1 Basics

Snake is a relatively simple system which adds elements of its key to the plaintext, with the addition being modulo some fixed base. Let the key be denoted by f, for instance, with base = 3, we might have $f = 021022012102$. Then $f[0] = 0, f[1] = 2, f[2] = 1, ...$

To compute a symbol, we do the following: Let p be the current plaintext value. Let x be the current position (reading head) of the key (the initial value of x is exactly the round number.) Let c be the next cipher text symbol. Then $c = p + f[x]$ and $x = x + p$. Note that $p + f[x]$ must be performed mod b, where b is the fixed base of the key. Note also that $x + p$ must be performed mod n, where n is the length of the key.

Changing the value of x is equivalent to a circular shift of the key.

The system assumes a round for each symbol in the key, and x is set to the number of the round. This is to get the most milage out of the key that we can (at least without doing anything complicated).

2 Motivation

This system is more of a toy or a sculpture than a serious tool. Nevertheless, the variable length key makes for a huge keyspace. The easiest way to use it is probably to use base-27, so that one has the alphabet and an all purpose punctuation symbol (I tend to use an underscore.)