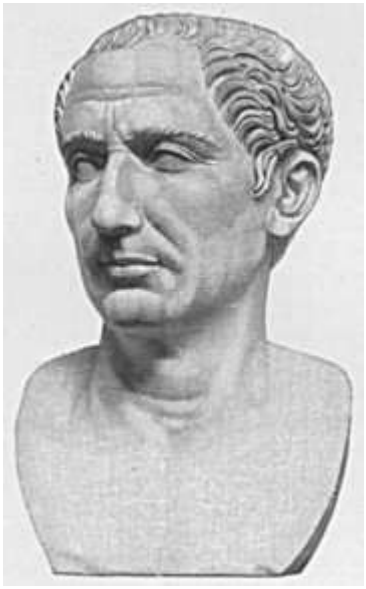
CAESAR

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:

> *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.*



While Caesar's was the first recorded use of this scheme, other substitution ciphers are known to have been used earlier. Julius Caesar's nephew Augustus also used the cipher, but with a shift of one:

> *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. — Suetonius, Life of Augustus 88.*

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. — Aulus Gellius, 17.9.1–5.*

It is unknown how effective the Caesar cipher was at the time, but it is likely to have been reasonably secure, not least because few of Caesar's enemies would have been literate, let alone able to consider cryptanalysis. Assuming that an attacker could read the message, 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 AD in the Arab world with the discovery of frequency analysis.

In the 19th Century, the personal advertisements section in newspapers would sometimes be used to exchange messages encrypted using simple cipher schemes. Kahn (1967) describes instances of lovers engaging in secret communications enciphered using the Caesar cipher in The Times. 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.

Caesar ciphers can be found today in children's toys such as secret decoder rings. A Caesar shift of 13 is also performed in the ROT13 algorithm, a simple method of obfuscating text used in some Internet forums to obscure text (such as joke punchlines and story spoilers), but not used as a method of encryption.

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. If the keyword were 1) chosen randomly and 2) was as long as the message (so that it did not repeat), the resultant system would be theoretically unbreakable — equivalent to the one-time pad cipher.

Usage

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 right rotation of three places (the shift parameter, here 3, is used as the key):

```
Plain:  abcdefghijklmnopqrstuvwxyz
Cipher: DEFGHIJKLMNOPQRSTUVWXYZABC
```

To encipher a message, simply look up each letter of the message in the "plain" line and write down the corresponding letter in the "cipher" line. To decipher, do the reverse.

```
Plaintext:  thequickbrownfoxjumpsoverthelazydog
Ciphertext: WKHTXLFNEURZQIRAMXPSVRYHUWKHODCBGRJ
```

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. Encryption of a letter x by a shift n can be described mathematically as,

Decryption is performed similarly,

[Excerpt from “Caesar cipher” at Wikipedia]