

Revolver is just Prefix with an extra feature, which is to say a symmetric cryptosystem based primarily on prefix/instantaneous codes. Since the union of prefix codes is not in general itself a prefix code, this makes the encrypted output difficult to tokenize. Please see the pdf in **prefix-jl** repo to understand Prefix.

What Revolver adds is an evolution of the Prefix key that maintains its functionality. Essentially an entire mode's prefix code is “rolled” forward using both the plaintext and ciphertext so that it remains a prefix code. Its symbols are permuted. Actually the input code (not a prefix code) is also permuted, for a different but also compatible effect. This small tweak might (intuitively seems that it should) make the same key far more secure.