CSCI 251 – Introduction to Information Security, Laws, & Ethics

Spring 2012

HW2

Due Date 4/25/2012

Instruction: This is an individual assignment, sharing your answers with other students is not allowed. Write your answers on a separate sheet and make sure you include your name on each of the sheet that you will be submitting. To submit your assignment you have to use the online DropBox that is provided thru eCollege.

(100 points)

1. Implement the A5/1 algorithm in C/C++. Suppose that, after a particular step, the values in the registers are

$$X = (x_0, x_1, \ldots\ldots, x_{18}) = (1010101010101010101)$$
$$Y = (y_0, y_1, \ldots\ldots, y_{18}, y_{19}, y_{20}, y_{21}) = (1100110011001100110011)$$
$$Z = (z_0, z_1, \ldots\ldots, z_{18}, z_{19}, z_{20}, z_{21}, z_{22}) = (1110000111100001111000 0)$$

   List the next 32 key stream bits and give the contents of X, Y, and Z after these 32 bits have been generated