THORIUM

Thorium is a simple symmetric cryptosystem. It uses an $n \times n$ matrix of bits (sometimes ternary “bits”) as a key. This key is the initial state of the “machine,” and the rows and columns of this state matrix are circularly shifted as the plaintext as encoded. The trace of the matrix (the sum of the diagonal) is added (mod the base) to the plaintext symbol to get the ciphertext symbol. Then the rows and columns of the state matrix are circularly shifted using both their current diagonal entries and the plaintext symbol. Encoding is repeated for n rounds, and an “autospin” feature is used for extra security, so that the machine meets each round of encoding in a different state. This is accomplished by using the columns of the key as something like priming prefixes to the text to be (re)encoded.

Please note that Thorium and Cesium are basically the same system, but base-2 Thorium was its initial form, and I hope to do more with just the base 2 version, given its attractive simplicity.

The Julia implementation is easier to understand. This is not only because Julia is a high level language but also because of its ecellent built-in matrix support. I hope to pick up some Nim soon and add a Nim version.