Homework for section#5B (approximate due date: Sept 28th, 2020)

Part 1 Encryption: Find the stream {C0 C1 C2 C3} from the initial steam {A0 A5 A10 A15}

Initial	Inverse	After affine	After shift & Mix column
$\mathbf{A_i}$	$\boldsymbol{B'_i}$	$\boldsymbol{B_i}$	$\boldsymbol{C_i}$
A0 = 0101 1010 = 5A	B'0 = 22 = 0010 0010	B0 = 1011 1110 = BE	C0 = 0011 1011 = 3B
A5 = 0101 1001 = 59	B'5 = 3E 0011 1110	B5 = 1100 1011 = CB	C1 = 0110 0001 = 61
A10 = 1010 0110 = A6	B'10 = 65 = 0110 0101	B10 = 0010 0100 = 24	C2 = 0111 1111 = 7F
A15 = 1101 0001 = D1	B'15 = 07 = 0000 0111	B15 =0011 1110 = 3E	C3 = 0100 1010 = 4A

Part 2 Decryption: Find the stream {A0 A5 A10 A15} from the initial steam {C0 C1 C2 C3}

Initial	After reverse shift & Mix column	After reverse byte substitution
$\mathbf{C_i}$	$\boldsymbol{B_i}$	$\boldsymbol{A_i}$
C0 = 1001 1100 = 9C	B0 = 1001 1010 = 9A	A0 = 0011 0111 = 37
C1 = 1100 0101 = C5	B5 = 0001 0110 = 16	A5 = 1111 1111 = FF
C2 = 0111 0001 = 71	B10 = 0111 1101 = 7D	A10 = 0001 0011 = 13
C3 = 0010 1101 = 2D	B15 = 1111 0100 = F4	A15 = 1011 1010 = BA

Homework for Section#6A (due date September 28th, 2020)

Alice uses the two following random numbers:

a. Random numbers for polarizer (0=+ ; 1=x) are:

10101100 11110110 01000110 11000111 10001110 01011110 00001011 10100110

00011001 11100001 01100001 11100001 10111001 00111010 01111111 11000101

10101110 10001110 11001011 10000100 01000010 10100010 11010110 01001011

01101100 10100100 11100000 10101010 00101011 00110101 11111101 10011110

b. Random numbers for data stream are:

01100111 00110001 10001101 10010011 11101000 01001111 10010011 01001000

00000001 00001011 10100111 01101001 00000101 01100101 10011101 00111000

10000010 11001110 00100000 10110110 10001100 10000011 00010111 11001100

11010000 00001001 10001111 00001011 10001000 01001010 01000100 01011111

Bob random numbers for polarizer (0=+ ; 1=x) are:

10100000 00000011 01111000 01010011 10001110 00000010 10000110 11001111

10100011 00101001 11010101 11111000 11001101 00011011 11110010 11111010

00001010 11110010 10100000 11001001 10100011 10010111 11111110 10000100

00100100 10000001 11000011 00100010 10010000 11011110 10100111 10010101

QUESTION: Find <u>two</u> possible sequences of matching positions to send the following key:

00110100 00111001 11101101 01110100 10010001 10101101 10111101 00110001

Data bits received by Bob:

0110??11????0?0?10?????1?00?0?11111010000?0???11?001??1?0??0?00??0???0?1??00?011
?0??0?11011??00?0???0?0101?0010??001??0?00???????0?00?101?????100??0?0??1?11??1??
??0110?10??0?1?00?1?111??00????1?01?00000?01?0?10?011???000?011?0???0?????0?0??0
?0??1?00101?1??

1st key positions:

[1, 4, 2, 3, 13, 7, 15, 18, 26, 27, 8, 17, 24, 29, 36, 31, 32, 33, 34, 38, 35, 37, 39, 47, 40, 48, 52, 55, 41, 72, 43, 50, 79, 51, 57, 80, 60, 62, 63, 87, 88, 66, 90, 70, 91, 104, 75, 106, 110, 76, 116, 135, 137, 143, 78, 153, 82, 85, 155, 156, 89, 94, 95, 159]

2nd key positions:

[251, 249, 254, 252, 248, 250, 243, 241, 238, 236, 246, 224, 223, 230, 226, 214, 213, 209, 205, 222, 196, 193, 220, 184, 219, 183, 182, 180, 218, 175, 212, 210, 169, 207, 204, 166, 202, 201, 200, 165, 159, 199, 156, 198, 155, 153, 195, 143, 137, 188, 135, 116, 110, 106, 187, 104, 178, 177, 91, 90, 173, 170, 167, 88]