Homework 3

Casey Bates

24 April 2020

1 RC4 By Hand

n = 3, Key = [1, 2, 3, 6]
m = BACDDAH = 001 000 010 011 011 000 111

S[0]	S[1]	S[2]	S[3]	S[4]	S[5]	S[6]	S[7]
0	1	2	3	4	5	6	7
T[0]	T[1]	T[2]	T[3]	T[4]	T[5]	T[6]	T[7]
1	2	3	6	1	2	3	6

Permutation:
j = (j + S[i] + T[i]) mod 8
Swap(S[i], S[j])

i	j	S[0]	S[1]	S[2]	S[3]	S[4]	S[5]	S[6]	S[7]
	0	0	1	2	3	4	5	6	7
0	1	1	0	2	3	4	5	6	7
1	3	1	3	2	0	4	5	6	7
2	0	2	3	1	0	4	5	6	7
3	6	2	3	1	6	4	5	0	7
4	3	2	3	1	4	6	5	0	7
5	2	2	3	5	4	6	1	0	7
6	5	2	3	5	4	6	0	1	7
7	2	2	3	7	4	6	0	1	5

Keystream Generation:
i = (i + 1) mod 8
j = (j + S[i]) mod 8
Swap(S[i], S[j])
t = (S[i] + S[j]) mod 8
KS = S[t]

i	j	t	KS	S[0]	S[1]	S[2]	S[3]	S[4]	S[5]	S[6]	S[7]
0	0			2	3	7	4	6	0	1	5
1	3	7	5	2	4	7	3	6	0	1	5
2	2	6	1	2	4	7	3	6	0	1	5
3	5	3	0	2	4	7	0	6	3	1	5
4	3	6	1	2	4	7	6	0	3	1	5
5	6	4	0	2	4	7	6	0	1	3	5
6	1	7	5	2	3	7	6	0	1	4	5
7	6	1	3	2	3	7	6	0	1	5	4

Keystream = 5101053 = 101 001 000 001 000 101 011

Encryption:

$$Keystream \oplus M = Ciphertext$$

	101	001	000	001	000	101	011
$\oplus$	001	000	010	011	011	000	111
	100	001	010	010	011	101	100
	E	B	C	C	D	F	E

Ciphertext: EBCCDFE

2 RC4 With Python

(a) Code that generates RC4 keystream is called 'keystream.py'
(b) KeystreamGen(3, 7, [0,0,1,0,1,0,0,1,1,1,1,0]) will output:

$$[1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1]$$

(c) KeystreamGen(8, 24, [1,0,1,1,1,0,0,1,0,1,0,1,0,0,1,1,1,1,1,1,1,0,1,1,0,0,1,0,0,1,0,
0,0,1,1,0,0,0,0,0,1,1,0,0,1,0,1,0,0,1,0,1,0,0,0,1,1,0,0,0,0,1,1,1,0,0,0,1,0,1,0,1,1,1,0,1,
0,0,0,1]):

[1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0,
1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0,
1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1,
0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1,
1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0,
0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0,
0, 0, 1, 1, 0, 1]

(d) Decryption:

$$Keystream \oplus Ciphertext = Plaintext$$

Plaintext: You've found the answer!