CPSC 121 Lab 7 Pre-lab Brian Taylor

1. Substitution cipher, transposition cipher, block cipher

A substitution cipher is a cipher in which one character in plaintext is substituted for a character in cipher text. The substitution goes both ways and is consistent. For example, in a Caesar cipher (a type of substitution cipher) the plain text letter A might be substituted for the cipher text letter D, and the reverse will be true: the cipher text letter D will always be substituted for the plain text letter A.

A transposition cipher is a cipher in which the characters in the plain text message are shifted according to some system, pattern or function. An inverse system or function is required to decode the message. Examples are: ‘rail fence cipher’, ‘route cipher’, ‘columnar transposition’, ‘double transposition’.

A block cipher is a cipher in which the plaintext message is divided up into equal length blocks (for example blocks of 4 letters, or 8 bits) and then the blocks are encoded using an algorithm that produces a block of the same length.

1.2 prelab question

The circuit I designed is a substitution cipher, so it would be possible to be decrypted since a particular 3-bit input will always produce the same 3-bit output.