LAB2 : STREAM CIPHERS

EXERCISE 1 : RC4 ALGORITHM AND WEAKNESSES

1. Given the packet capture file `wep.cap`, answer the following questions :
   a. How many IVs are in the packet capture ?
   b. What is the IV for the first packet in the capture in hexadecimal representation?
   c. What is the WEP key?
   d. What is the TCP checksum of the first packet in the capture (in hex)?
2. Generate a random sequence using the RC4 algorithm. Test the randomness of the sequence using NIST SP 800-22 test suite tool and explain some tests.

EXERCISE 2 : LFSR

1. Show the table of states of the following LFSRs for nine clock impulses:
   a. First LFSR: feedback polynomial $F_1(x) = x^3 + 1$ and $seed = (0, 1, 0)$
   b. Second LFSR: feedback polynomial $F_2(x) = x^3 + x^2 + 1$ and $seed = (0, 1, 0)$
   c. Why the second LFSR has more states ?

2. A plaintext $P = 1001\ 0010\ 0110\ 11011001\ 0010\ 0110$ is encrypted with an LFSR-based stream cipher and the ciphertext is $C = 1011\ 1100\ 0011\ 0001\ 0010\ 1011\ 0001$. Assume that the pair (M, C) is given and the period of the keystream generator is less than 15.
   a. What is the period of the keystream generator used to encrypt P ?
   b. What is its degree, initialization value, and feedback polynomial?

3. **RootMe:** *LFSR - Known plaintext attack*: One of your friends argues that stream ciphers are safer than ever with LFSR. You smile and tell him he is not right. Upset, he challenges you by sending you the encrypted file challenge.png.encrypt. Show him he's wrong!