Cyclone is a symmetric cryptosystem inspired loosely by the famous Enigma machine. The $n \times n$ square matrix key is best thought of as a cylinder of stacked wheels.

Each row or a "wheel" of the key is a permutation on $\{1, 2, 3, ..., n\}$ expressed in the abbreviated form of $[f(1) \quad f(2) \quad ...f(n-1) \quad f(n)]$. Let f_i be the permutation of row i.

Then $f = f_1 \circ f_2 \circ ...f_{n-1} \circ f_n$ is itself a permutation, and this f is used to transform a symbol of the plaintext into a symbol of the ciphertext. Note that this means f is invertible, which is necessary for decoding.

Then this f is shifted to the right in a circular fashion by the value of the plaintext symbol.

Finally, each row of the key is itself shifted using this shifted f. Row i is circularly rightshifted by the plaintext shifted $f(i)$.

Here's the crucial function for encoding a single round.

```
function encode(p,k)
    l = length(p)
    c = zeros(Symbol,l)
    n = size(k)[begin]
    s = zeros(Symbol,n)
    for i in 1:l
        f = getf(k,s)
        c[i] = f[p[i]]
        f = circshift(f,p[i])
        for j in 1:n s[j] = (f[j]+s[j])%n end
    end
    c
end
```

The s represents a state vector which only serves to make the computation more efficient. Instead of *actually* rotating the rows, the program uses s to track their virtual rotation.

This is the essence of the algorithm, but the encrypt function uses features like autospin and reversal to make an arbitrary number of rounds (hopefully) more effective.

When $n = 27$, the compositions f tend to be unique. So the key constantly wanders into a new state, meeting each symbol of plaintext

with a fresh permutation.