Homework 3 - CSCI 181

1. (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 separately.

   (b) Suppose you want to encrypt the message M = BACDDAH, with key K= [1 2 3 6] when n =3. Run your program for the these values to generate the keystream. Write the keystream from your code in your writeup. Then use the keystream to encrypt M and write down the result in your writeup. (you can leave the ciphertext as a bit string).

   (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, 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, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1]. Write the keystream in your writeup.

   (d) Then use this keystream to find the corresponding ASCII plaintext from the ciphertext. Write the plaintext in ASCII letters in your writeup. Both the key and the ciphertext are available in file hw3.txt so you can easily read or copy from.

   [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]

2. (a) (5 points) Consider the CFB mode of operation. Alice has a message to send and she breaks it into 10 blocks (M_1,...,M_{10}) and encrypts them using AES in CFB mode and sends Bob C_1, . . . , C_{10}. Suppose during transmission of ciphertext,

there are two bit errors in the transmission of C_2 and Bob knows that. Explain which M_i's will Bob correctly decrypt? and which ones are completely wrong? Briefly explain.

(b) (5 points) We said that If the value of IV used in CBC mode is not reused then the encryption is CPA-secure (resistant against Chosen plaintext attack). Explain why CBC mode with a repeating IV is not CPA-secure. In order to show that an ecnryption scheme is not CPA-secure, suppose Eve knows M and M' and has observed C and C' (the corresponding ciphertexts), but does not know which ciphertext corresponds to which message and she would like to learn this information. Eve can ask Bob to encrypt any message she chooses for her under the chosen plaintext threat model. Show that Eve can choose a specific message and ask Bob to encrypt it such that from the ciphertext Eve can determine whether C was the encryption of M or M'.