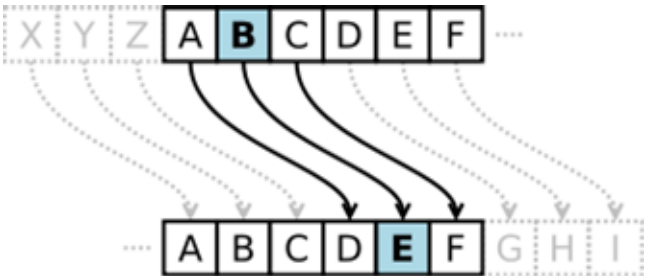
Caesar cipher

Caesar cipher



The action of a Caesar cipher is to replace each plaintext letter with one fixed number of places down the alphabet. This example is with a shift of three, so that a B in the plaintext becomes E in the cipher text.

Detail

Structure substitution cipher

Best public cryptanalysis

Susceptible to frequency analysis and brute force attacks.

In cryptography, a **Caesar cipher**, also known as a **Caesar's cipher**, the **shift cipher**, **Caesar's code** or **Caesar shift**, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plain text is replaced by a letter some fixed number of positions down the alphabet. For example, with a shift of 3, A would be replaced by D, B would become E, and so on. The method is named after Julius Caesar, who used it to communicate with his generals.

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 communication security.

Example

The transformation can be represented by aligning two alphabets; the cipher alphabet 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 (the shift parameter, here 3, is used as the key):

```
Plain:    ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher:   DEFGHIJKLMNOPQRSTUVWXYZABC
```

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. Deciphering is done in reverse.

```
Cipher text: WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ
```

```
Plaintext:  the quick brown fox jumps over the lazy dog
```

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.[1] Encryption of a letter *x* by a shift *n* can be described mathematically as,[2]

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

Decryption is performed similarly,

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

(There are different definitions for the modulo operation. In the above, the result is in the range 0...25. I.e., if *x*+*n* or *x*-*n* are not in the range 0...25, we have to subtract or add 26.)

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 for Julius Caesar, who used an alphabet with a left shift of three.

The Caesar cipher is named after Julius Caesar, who, according to Suetonius, used it with a shift of three to protect messages of military significance. While Caesar's was the first recorded use of this scheme, other substitution ciphers are known to have been used earlier.

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.

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 X.

There is evidence that Julius Caesar used more complicated systems as well, 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.

It is unknown how effective the Caesar cipher was at the time, but it is likely to have been reasonably secure, not least because most of Caesar's enemies would have been illiterate and others would have assumed that the messages were written in an

unknown foreign language.[4] 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. A Caesar cipher with a shift of one is used on the back of the Mezuzah to encrypt the names of God. This may be a holdover from an earlier time when Jewish people were not allowed to have Mezuzahs. The letters of the cryptogram themselves comprise a religiously significant "divine name" which Orthodox belief holds keeps the forces of evil in check.

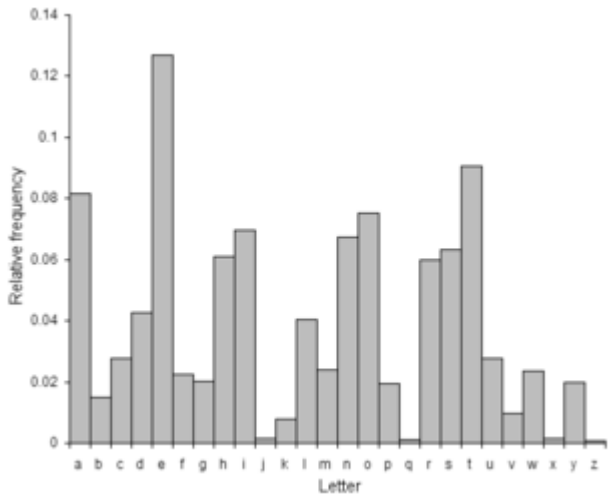
Breaking the cipher

The Caesar cipher can be easily broken even in a cipher text-only scenario. Two situations can be considered:

1. an attacker knows (or guesses) that some sort of simple substitution cipher has been used, but not specifically that it is a Caesar scheme;
2. An attacker knows that a Caesar cipher is in use, but does not know the shift value.

In the first case, the cipher can be broken using the same techniques as for a general simple substitution cipher, such as frequency analysis or pattern words.[13] While solving, it is likely that an attacker will quickly notice the regularity in the solution and deduce that a Caesar cipher is the specific algorithm employed.

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



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.

In the second instance, breaking the scheme is even more straightforward. Since there are only a limited number of possible shifts (26 in English), they can each be tested in turn in a brute force attack.[14] One way to do this is to write out a snippet of the ciphertext in a table of all possible shifts. - a technique sometimes known as "completing the plain component".[16] The example given is for the ciphertext "EXXEGOEXSRGI"; the plaintext is instantly recognisable by eye at a shift of four. Another way of viewing this method is that, under each letter of the ciphertext, the entire alphabet is written out in reverse starting at that letter. This attack can be accelerated using a set of strips prepared with the alphabet written down them in reverse order. The strips are then aligned to form the ciphertext along one row, and the plaintext should appear in one of the other rows.

Another brute force 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. Computers can also do this by measuring how well the actual frequency distribution matches up with the expected distribution; for example, the chi-squared statistic can be used.[18]

For natural language plaintext, there will, in all likelihood, be only one plausible decryption, although for extremely short plaintexts, multiple candidates are possible. For example, the ciphertext MPQY could, plausibly, decrypt to either "aden" or "know" (assuming the plaintext is in English); similarly, "ALIIP" to "dolls" or "wheel"; and "AFCCP" to "jolly" or "cheer" (see also unicity distance).

Multiple encryptions and decryptions provide no additional security. This is because two encryptions of, say, shift *A* and shift *B*, will be equivalent to an encryption with shift *A* + *B*. In mathematical terms, the encryption under various keys forms a group.