Decrypt Vulnerable Data #2

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 #2 is about actual decryption of DVB-CSS protected contents.

Intended Solution

1. find keyHash
2. find key
3. decrypt message (decryption is same as encryption)

Please refer to the first reference site for more details.