Breaking Linear-Feedback Shift Registers (LFSR) Pseudo-Random Number Generation (PRNG)

---

1 Overview

Applications of linear-feedback shift registers (LFSRs) include generating pseudo-random numbers, pseudo-noise sequences, fast digital counters, and whitening sequences. Both hardware and software implementations of LFSRs are common.

The initial value of the LFSR is called the seed, and because the operation of the register is deterministic, the stream of values produced by the register is completely determined by its current (or previous) state. Likewise, because the register has a finite number of possible states, it must eventually enter a repeating cycle. However, an LFSR with a well-chosen feedback function can produce a sequence of bits that appearsrandom and has a very long cycle.

In this challenge lab, students will attempt to attack an LFSR implementation commonly used for random number generation in trying to figure out the starting state of LFSR, decode an encrypted image, and get the flag and code as proof you've solved the lab.

2 Lab Tasks

2.1 Task 1: Connect to the challenge server and get an encrypted challenge image

Update: You can just use the flag.enc file from Brightspace instead of connecting to the challenge server which is currently offline.

You need to connect to the challenge server and answer a couple of questions before it will spit out an encrypted image for you to try and crack. You'll need to download the encrypted file and attempt to break it offline.

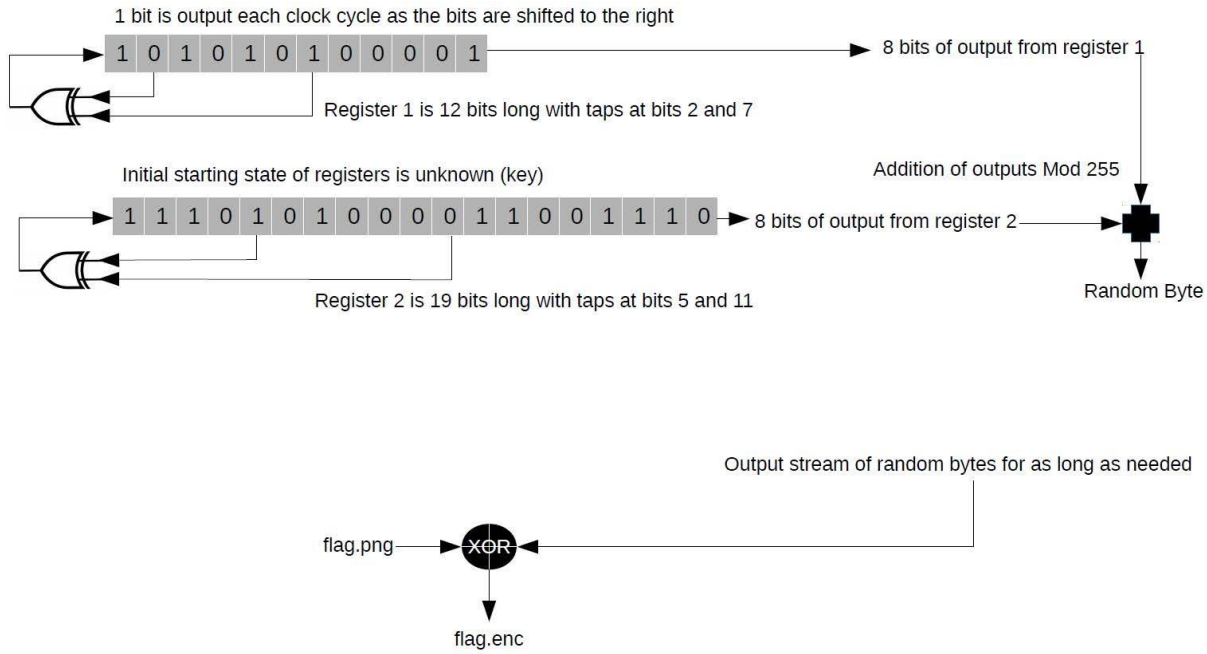
You can connect to the challenge server using Netcat with the commands $nc 192.168.1.1 4322

The challenge server basically generates a unique PNG image file for you and then uses its own internal LFSRfunction to generate a stream of bits that it then uses to XOR with the challenge image to produce the outputted encrypted file.

2.2 Task 2: Brute Force the Key

Once you have obtained your challenge image from the server, your next task is to attempt to brute force it. You'll need to use the fixed header format of the PNG image to your advantage to allow you to brute force part of the LFSR before finally attempting to break the entire starting state.

A diagram showing how the LFSR operates is shown below, but unfortunately, we don't know the startingstate of the registers.



The challenge is very similar to that faced by the first DVD pirates, as they attempted to break CSS so you should be able to use the same attack method to help you solve the challenge.

3 Submission

You need to submit a detailed lab report, with screenshots, to describe what you have done and what you have observed. You also need to explain the observations that are interesting or surprising. Please also list the important code snippets followed by an explanation. Simply attaching a code without any explanation will not receive credits.