**Caesar Shift**

**History**

Invented by: Julius Casear

When: around 58BC

Why: To communicate with his army

**Key Generation**

Just pick a random number from 1-25

**Encoding Steps**

Using the key k, shift right all letters in plaintext in the alphabet k times. For example, using the alphabet “abcdefghijklmnopqrstuvwxyz” and with a key of 5, the letter “a” becomes “f” and “x” becomes “c”.

**Decoding Steps**

Using the key k, shift left all letters in ciphertext in the alphabet k times. For example, using the alphabet “abcdefghijklmnopqrstuvwxyz” and with a key of 5, the letter “f” becomes “a” and “c” becomes “x”.

**Security**

This is one of the least secure encryption methods ever, due to it only having 25 possible keys, meaning it can be brute forced by hand.

**Possible Attacks**

1. Brute Force
2. Frequency Analysis
3. Chi-Square Statistic (see website 5 for more info)

**Websites Used**

1. <https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/caesar-cipher>
2. <https://academic.oup.com/book/40641/chapter-abstract/348304993?redirectedFrom=fulltext>
3. <https://courses.cs.washington.edu/courses/cse490h1/19wi/exhibit/artifacts/crypto.pdf>
4. <https://www.secretcodebreaker.com/history2.html>
5. <http://www.cs.trincoll.edu/~crypto/historical/caesar.html>