The Talos Encryption Protocol

Steven Chiacchira

Abstract

This document describes the first draft of the mathematical specification of the Talos encryption protocol. If adopted, it will become the authoritative description of the algorithm's encryption and decryption processes. Any implementations which do not strictly conform to this document will be considered wholly noncompliant.

1 Formal Specification

Formal details are given in the main text of this document. Additional commentary providing context for definitions is given in separated blocks. An example of such a block is shown below.

> We suffer more in imagination than reality.
>
> — L. Annaeus Seneca

1.1 Definitions

Although definitions provided in this section may coincide with those of other, external, documents, this is not always the case. Many of these definitions carry specific restrictions or clauses as required by the design of the Talos algorithm. Thus, they are only meant to be understood in the context of this work unless otherwise specified.

1.1.1 Bit Strings

A **bit string** is an ordered, finite sequence of N bits $s_N = \{s_0, s_1, ...s_n\} \mid s_i \in \mathbb{Z}_2$.

> The talos specification (and indeed its reference implementation) do not prescribe an encoding for messages. This is to allow for encryption of various media types, including UTF-8 encoded text, images, videos, sound files, etc. Any message with a corresponding binary representation is compatible with this algorithm.

1.1.2 State Spaces, Evolution Rules, and Cellular Automata

An $N \times N$ **state space** is an $N \times N$ bit grid $\mathcal{S}_{N\times N} \in \mathbb{Z}_2^{N\times N}$.

An **evolution rule** is an endomorphic function $R : D \to D$ over any domain D. The repeated application of R to an element $d \in D$ N times is denoted as $R^N(d)$. That is,

$$\underbrace{R \circ R \circ ... R}_{\text{N times}}(d) = R^N(d)$$

An $N \times N$ **cellular automaton** is a tuple $A_{N\times N} = (R, S) \mid S \in \mathcal{S} \wedge R : \mathcal{S} \to \mathcal{S}$. R is said to be the evolution rule of A, and S is said to be the state of A.

1.2 Plaintext, Ciphertext, and Keys

Plaintexts, **ciphertexts**, and **encryption keys** are all special cases of bit strings.

A plaintext is a bit string with N bits s_N, where $N \in \{n * 256 \mid n \in \mathbb{N}\}$.

A ciphertext is a bit string with N bits s_N, where $N \in \{n * 256 \mid n \in \mathbb{N}\}$.

An encryption key is a bit string with 32 bits.

A plaintext is never considered a ciphertext, and a ciphertext is never considered a plaintext.

> Although plaintext and ciphertext share definitions, the two carry additional connotations from their usecases. A plaintext is informally considered sensitive, while a ciphertext is informally considered insensitive. Given plaintext P, derived ciphertext C, and associated encryption key K, P should be derivable from C if and only if K is known.