Andy Chronister

Nikko Rush

Abstract

Current methods for encryption commonly use the factors of large numbers to generate keys; the authors propose a new approach that uses a cellular automaton to encrypt and decrypt the message, thus potentially future-proofing cryptographic algorithms for a time when computers will be able to find solutions to these problems, as certain classes of cellular automata have been proven to be sufficiently complex as to have no mathematical simplification. Messages are encrypted by running a cellular automaton seeded from the cryptographic key while performing sequential bitwise XOR operations. Decryption takes the seed used in the encryption, creates the cellular automaton with the proper number of generations, and works backwards from the encrypted message. Sets of 15,000 messages were generated in python, from which the frequency and value change of the messages were analyzed. Results show that the specific implementation used is vulnerable to somewhat incomplex methods of attack, primarily through analysis of encoded character data. Additional work will need to be performed to verify which features of the implementation result in the security vulnerabilities, as well as to conclusively determine whether or not a cellular automaton is a viable method of hard cryptographic encoding.