CSSE 340 Project Deliverable 2
Xander Lewis, Mathew Leister, Carson Holscher, David Creen

References:

Arnab, Alapan, et al. "Investigation of a kernel level DRM implementation." Proceedings of AXMEDIS (2007).

Arthur, Will, et al. "History of the TPM." *A Practical Guide to TPM 2.0: Using the New Trusted Platform Module in the New Age of Security* (2015): 1-5.

Camp, L. Jean. "First principles of copyright for DRM design." IEEE Internet Computing 7.3 (2003): 59-65.

Cherry, Jason. "Case Study Overview and Cryptanalysis of the DvD Contents Scrambling System and DeCSS". March 8th, 2001. https://www.cs.cmu.edu/~dst/DeCSS/Cherry/index.html

Ciriello, Raffaele Fabio, et al. "Blockchain-based digital rights management systems: Design principles for the music industry." *Electronic markets* 33.1 (2023): 5.

Claburn, Thomas. “DeCENC Is yet Another Way to Beat Amazon, Netflix Video DRM.” The Register® - Biting the Hand That Feeds IT, The Register, 12 Sept. 2024, www.theregister.com/2024/09/12/cenc_encryption_stream_attack/.

Cochrane, Jane. "It's Encodings All the Way Down". December 12th, 2017. https://jeancochrane.com/blog/encodings-all-the-way-down

Cohen, Julie E. "DRM and Privacy." Communications of the ACM 46.4 (2003): 46-49.

Court of Appeal of California, Sixth District. *DVD Copy Control Assn., Inc v Bunner*.

“DVD Descrambling Code Not a Trade Secret.” *EFF*, Electronic Frontier Foundation, January 22, 2004, https://web.archive.org/web/20071014063720/http://w2.eff.org/IP/Video/DVDCCA_case/20040122_eff_pr.php, January 22nd 2025.

Hassan, Heba El-Rahman, Mohamed Tahoun, and Gh S. ElTaweel. "A robust computational DRM framework for protecting multimedia contents using AES and ECC." Alexandria Engineering Journal 59.3 (2020): 1275-1286.

“High-bandwidth Digital Content Protection System.” Digital Content Protection LLC, October 16, 2012, https://www.digital-cp.com/sites/default/files/specifications/HDCP%20Interface%20Independent%20Adaptation%20Specification%20Rev2_2_FINAL.pdf, January 22, 2025.

Kesden, Gregory. “Operating Systems: Design and Implementation.” *Content Scrambling System (CSS): Introduction*, 2006, www.cs.cmu.edu/~dst/DeCSS/Kesden/index.html.

Korba, Larry, and Steve Kenny. "Towards meeting the privacy challenge: Adapting drm." *ACM Workshop on Digital Rights Management*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002.

Madushanka, Tiroshan, Dhammika S. Kumara, and Atheesh A. Rathnaweera. "SecureRights: A Blockchain-Powered Trusted DRM Framework for Robust Protection and Asserting Digital Rights." *arXiv preprint arXiv:2403.06094* (2024).

Perlman, Radia, Charlie Kaufman, and Ray Perlner. "Privacy-preserving DRM." *Proceedings of the 9th Symposium on Identity and Trust on the Internet*. 2010.

Suehle, Ruth. “The Drm Graveyard: A Brief History of Digital Rights Management in Music.” *Opensource.Com*, 3 Nov. 2011, opensource.com/life/11/11/drm-graveyard-brief-history-digital-rights-management-music.

“The Digital Millenium Copyright Act”. *U.S. Copyright Office*, https://www.copyright.gov/dmca/, January 22nd, 2025.

Touretzky, D. S. (2000) Gallery of CSS Descramblers. Available: <http://www.cs.cmu.edu/~dst/DeCSS/Gallery>, January 22nd, 2025

United States, Congress, *Digital Millenium Copyright Act: Public Law 105-304, Oct. 28, 1998*. 1998. U.S. G.P.O. Congress.

Yun, Jian, et al. "DRPChain: A new blockchain-based trusted DRM scheme for image content protection." *PloS one* 19.9 (2024): e0309743.

Description of the demo/prototype:

We will attempt to implement a similar encryption scheme to the Content Scramble System and attempt to brute force its 40 bit key after demonstrating how the system works.