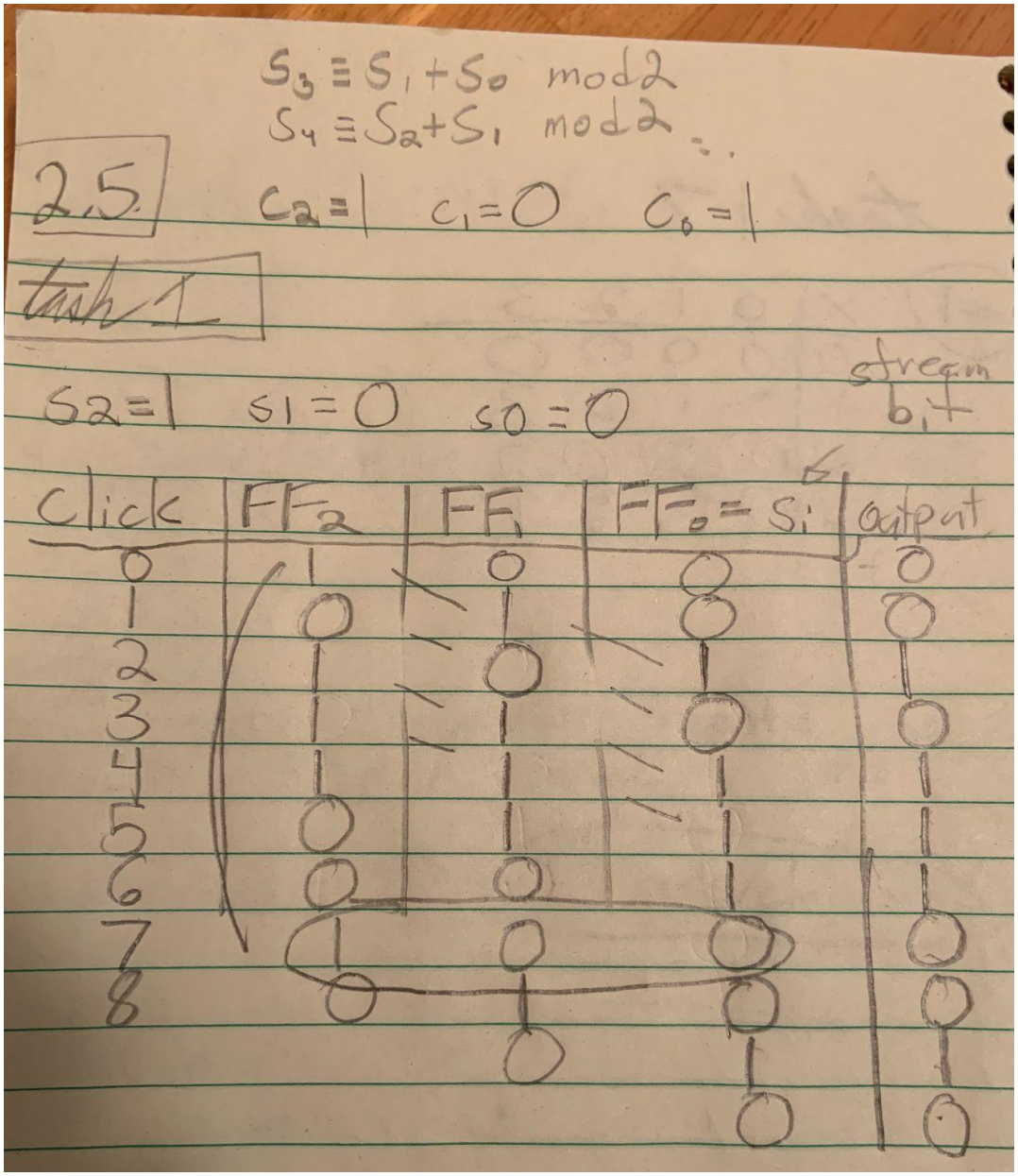
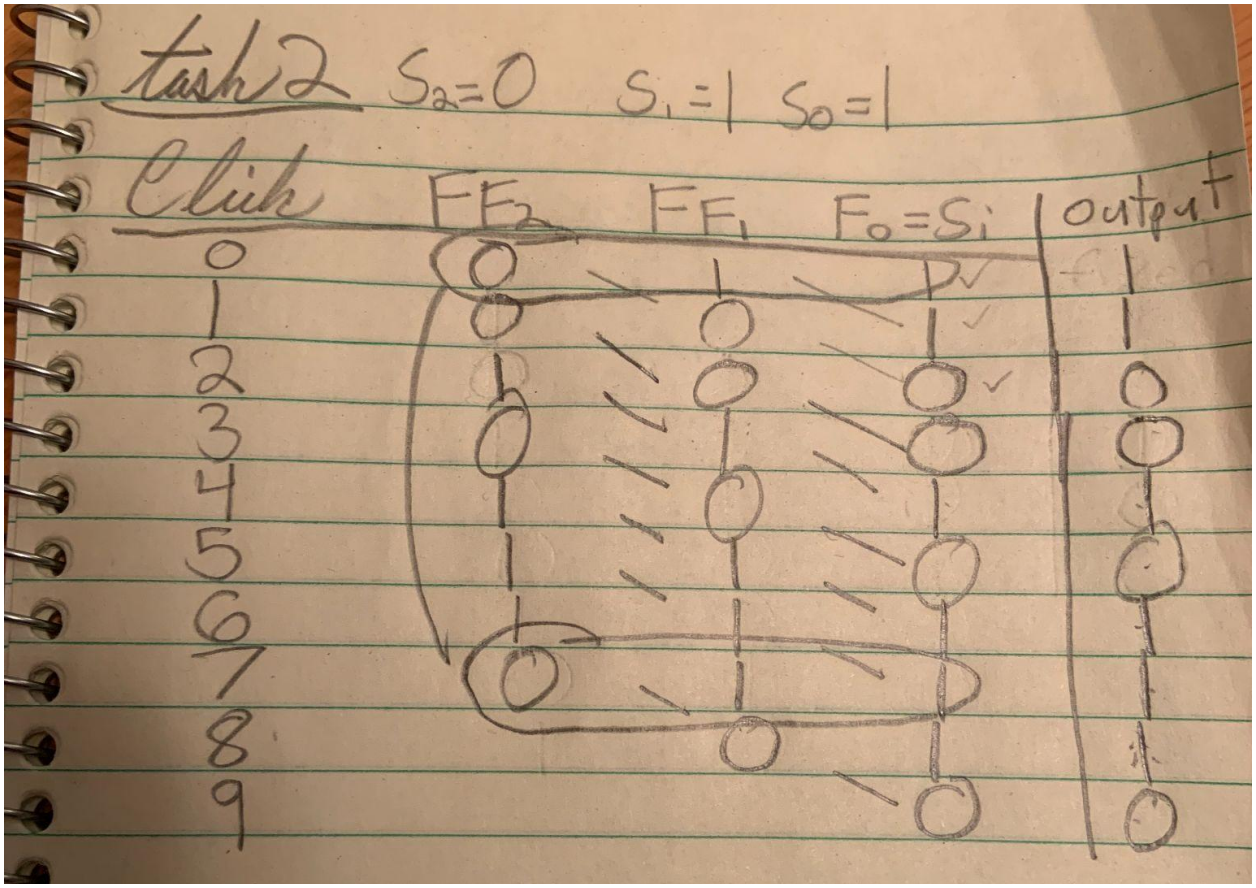
Carl Cortez
CIS 628
Chapter 2
Lab 4

2.5


$S_3 \equiv S_1 + S_0 \mod 2$
$S_4 \equiv S_2 + S_1 \mod 2$ ...
2.5
$c_2 = 1$ $c_1 = 0$ $c_0 = 1$
task 1
$S2 = 1$ $S1 = 0$ $S0 = 0$
stream bit
Click
FF_2
FF_1
$FF_0 = S_i$
output
0
1
2
3
4
5
6
7
8



2.6

One key element of this hack is that we know the period is 150-200 bits in length. With this information, we can attack the cipher with plaintext of a similar size. Knowing that we should have some repetition in the 150-200 mark is a key element to focus on. If we cross check our plaintext with the ciphertext, we can discover the key. This would use a similar method from task 2.5 involving XOR.

We can decrypt all ciphertext by using our key on the remaining bits *(should be < 50).* We can start at the beginning of the ciphertext and ensure that the covered bits match up with our key. If it doesn't match up at some point, we could conclude that it worked for those bits but not the majority of the ciphertext. Naturally, this goes against our goal of attacked the entire message and decrypting everything.