CECS 564

Programming Project #2

Due March 17, 2020

Content Scrambling System (CSS)

CSS was introduced in 1996. It is a 40 bit stream cipher that uses 2 linear feedback shift registers (LFSRs) of respectively 17-bit and 25-bit denoted by R1 and R2. The taping polynomials for R1 and R2 are respectively:

$$C1(x) = x^{15} + x + 1$$

$$C2(x) = x^{15} + x^5 + x^4 + x + 1$$

The LFSRs are initialized with the 40-bit key such that the 4^{th} bit of each LFSR is initialized with 1 to prevent the 0 state which generate only 0 keystream. A byte of the keystream is generated by 8 shifts of both registers then added using of an 8-bit full adder. The initial carry bit is 0

Encryption and decryption are done by bitxor of input bytes with the keystream bytes. Write an application to implement CSS with given specifications to do both encrypt and decrypt of any binary file.

Write a report to document your CSS application with a discussion about statistical changes as the result of CSS encryption.