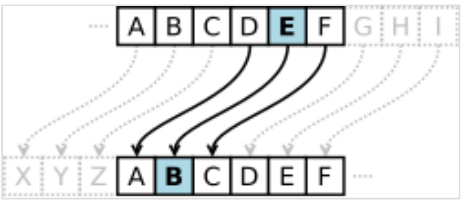
WIKIPEDIA
The Free Encyclopedia

Caesar cipher

A **Caesar cipher**[a] is one of the simplest and most widely known encryption techniques used in cryptography. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a left shift of 3, D would be replaced by A, E would become B, and so on.[1] The method is named after Julius Caesar, who used it in his private correspondence.



The action of a Caesar cipher is to replace each plaintext letter with a different one a fixed number of places down the alphabet. The cipher illustrated here uses a left shift of 3, so that (for example) each occurrence of E in the plaintext becomes B in the ciphertext.

The encryption step performed by a Caesar cipher is often incorporated as part of more complex schemes, such as the Vigenère cipher, and still has modern application in the ROT13 system. As with all single-alphabet substitution ciphers, the Caesar cipher is easily broken and in modern practice offers essentially no communications security.

Example

The transformation can be represented by aligning two alphabets; the cipher is the plain alphabet rotated left or right by some number of positions. For instance, here is a Caesar cipher using a left rotation of three places, equivalent to a right shift of 23 (the shift parameter is used as the key):

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

When encrypting, a person looks up each letter of the message in the "plain" line and writes down the corresponding letter in the "cipher" line.

```
Plaintext:  THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG
Ciphertext: QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD
```

Deciphering is done in reverse, with a left shift of 3.

The encryption can also be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A → 0, B → 1, ..., Z → 25.[2] Encryption of a letter x by a shift n can be described mathematically as,[3][4]

$$E_n(x) = (x + n) \mod 26.$$

Decryption is performed similarly,

$$D_n(x) = (x - n) \mod 26.$$

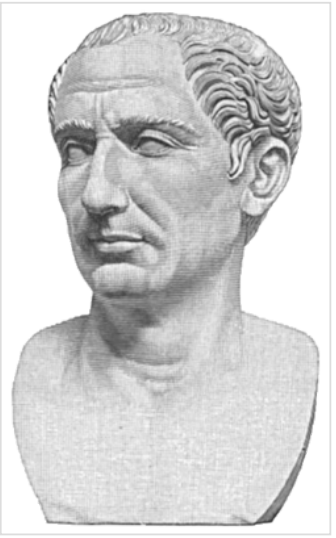
(Here, "mod" refers to the modulo operation. The value x is in the range 0 to 25, but if $x + n$ or $x - n$ are not in this range then 26 should be added or subtracted.)

The replacement remains the same throughout the message, so the cipher is classed as a type of *monoalphabetic substitution*, as opposed to *polyalphabetic substitution*.

History and usage

The Caesar cipher is named after Julius Caesar, who, according to Suetonius, used it with a shift of three (A becoming D when encrypting, and D becoming A when decrypting) to protect messages of military significance.[5] While Caesar's was the first recorded use of this scheme, other substitution ciphers are known to have been used earlier.[6][7]

> "If he had anything confidential to say, he wrote it in cipher, that is, by so changing the order of the letters of the alphabet, that not a word could be made out. If anyone wishes to decipher these, and get at their meaning, he must substitute the fourth letter of the alphabet, namely D, for A, and so with the others."
>
> —Suetonius, *Life of Julius Caesar* 56



The Caesar cipher is named for Julius Caesar, who used an alphabet where decrypting would shift three letters to the left.

His nephew, Augustus, also used the cipher, but with a right shift of one, and it did not wrap around to the beginning of the alphabet:

> "Whenever he wrote in cipher, he wrote B for A, C for B, and the rest of the letters on the same principle, using AA for Z."
>
> —Suetonius, *Life of Augustus* 88

Evidence exists that Julius Caesar also used more complicated systems,[8] and one writer, Aulus Gellius, refers to a (now lost) treatise on his ciphers:

> "There is even a rather ingeniously written treatise by the grammarian Probus concerning the secret meaning of letters in the composition of Caesar's epistles."
>
> —Aulus Gellius, *Attic Nights 17.9.1–5*

It is unknown how effective the Caesar cipher was at the time; there is no record at that time of any techniques for the solution of simple substitution ciphers. The earliest surviving records date to the 9th-century works of Al-Kindi in the Arab world with the discovery of frequency analysis.[9]

A piece of text, encrypted in a Hebrew version of the Caesar cipher not to be confused with Atbash, is sometimes found on the back of Jewish mezuzah scrolls. When each letter is replaced with the letter before it in the Hebrew alphabet, the text translates as "YHWH, our God, YHWH", a quotation from the main part of the scroll.[10][11]

In the 19th century, the personal advertisements section in newspapers would sometimes be used to exchange messages encrypted using simple cipher schemes. David Kahn (1967) describes instances of lovers engaging in secret communications enciphered using the Caesar cipher in *The Times*.[12] Even as late as 1915, the Caesar cipher was in use: the Russian army employed it as a replacement for more complicated ciphers which had proved to be too difficult for their troops to master; German and Austrian cryptanalysts had little difficulty in decrypting their messages.[13]

Caesar ciphers can be found today in children's toys such as secret decoder rings. A Caesar shift of thirteen is also performed in the ROT13 algorithm, a simple method of obfuscating text widely found on Usenet and used to obscure text (such as joke punchlines and story spoilers), but not seriously used as a method of encryption.[14]

The Vigenère cipher uses a Caesar cipher with a different shift at each position in the text; the value of the shift is defined using a repeating keyword.[15] If the keyword is as long as the message, is chosen at random, never becomes known to anyone else, and is never reused, this is the one-time pad cipher, proven unbreakable. However the problems involved in using a random key as long as the message make the one-time pad difficult to use in practice. Keywords shorter than the message (e.g., "Complete Victory" used by the Confederacy during the American Civil War), introduce a cyclic pattern that might be detected with a statistically advanced version of frequency analysis.[16]

Caesar cipher translated to a disk has both outer and inner plates having alphabets in the same direction and not the reverse as seen in CipherDisk2000.

In April 2006, fugitive Mafia boss Bernardo Provenzano was captured in Sicily partly because some of his messages, clumsily written in a variation of the Caesar cipher, were broken. Provenzano's cipher used numbers, so that "A" would be written as "4", "B" as "5", and so on.[17]

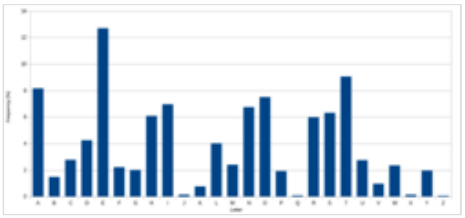
In 2011, Rajib Karim was convicted in the United Kingdom of "terrorism offences" after using the Caesar cipher to communicate with Bangladeshi jihadi activists discussing plots to blow up British Airways planes or disrupt their IT networks. Although the parties had access to far better encryption techniques (Karim himself used PGP for data storage on computer disks), they chose to use their own scheme (implemented in Microsoft Excel), rejecting a more sophisticated code program called Mujahedeen Secrets "because 'kaffirs', or non-believers, know about it, so it must be less secure".[18]

Breaking the cipher

The Caesar cipher can be easily broken even in a ciphertext-only scenario. Since there are only a limited number of possible shifts (25 in English), an attacker can mount a brute force attack by deciphering the message, or part of it, using each possible shift. The correct decryption will be the one which makes sense in the language of the plaintext.[19] An example is shown on the right for the ciphertext "`exxegoexsrgi`"; the candidate plaintext for shift four, "`attackatonce`", is the only one which makes sense as English text. Another type of brute force attack is to write out the alphabet beneath each letter of the ciphertext, starting at that letter. Again the correct decryption is the one which makes sense as English text. This technique is sometimes known as "completing the plain component".[20][21]

Decryption shift	Candidate plaintext
0	`exxegoexsrgi`
1	`dwwdfndwrqfh`
2	`cvvcemcvqpeg`
3	`buubdlbupodf`
4	`attackatonce`
5	`zsszbjzsnmbd`
6	`yrryaiyrmlac`
...	
23	`haahjrhavujl`
24	`gzzgiqgzutik`
25	`fyyfhpfytshj`

Another approach is to match up the frequency distribution of the letters. By graphing the frequencies of letters in the ciphertext, and by knowing the expected distribution of those letters in the original language of the plaintext, a human can easily spot the value of the shift by looking at the displacement of particular features of the graph. This is known as frequency analysis. For example, in the English language the plaintext frequencies of the letters `E`, `T`, (usually most frequent), and `Q`, `Z` (typically least frequent) are particularly distinctive.[22] Computers can automate this process by assessing the similarity between the observed frequency distribution and the expected distribution. This can be achieved, for instance, through the utilization of the chi-squared statistic[23] or by minimizing the sum of squared errors between the observed and known language distributions.[24]



The distribution of letters in a typical sample of English language text has a distinctive and predictable shape. A Caesar shift "rotates" this distribution, and it is possible to determine the shift by examining the resultant frequency graph.

The unicity distance for the Caesar cipher is about 2, meaning that on average at least two characters of ciphertext are required to determine the key.[25] In rare cases more text may be needed. For example, the words "`river`" and "`arena`" can be converted to each other with a Caesar shift, which means they can produce the same ciphertext with different shifts. However, in practice the key can almost certainly be found with at least 6 characters of ciphertext.[26]

With the Caesar cipher, encrypting a text multiple times provides no additional security. This is because two encryptions of, say, shift *A* and shift *B* will be equivalent to a single encryption with shift *A* + *B*. In mathematical terms, the set of encryption operations under each possible key forms a group under composition.[27]

See also

- Scytale – Encryption tool used to perform a transposition cipher

Notes

a. also known as Caesar's cipher, the shift cipher, Caesar's code, or Caesar shift

References

1. Smith, James (2021-11-30). "Writing Secret Messages With a Caesar Cipher" (https://golangprojectstructure.com/caesar-cipher-secret-messages/). *Golang Project Structure*. Archived (https://web.archive.org/web/20241105025547/https://golangprojectstructure.com/caesar-cipher-secret-messages/) from the original on 2024-11-05. Retrieved 2024-10-20.
2. Luciano, Dennis; Gordon Prichett (January 1987). "Cryptology: From Caesar Ciphers to Public-Key Cryptosystems". *The College Mathematics Journal*. **18** (1): 2–17. CiteSeerX 10.1.1.110.6123 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.110.6123). doi:10.2307/2686311 (https://doi.org/10.2307%2F2686311). JSTOR 2686311 (https://www.jstor.org/stable/2686311).
3. Wobst, Reinhard (2001). *Cryptology Unlocked* (https://archive.org/details/Cryptology_Unlocked). Wiley. p. 19. ISBN 978-0-470-06064-3.
4. "Caesar Cipher" (https://solidify.software/posts/caesar-cipher). *Solidify Software*. Archived (https://web.archive.org/web/20250621223017/https://solidify.software/posts/caesar-cipher) from the original on 2025-06-21. Retrieved 2025-06-21.
5. Suetonius. "56.6". *Vita Divi Julii* (http://thelatinlibrary.com/suetonius/suet.caesar.html#56) (in Latin).
6. "Cracking the Code" (https://web.archive.org/web/20201226065538/https://www.cia.gov/news-information/featured-story-archive/2007-featured-story-archive/cracking-the-code.html). *Central Intelligence Agency*. Archived from the original (https://www.cia.gov/news-information/featured-story-archive/2007-featured-story-archive/cracking-the-code.html) on 26 December 2020. Retrieved 21 February 2017.
7. Singh, Simon (2000). *The Code Book*. Anchor. pp. 289–290 (https://archive.org/details/codebook00simo/page/289). ISBN 0-385-49532-3.
8. Reinke, Edgar C. (December 1962). "Classical Cryptography". *The Classical Journal*. **58** (3): 114.
9. Singh, Simon (2000). *The Code Book*. Anchor. pp. 14–20 (https://archive.org/details/codebook00simo/page/14). ISBN 0-385-49532-3.
10. Eisenberg, Ronald L. (2004). *Jewish Traditions* (1st ed.). Philadelphia: Jewish Publication Society. p. 582. ISBN 9780827610392.
11. Sameth, Mark (2020). *The Name : a history of the dual-gendered Hebrew name for God*. Eugene, Oregon: Wipf & Stock. pp. 5–6. ISBN 9781532693830.

12. Kahn, David (1967). *The Codebreakers*. pp. 775–6. ISBN 978-0-684-83130-5.
13. Kahn, David (1967). *The Codebreakers*. pp. 631–2. ISBN 978-0-684-83130-5.
14. Wobst, Reinhard (2001). *Cryptology Unlocked* (https://archive.org/details/Cryptology_Unlocked). Wiley. p. 20. ISBN 978-0-470-06064-3.
15. Kahn, David (1967). *The Codebreakers*. pp. 148–149. ISBN 978-0-684-83130-5.
16. Kahn, David (1967). *The Codebreakers*. pp. 398–400. ISBN 978-0-684-83130-5.
17. Leyden, John (2006-04-19). "Mafia boss undone by clumsy crypto" (https://www.theregister.co.uk/2006/04/19/mafia_don_clueless_crypto/). *The Register*. Retrieved 2008-06-13.
18. "BA jihadist relied on Jesus-era encryption" (https://www.theregister.co.uk/2011/03/22/ba_jihadist_trial_sentencing/). *The Register*. 2011-03-22. Retrieved 2011-04-01.
19. Beutelspacher, Albrecht (1994). *Cryptology*. Mathematical Association of America. pp. 8–9. ISBN 0-88385-504-6.
20. Leighton, Albert C. (April 1969). "Secret Communication among the Greeks and Romans". *Technology and Culture*. **10** (2): 139–154. doi:10.2307/3101474 (https://doi.org/10.2307%2F3101474). JSTOR 3101474 (https://www.jstor.org/stable/3101474).
21. Sinkov, Abraham; Paul L. Irwin (1966). *Elementary Cryptanalysis: A Mathematical Approach*. Mathematical Association of America. pp. 13–15. ISBN 0-88385-622-0.
22. Singh, Simon (2000). *The Code Book* (https://archive.org/details/codebook00simo/page/72). Anchor. pp. 72–77 (https://archive.org/details/codebook00simo/page/72). ISBN 0-385-49532-3.
23. Savarese, Chris; Brian Hart (2002-07-15). "The Caesar Cipher" (http://www.cs.trincoll.edu/~crypto/historical/caesar.html). Trinity College. Archived (https://web.archive.org/web/20110813232738/http://www.cs.trincoll.edu/~crypto/historical/caesar.html) from the original on 2011-08-13. Retrieved 2008-07-16.
24. Eisele, Robert (2007-05-18). "Caesar Cipher Decryption" (https://raw.org/tool/caesar-cipher/). Archived (https://web.archive.org/web/20240324224211/https://raw.org/tool/caesar-cipher/) from the original on 2024-03-24. Retrieved 2024-04-02.
25. Lubbe, Jan C. A. (12 March 1998). *Basic Methods of Cryptography*. Cambridge University Press. pp. 47–8. ISBN 9780521555593.
26. Pardo, José Luis Gómez (19 December 2012). *Introduction to Cryptography with Maple*. Springer Berlin Heidelberg. p. 5. ISBN 9783642321665.
27. Wobst, Reinhard (2001). *Cryptology Unlocked* (https://archive.org/details/Cryptology_Unlocked). Wiley. p. 31. ISBN 978-0-470-06064-3.

Bibliography

- Kahn, David (1996). *The Codebreakers: The Story of Secret Writing* (https://archive.org/details/codebreakersstor0000kahn_k4s3) (Revised ed.). New York. ISBN 0-684-83130-9. OCLC 35159231 (https://search.worldcat.org/oclc/35159231).
- Chris Savarese and Brian Hart, *The Caesar Cipher (http://www.cs.trincoll.edu/~crypto/historical/caesar.html)*, Trinity College, 1999

Further reading

- Bauer, Friedrich Ludwig (2000). *Decrypted Secrets: Methods and Maxims of Cryptology* (2nd and extended ed.). Berlin: Springer. ISBN 3-540-66871-3. OCLC 43063275 (https://search.worldcat.org/oclc/43063275).

External links

- Weisstein, Eric W. "Caesar's Method" (https://mathworld.wolfram.com/CaesarsMethod.html). *MathWorld*.
- Use this decoder, Agent 2S. (https://ciphersonline.com/es/cifrado-cesar)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Caesar_cipher&oldid=1328217364"