CPTS 515 HW3

Yang Zhang 11529139

1. a. Build a bipartite graph from the sample from C by finding the mapping from high bit to low bit

b. Run max flow algorithm over the bipartite graph to calculate the max matching number M.

c. apply the Theorem 2 from the paper Security of Numeric Sensors in Automata, the average Leaking bits is $\log(M)$

2. Write another program that take X as input and int[] $\{x_1, x_2, \dots, x_7\}$ as output.
the Logic of the program is the same as myFunction but in reversed order. Input a negative number X to the program. if there is a valid output int[]$\{x_1, x_2, \dots, x_7\}$ returned, then there are values for $x_1, x_2, \dots, x_7$ passed to the myFunction the can return a negative integer.

3. For a set $K = \{1, \cdots, k\}$ any subset p of k can be expressed as $\{b_1, \cdots, b_k\}$ where b_i is a boolean varible to indicate whether element k_i in the subset. (Using $b_i = 0$ for false, $b_i = 1$ for true) In this way each subset can be encoded in to a binary format

e.g. $\emptyset = \{0\}$

$$K = \{\underbrace{1, 1, 1, 1, \cdots, 1}_{k}\}$$

Then covert the binary reprensation into decimal integer where the bound is $[0, 2^k]$

Since each binary reprensation is unique, each converted decimal integer is also unique. (C is 1-1)

The number of subset of K is 2^k, so $C_p \in \{1, \cdots, B_K\}$

4. The number of boolean varible for nodes $= \log(2048) = 11$

11 varibles needed to encode every node, so $11 \times 2 = 22$ needed to encode the graph (each edge has two nodes)

5. $\log(40) \approx 6$, There are at least 6 bits needed to hash 40 students that each students has a unique hashcode assigned