Cellular Automata Based Stream Ciphers Homework

Prof. Alan Kaminsky
Department of Computer Science
Rochester Institute of Technology
Rochester, NY, USA
ark@cs.rit.edu

April 22, 2004

A plaintext consists of a sequence of 8-bit ASCII characters. The plaintext is encrypted using a Rule 30 Stream Cipher. The ciphertext consists of the following 8-bit characters:

10111010 00000100 10111110 10011111 00011101
01111111 10010101 01110100 01011001 11110111

The keystream is produced by a 16-cell Rule 30 cellular automaton with wraparound boundary conditions. The key (initial state) is:

10110000 00111010

The keystream comes from the leftmost cell. The first bit of the keystream is the initial state of the leftmost cell, the second bit of the keystream is the state of the leftmost cell after one step, the third bit of the keystream is the state of the leftmost cell after two steps, and so on.

Question 1. Give the sequence of keystream bits. Include enough bits to decrypt the above ciphertext.

Question 2. Give the sequence of plaintext bits obtained by decrypting the above ciphertext.

Question 3. Convert the plaintext bits from ASCII back to characters to answer this riddle:

Why couldn't the inmate call his lawyer? Because he didn't have a "_____".

(You can find an ASCII chart at `http://www.unicode.org/charts/PDF/U0000.pdf`.)