Decrypt Vulnerable Data #1

Background

This challenge is orignated from weakness of DVB-CSS, the content scrambling system for DVDs.

You can find some references from the web.

- https://web.archive.org/web/20000302000206/http://www.dvd-copy.com/news/cryptanalysis_of_contents_scrambling_system.htm
- https://www.cs.cmu.edu/~dst/DeCSS/Kesden/index.html

DVD #1 is about the first step of DVB-CSS cracking, the LFSR rewinding attack.

Intended Solution

1. review the source code
   2 LFSRs with 2 and 3 bytes key
     ciphertext has enough prefix
2. guess first LFSR's 2 byte key
   We can calculate second LFSR's 25 bit output according to the first LFSR's output
3. calculate second LFSR's 3 byte key by rewinding
4. encrypt prefix data, and if it's same with the encrypted message,
5. decrypt all the encrypted message and get the flag!