAOIG

How to decrypt Rail Fence cipher? Deciphering Rail Fence requires knowing the number of levels N and is broken down into three steps:

Example: Decipher the message DEZCDZGAOIG and N=3

— Reconstruct the zigzag pattern with the expected number of levels.

Example:

|  |
| --- |
| X---X---X-- |
| -X-X-X-X-X- |
| --X---X---X |

— Write the numbered letters in the pattern, line by line.

Example:

|  |
| --- |
| D---E---Z-- |
| -C-D-Z-G-A- |
| --O---I---G |

— Read the letters along the zigzag path to reconstruct the original message.

Example: The plain text is DCODEZIGZAG.

Rail Fence Puzzle #1 (Height =3) :

PASOOIAIGRVCINTPINLTSBSCIHIYOTAIART

Puzzle #2 (Height =4):

TNESHGLUHIGRWIEGINESYGIIKAIALNUSARUMSDDNFLODOIE

Atbash Cipher

What is Atbash cipher? Atbash cipher *(also called mirror cipher or backwards alphabet or reverse alphabet)* is the name given to a monoalphabetical substitution cipher which owes its name and origins to the Hebrew alphabet.

Atbash replaces each letter with its symmetrical one in the alphabet, that is, A becomes Z, B becomes Y, and so on.

How to encrypt using Atbash cipher? Atbash encryption uses a substitution alphabet and its reciprocal, a combination of the normal alphabet and its reverse alphabet *(mirrored).*

Example: The latin alphabet ABCDEFGHIJKLMNOPQRSTUVWXYZ and its reverse: ZYXWVUTSRQPONMLKJIHGFEDCBA are combine in the substitution table:

|  |  |
| --- | --- |
| Normal | ABCDEFGHIJKLMNOPQRSTUVWXYZ |
| Reverse | ZYXWVUTSRQPONMLKJIHGFEDCBA |

Encryption consists in replacing letters from the first with letters from the other one, with is equivalent to replace the first letter of the alphabet A with the last one Z, the second one B with the penultimate Y etc.

Example: MIRROR becomes NRIILI

How to decrypt Atbash cipher? Decryption is identical to encryption because of the reversible alphabet *(due to the symmetry of the backwards alphabet)*

Example: ZGYZHS is decrypted ATBASH

Atbash Puzzle #1

Szxpvih wlm’g mvvw blfi urmtvikirmg, qfhg gsv wzgz gszg ivkivhvmgh rg.

Puzzle #2

Lmob ylirmt orevh xzm zuuliw gl trev fk kirezxb.

Polybius

What is the Polybius cipher? The Polybius cipher is a substitution cipher using a grid *(the Polybius square).* Invented in ancient times by the Greek general Polybius, it transforms each letter into a pair of coordinates according to its position in the grid.

How to encrypt using Polybius cipher? The Polybius square cipher uses a 5x5 grid of letters with rows and columns marked with numerical coordinates from 1 to 5.

Example:

| \ | **1** | **2** | **3** | **4** | **5** |
| --- | --- | --- | --- | --- | --- |
| **1** | A | B | C | D | E |
| **2** | F | G | H | I | K |
| **3** | L | M | N | O | P |
| **4** | Q | R | S | T | U |
| **5** | V | W | X | Y | Z |

— Associate each letter with a pair of numbers corresponding to its coordinates in the grid (row, column).

— Replace each letter of the plain text with its pair of numbers to obtain the encrypted message.

Example: Encode DCODE with the grid above: D is located in row 1, column 4, it is coded 14; C is located in row 1, column 3, it is coded 13. The encrypted DCODE message is 14,13,34,14,15

How to generate Polybius' square grid?

The grid is limited to 25 letters while the Latin alphabet has 26, so one letter must be omitted. Usually, I and J merge to fit in the 25 boxes, but sometimes it is U and V or even the Z that is omitted.

In addition, the position of the letters in the grid defines the encrypted message, it is recommended to mix the letters in the grid, one method is to use a password to generate a disordered alphabet that will be used to fill the grid.

In his original version, Polybius describes the grid with 24 characters of the Greek alphabet

| \ | **1** | **2** | **3** | **4** | **5** |
| --- | --- | --- | --- | --- | --- |
| **1** | A | B | Γ | Δ | E |
| **2** | Z | H | Θ | I | K |
| **3** | Λ | M | N | Ξ | O |
| **4** | Π | P | Σ | T | Y |
| **5** | Φ | X | Ψ | Ω |  |

How to decrypt Polybius cipher? Polybius decryption requires to know the grid and consists in a substitution of couples of coordinates by the corresponding letter in the grid.

Example: The message to decrypt is 351332542114 with the grid *(created with DCODE as key & without letter J):*

| \ | **1** | **2** | **3** | **4** | **5** |
| --- | --- | --- | --- | --- | --- |
| **1** | D | C | O | E | A |
| **2** | B | F | G | H | I |
| **3** | K | L | M | N | P |
| **4** | Q | R | S | T | U |
| **5** | V | W | X | Y | Z |

Split the message in bigrams, couples of numbers that are the coordinates of each plain text letter.

Example: 35,13,32,54,21,14, 35 stands for 3rd row, 5th column, so letter P, and so on. The plain message is POLYBE.

| \ | **1** | **2** | **3** | **4** | **5** |
| --- | --- | --- | --- | --- | --- |
| **1** | A | B | C | D | E |
| **2** | F | G | H | I | K |
| **3** | L | M | N | O | P |
| **4** | Q | R | S | T | U |
| **5** | V | W | X | Y | Z |

Polybius Puzzle #1

113211441545424323111325435443441532433542342115434324343311314323111325351534353115

Puzzle #2

44424543442443442315453144243211441551453133154211122431244454243313541215424315134542244454

Answer Key:

Caesar #1 (ROT 13) There’s no silver bullet in cybersecurity; only layered defense works.

Caesar #2 (ROT 29) Security used to be an inconvenience; now it’s essential.

Pigpen #1 Want to keep your online privacy? Stay off the internet.

Pigpen #2 Humans are the weakest link in any security chain.

Rail Fence #1 Privacy is not optional—it is a basic right.

Rail Fence #2 Thinking a firewall is enough is dangerously misguided.

Atbash #1 Hackers don’t need your fingerprint, just the data that represents it.

Atbash #2 Only boring lives can afford to give up privacy.

Polybius #1 Amateurs hack systems. Professionals hack people.

Polybius #2 Trust is the ultimate vulnerability in cybersecurity