Cyclone is a symmetric cryptosystem inspired loosely by the famous Enigma machine (note that Glisten was the name of a variant). The key is an $n \times n$ square matrix key, and each row of this matrix is a permutation on $\{1, 2, 3, ..., n\}$, expressed in the abbreviated form of $f(1)f(2)...f(n-1)f(n)$.

Each element $k[i, j]$ represents the response of state i to finding the plaintext j. This response is both the cipher text symbol to be written **and** the next state of the machine. The cipher text is therefore a history of the machine's states.

This might sound insecure, but states as the plaintext is processed. We say that the permutation of row i (which we'll call f_i) is "rolled" by j, when j is added to each of its entries.

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 it is this f which 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. This means that the evolution of the key is intensely the function of the plaintext, so that small differences in the plaintext should lead to strong divergence in keystates, hopefully providing more security.