

**Prefix** is a symmetric cryptosystem based primarily on prefix codes, also known as instantaneous codes. Since the union of prefix codes is not in general itself a prefix code, this makes the encrypted output difficult to tokenize. Even the numbers of symbols transmitted is unclear.

It is often the case that a single plaintext symbol becomes several ciphertext symbols. So the output tends to be longer than the input. Yet this crypto system also occasionally compresses its input, replacing several symbols with just one. While this feature could be removed (in fact, simply by choosing  $e = 0$ ), leaving the system intact, it's a nice complement that only increases the unpredictable relationship between the length of the plaintext and the ciphertext.

I've included a simpler, Javascript version which may help programmers familiar with that language understand the Julia version. The actual encoding and decoding algorithms are fairly simple. Generating decent random keys is at least as complicated. The JS version doesn't include key generation, so it's the bare bones of Prefix.

I've also included sample computations created with a Typescript version. Studying these in relation to the key is probably the fastest/easiest way to understand the system.