

Input: Sentence, Integer n

Pad sentence to 16-byte multiple

Encrypt sentence with AES (CBC mode, IV)

Encrypt AES key with Twofish

Extract first n bytes from Twofish key, encrypt with ChaCha20 (nonce)

Create modified Twofish key (remove first n bytes)

Output: AES ciphertext, Twofish-encrypted AES key, modified Twofish key, ChaCha20-encrypted bytes, nonce