Cryptology and Intellectual Property Rights: A Term Project Proposal

Herbert Chang

March 10, 2008

Abstract

Today especially, having a vastly developed network of information and communication technologies, the ease with which to share digital information is almost too convenient. While the ethics of digital media management are extremely controversial and hotly debated, indisputably, cryptological techniques and technologies are utilized in this space. This project thus seeks to understand how cryptology is involved with digital media management: the motivations, the design parameters for the cryptosystems, the actual cryptosystems employed, as well as possible future directions for cryptology in a context of digital media management.

1 Introduction

Modern cryptography, said to have been founded with Claude Shannon's landmark paper titled Communication Theory of Secrecy Systems [1], is mainly contrasted with classical cryptography in that modern cryptographic methods have moved away from use of mechanical ciphers to more mathematical abstractions, especially based upon those of probability and information theories. Because of this move towards mathematical abstractions, coupled with various advancements in digital technologies, cryptosystems have increasingly lent itself to applications in hardware and software.

With the advent and popularization of the internet, and general movement of the society towards information and communication technologies, the application and use of cryptosystems are no longer limited to governmental identities. One such sector that has welcomed cryptographical systems and technologies is the digital media market.

2 Scope of Project

In an effort to prohibit illegal distribution of digital media, a number of cryptosystems, both hardware and software, have been designed and employed to keep the end-users from using digital media 'inappropriately'. This project thus intends to understand the cryptosystems designed for purposes of digital media management, from its intentions and cryptosystem design parameters, to performance, to possible future directions. What this project will not do is attempt to design a cryptosystem for better digital media management, nor will this project attempt to break any existing cryptosystem employed. Furthermore, no discussion of whether the author agrees or disagrees with digital media management will be presented.

3 Proposed Schedule/Timeline

Week	Topic
March 10 - March 14	Proposal due Background: DRM and digital media management
March 17 - March 21	More on DRM and digital media management Begin study of cryptosystems used for DRM
March 24 - March 28	First Project Report due; More on cryptosystems for DRM
March 31 - April 1	Study for midterm
April 7 - April 11	More cryptosystems for DRM
April 14 - April 18	Begin cryptanalysis of cryptosystems for DRM
April 21 - April 25	More cryptanalysis
April 28 - May 2	More cryptanalysis
May 5 - May 9	More cryptanalysis
May 12 - May 16	Begin writing
May 19 - May 23	More writing; Studying for final

4 Expectations

Final deliverable can be expected to be in the form of a report. This report will include background information on cryptography and digital media management, as well as how cryptography fits within the context of digital media management. Details regarding cryptosystems employed will also be discussed, ranging from design goals, and theoretical and/or perceived weaknesses. The report will end with a discussion on future directions of cryptography in digital media management.

References

[1] C. Shannon, *Communication Theory of Secrecy Systems.* Bell System Technical Journal, vol. 28, pp. 656-715, 1949.

[2] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone. *Handbook of Applied Cryptography.* Boca Raton, Florida: CRC Press, 1997.

[3] D. R. Stinson. *Cryptography – Theory and Practice.* 5^{th} Edition. Boca Raton, Florida: CRC Press, 2006.