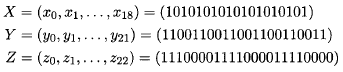
**CS 430 – Introduction to Computer Security**

**Project 1**

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



List the next 32 keystream bits and give the contents of X, Y, and Z after these 32 bits have been generated. Unless you are an expert in Java, it is better to use C.

1. Implement the Tiny Encryption Algorithm (TEA). Use your TEA algorithm to encrypt the 64-bit plaintext block

0x0123456789ABCDEF

using the 128-bit key

0xA56BABCD00000000FFFFFFFFABCDEF01

Decrypt the resulting ciphertext and verify that you obtain the original plaintext. The prefix 0x means hexadecimal integer.

*What to upload in a compressed folder (Canvas):**Your code, the results, your conclusions/observations.*