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. Messages are encrypted from a randomly seeded cellular automaton running for a random number of generations between 75 and 125. Decryption takes the seed used in the encryption and creates the cellular automaton with the proper number of generations and works backwards from the encrypted message. Sets of 10,000 messages were generated in python and then the frequency and value change of the messages was analyzed. Results show that the algorithm is not completely secure in its current state. Additional work will need to be performed to create a completely secure method of encryption.