# Homework 3 - CSCI 181 - S20

1. (20 points) Use RC4 with n=3 to encrypt the message M = BACDDAH using the secret key K= [1 2 3 6]. Go through the steps to generate the keystream as shown in class. Show your work and the steps. Then use the keystream to encrypt the plaintext message. Do this exercise by hand without writing a code. In this problem, we use 3-bit encoding for the letters A - H by A = 000, B = 001, . . . , H = 111.

2. (30 points) Write a program that generates the RC4 keystream. The program has three inputs: the integer $n$ (as described in Rc4), the integer $l$ which is the length of plaintext or ciphertext (the number of characters) and the array of bits which is the secret key. The output of the program should be an array of bits which is the keystream (it should have length $n * l$).

   Your program must include two functions. 1) A function called DecimalToBinary(int number, int n), with two integer inputs *number* and $n$. Its output is an array of length $n$ giving the binary representation of *number*. So DecimalToBinary(100, 8) should output [0,1,1,0,0,1,0,0].

   2) A function called ConvertBitArraytoInt(Array k, int n) should take an array of bits and $n$, and output an array of integers with every $n$ bits converted to its decimal representation. So ConvertBitArraytoInt([1,0,0,0,0,0,1,1,1,0,0,1], 3) should output [4, 0, 7, 1]. This will be used to convert the secret key input to RC4 to its decimal equivalent to be used in the RC4 algorithm.

   **Make sure to include lots of comments so that it is easy to follow your work. Each function should have a description of what it does.**

   (a) Submit your code.

   (b) Have your program check your work from Question 1 by taking the inputs: $n$ =3, $l$ = 7, key=[0,0,1,0,1,0,0,1,1,1,1,0]. Write the result from your code in your writeup.

   (c) Have your program find the keystream for the inputs: $n$ = 8, $l$ = 24, key=[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]. Write the keystream in your writeup.

   (d) Then use this keystream to find the corresponding ASCII plaintext from the ciphertext: [1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0]

   Write the plaintext in ASCII letters.