**Monoalphabetic Substitution Ciphers**

*Substitution ciphers* are probably the most common form of cipher. They work by replacing each letter of the plaintext (and sometimes puntuation marks and spaces) with another letter (or possibly even a random symbol).   
  
A *monoalphabetic substitution cipher*, also known as a simple substitution cipher, relies on a fixed replacement structure. That is, the substitution is fixed for each letter of the alphabet. Thus, if "a" is encrypted to "R", then every time we see the letter "a" in the plaintext, we replace it with the letter "R" in the ciphertext.

A simple example is where each letter is encrypted as the next letter in the alphabet: "a simple message" becomes "B TJNQMF NFTTBHF". In general, when performing a simple substitution manually, it is easiest to generate the *ciphertext alphabet* first, and encrypt by comparing this to the plaintext alphabet. The table below shows how one might choose to, and we will, lay them out for this example.

[Picture](https://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/4433929_orig.jpg)

The ciphertext alphabet for the cipher where you replace each letter by the next letter in the alphabet

There are many different monoalphabetic substitution ciphers, in fact infinitely many, as each letter can be encrypted to any symbol, not just another letter.

The history of simple substitution ciphers can be traced back to the very earliest civisilisations, and for a long time they were more than adequate for the purposes for which they were needed. By today's standards they are very weak, and incredibly easy to break, but they were a very important step in developing cryptography.