**Substitution Cipher (simple)**

**History**

????

**Key Generation**

Shuffle letters in alphabet randomly, or in a chosen order. You may also choose a word, then remove all duplicate characters and append the rest of the alphabet to the end. For example, RIGHT would make the key: RIGHTABCDEFJKLMNOPQSUVWXYZ.

**Encoding Steps**

Using the key, swap letters from the plaintext using their position in the alphabet with whatever letter is in that position in the key. For example, using the key provided above, “A” would encode to “R” and “F” would encode to “A”

**Decoding Steps**

Using the key, swap letters from the ciphertext using their position in the key with whatever letter is in that position in the alphabet. For example, using the key provided above, “A” would decode to “F” and “F” would decode to “K”

**Security**

This is more secure than a Caesar Shift, however it can still be broken by brute force and is especially vulnerable to frequency analysis.

**Possible Attacks**

1. Brute Force (not by hand, on a fast computer)
2. Frequency Analysis

**Websites Used**

1. <https://en.wikipedia.org/wiki/Substitution_cipher#Simple>