“God Rewards Fools”—
Whitfield Diffie and Martin Hellman’s Stand to Revolutionize Cryptography

Chloe Makdad
Senior Division
Historical Paper
Word Count: 2499

"No right of private conversation was enumerated in the Constitution. I don't suppose it occurred to anyone at the time that it could be prevented." —

Whitfield Diffie, testifying before the US House of Representatives[1]

When the United States Constitution was drafted, not even the most forward thinking individuals could have foreseen the direction that communication would take. At the time, private conversation could be assured simply by walking out of the earshot of eavesdroppers. With the advent of the digital age, however, cryptography became integral in assuring secure correspondence.[2] Without insight into our modern world, the Founding Fathers had little need to explicitly enumerate a right to privacy in the Constitution, with the vague language of the Fourth Amendment serving as one of the only bases for privacy rights.[3] This ambiguity has led to an increasing number of confrontations between the government and private citizens, struggling between privacy and security, between individual liberties and perceived safety. With the United States government possessing a virtual monopoly on the cryptography industry, Whitfield Diffie and Martin Hellman's 1976 publication, *New Directions in Cryptography,* took a stand for the individual's right to privacy. Facing repercussions such as fines, lawsuits, and prison, Diffie and Hellman nonetheless published their research. Their defiance toward the government and academia, who both discouraged research in cryptography, allowed encryption to become

[1] *The Impact of a Secret Cryptographic Standard on Encryption, Privacy, Law Enforcement and Technology: Hearings Before the Committee on Energy and Commerce*, 103d Cong. (1993) (statement of Whitfield Diffie). Accessed November 29, 2016. https://epic.org/crypto/clipper/diffie_testimony.html.
[2] "Cryptography Pioneers Receive ACM A.M. Turing Award," Communications of the ACM, accessed October 24, 2016, https://www.acm.org/awards/2015-turing.
[3] *Ibid;* U.S. Const. amend. IV. Accessed December 14, 2016. http://constitutionus.com/.

commercially available to all, opening the door for private communication to become a feasible aspect of the Digital Age and beginning a "revolution in cryptography."[4]

From the Zimmermann Telegram during World War I to the Enigma during World War II, the United States government took note of cryptography's growing importance during the twentieth century.[5] By V-J Day, the government possessed a monopoly on cryptography and research was primarily conducted within the National Security Agency after its founding in 1952.[6] Encryption predominantly protected diplomatic and military communications and remained in the domain of the government.[7] With the NSA conducting nearly all cryptographic research, bureaucrats decided what it was about and exercised tight control over any outside research to prevent foreign powers from improving their own methods.[8]

None of this discouraged Diffie and Hellman. Diffie's interest in cryptography began in the fifth grade, and after graduating from MIT in 1965 with a mathematics degree, he took a job in programming.[9] In 1972, following a discussion with an excited colleague about network security, a subject which many thought of as cryptography, Diffie began working on nothing else.[10] After graduating from Stanford with a Ph.D. in electrical engineering in 1969, Hellman

---

[4] Whitfield Diffie and Martin E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory* IT-22, no. 6 (November 1976): 644, accessed October 24, 2016, https://www-ee.stanford.edu/~hellman/publications/24.pdf.

[5] NSA, "National Cryptologic Museum Exhibit Information," National Cryptologic Museum, last modified May 3, 2016, accessed December 17, 2016, https://www.nsa.gov/about/cryptologic-heritage/museum/exhibits/; Malcom W. Browne, "Cryptography Is Too Good for Anyone's Comfort," *The New York Times*, June 4, 1978, E7, http://search.proquest.com.ezaccess.libraries.psu.edu/hnpnewyorktimes/docview/123682978/1A4825D7FDE0484EPQ/8?accountid=13158.

[6] Whitfield Diffie, e-mail interview by the author, December 9, 2016; David Burnham, "The Silent Power of the NSA," *The New York Times*, March 27, 1983, accessed December 20, 2016, http://www.nytimes.com/1983/03/27/magazine/the-silent- power-of-the-nsa.html?pagewanted=all.

[7] Susan Landau, e-mail interview by the author, December 12, 2016.

[8] Diffie, e-mail interview by the author; "Hearings Involve Secret Codes: 'Cracking' a Major Peril in War," *The New York Times*, May 13, 1951, 59, http://search.proquest.com.ezaccess.libraries.psu.edu/hnpnewyorktimes/docview/112238579/fulltextPDF/42107E5953004D5FPQ/1?accountid=13158.

[9] Whitfield Diffie, "Interview with Whitfield Diffie on the Development of Public Key Cryptography," by Franco Furger, Institute for Technology Assessment and Systems Analysis, last modified January 16, 2002, accessed December 14, 2016, http://www.itas.kit.edu/pub/m/2002/wedi02a.htm.

[10] *Ibid;* Diffie, e-mail interview by the author.

went to work for IBM, where his interest in cryptography began to develop. While there, he recognized that the commercial applications for cryptography were growing as the Internet was slowly seeping into everyday life.[11]

Martin Hellman's shift into working independently on cryptography baffled some of his colleagues. They wondered how he expected to discover anything new, given the NSA's control of the industry. While conceding he would devise theories and methods that the NSA was already aware of, Hellman's response was simple: "The person who gets credit is the first to publish, not the first to discover and keep things secret."[12] Whether his work overlapped advances already made by the NSA was inconsequential; the NSA's work was classified whereas what Hellman could potentially do would be available commercially.[13]

While standing against academia's skepticism about cryptography research, Diffie and Hellman first crossed paths in 1974, when Diffie was traveling to learn more about cryptography and Hellman was a professor at Stanford. The duo had immediate chemistry, each finding the other to be well-informed in cryptography.[14] Both were excited, not discouraged, by the research potential within the field, and what was originally supposed to be a half-hour meeting resulted in the pair talking for nearly nine hours. Of the meeting, Hellman said, "It was a mild epiphany, finding an intellectual soul mate in this."[15] And so began a partnership that would soon revolutionize the world of cryptography.

---

[11] Martin Hellman, "Oral History Interview with Martin Hellman," by Jeffrey R. Yost, University of Minnesota Digital Conservancy, last modified November 22, 2004, accessed October 19, 2016, https://conservancy.umn.edu/handle/11299/107353.
[12] Hellman, "Oral History," interview, University of Minnesota Digital Conservancy.
[13] *Ibid*.
[14] Gary McGraw, "The History of Public Key Cryptography with Whitfield Diffie," *Silver Bullet Security Podcast*, podcast audio, December 31, 2014, accessed December 5, 2016, https://www.cigital.com/podcasts/show-105/.
[15] Hellman, "Oral History," interview, University of Minnesota Digital Conservancy.

Before meeting Hellman, Whitfield Diffie had envisioned a digital revolution with the development of an information superhighway and personal computers for ordinary people. A digitally connected society would naturally include digital communications, communications which Diffie believed deserved to be protected through encryption.[16] At the time, however, encryption still required the distribution of keys—pieces of information that decrypt messages—so encrypted messages could be understood. Since the dawn of cryptography, keys had to be physically shared, a fundamental weakness and inconvenience in even the most advanced cryptosystems.[17] Key distribution had been a problem long before the advent of computers; if two parties were trying to exchange secret information during wartime or across international borders or even in inclement weather, this situation was not ideal. When computers did become an aspect of commerce, banks and businesses would send trusted employees around the world with padlocked briefcases containing keys to distribute to partners.[18] As the prevalence of computers in the workplace grew, this procedure became a logistical and financial problem.[19] Infatuated with the idea of enabling large-scale commerce and communication through the Internet, Diffie searched for a solution.

Finally working with someone who shared his passion, Diffie made headway. Inspired by the concept of trap-door ciphers and their concerns about the strength of the NSA's Data Encryption Standard proposal, Diffie and Hellman were led to the idea of public key cryptography.[20] Undeterred by the government's monopoly and discouragement from colleagues,

---

[16] Simon Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, 22nd ed. (New York: Anchor Books, 1999), 254.
[17] Diffie and Hellman, "New Directions," 644.
[18] Singh, *The Code*, 251; Richard A. Shaffer, "Cryptic Reaction: Companies Use Codes to Ward off Thieves and Safeguard Secrets," *The New York Times*, June 16, 1978, 1, http://ezaccess.libraries.psu.edu/login?url=http://search.proquest.com.ezaccess.libraries.psu.edu/docview/134245990?accountid=13158.
[19] Singh, *The Code*, 252; Shaffer, "Cryptic Reaction," 1.
[20] Hellman, telephone interview by the author.

Diffie and Hellman went through an arduous process of trial and error, developing ideas, learning they did not work, and repeating the process. Despite their failures, the pair maintained their passion to solve a problem that no one else believed could be solved. Hellman remarked, "The way to get to the top of the heap. . .is to be a fool, because only fools keep trying. . . Unless you're foolish enough to be continually excited, you won't have the motivation. . . to carry it through. God rewards fools."[21]

By 1976, Diffie and Hellman's "foolishness" had paid off. In 1975, Diffie was on his way to grab a Coke when a brilliant revelation flashed into his mind. He had concocted a cipher that utilized an asymmetric key, where, unlike any other cipher, the key used to encrypt a message is not the same key used to decrypt it.[22] The following year, working late into the night, Hellman proved two parties could securely exchange keys without ever meeting.[23] By the end of 1976, they published *New Directions in Cryptography*, outlining Diffie-Hellman key exchange[24] and asymmetric ciphers, both imperfect yet workable systems that finally convinced the rest of the world there was a solution to the key distribution problem.[25]

The genius behind public key encryption was not only its strength, but that it solved the key distribution problem, something that had plagued cryptographers for centuries.[26] Before Diffie and Hellman, two parties trying to communicate privately needed to share a secret: a key. Public key cryptography requires no meeting or personal exchange between parties to securely encrypt a message. Both parties have two keys, one private and one public. Key exchange

---

[21] Singh, *The Code*, 256.
[22] *Ibid*, 271.
[23] *Ibid*, 267.
[24] Diffie-Hellman key exchange is a method that can be used to share secret information between two parties and increasingly being referred to Diffie-Hellman-Merkle due to Ralph Merkle's contributions to Diffie and Hellman's research and publications.
[25] Singh, *The Code*, 271.
[26] "A Cryptic Ploy in Cryptography," *The New York Times*, October 29, 1977, 17, http://search.proquest.com .ezaccess.libraries.psu.edu/hnpnewyorktimes/docview/123289015/1A4825D7FDE0484EPQ/12?accountid=13158.

becomes unnecessary as the sender encrypts a message with the recipient's public key, and that message can only be decrypted by the recipient's private key [See Appendix A].[27] This is because Diffie-Hellman key exchange works using one-way functions, meaning functions that are easy to do, but difficult to undo, similar to the process of mixing paint [See Appendix B].[28] Because, like paint, one-way functions are so difficult to reverse, messages encrypted with such public keys are secure. By hiding secrets in plain sight, public key cryptography provided an unprecedented level of security and practicality that no other encryption system in history could offer.

Standing up to the government monopoly on relevant encryption research and against opinions that the key distribution problem had no solution, Diffie and Hellman's *New Directions in Cryptography* laid the foundations for modern cryptography. [29] The intellectual community was euphoric, and it was published with unheard of urgency.[30] Conversely, given the state of world affairs, the NSA and military community's response was apoplectic. Prior to Diffie-Hellman key exchange, the process for exchanging keys was arduous and expensive, but public key cryptography allowed communicators to exchange keys quickly and cheaply.[31] For both foreign and domestic security reasons, the NSA was concerned. In 1975, the Senate lauded the NSA for its intelligence-gathering capacity, but after Diffie and Hellman's publication and with

[27] Wellesley College, "Encryption and Security," Computer Science 110, accessed December 20, 2016, http://cs110.wellesley.edu/reading/cryptography-files/handout.html.
[28] Diffie and Hellman, "New Directions," 649-650; Elias Zamaria, "'Diffie-Hellman Key Exchange' in Plain English," Information Security, last modified November 24, 2013, accessed December 20, 2016, http://security.stackexchange.com/questions/45963/diffie-hellman-key-exchange-in-plain-english
[29] Steve Fyffe and Tom Abate, "Stanford cryptography pioneers Whitfield Diffie and Martin Hellman win ACM 2015 A.M. Turing Award," Stanford News. Last modified March 1, 2016, accessed October 24, 2016, http://news.stanford.edu/2016/03/01/turing-hellman-diffie-030116/.
[30] McGraw, "The History."
[31] Martin E. Hellman, "An Overview of Public Key Cryptography," *IEEE Communications Society Magazine* 16, no. 6 (November 1978): 24-25, https://doi.org/10.1109/MCOM.1978.1089772.

the Cold War in the backdrop, officials feared its abilities could be compromised.[32] To collect intelligence about the Soviet Union, the U.S. often relied on Third World countries' weakly encrypted messages. The NSA feared that these countries could access a working public key cryptosystem, keeping valuable information from the U.S.[33]

As a result, Diffie and Hellman's stand resulted in some backlash. In July 1977, J. A. Meyer, who was later revealed to be an NSA employee, sent a letter to the Institute of Electrical and Electronics Engineers arguing that several of their publications were in violation of the International Traffic of Arms Regulations (ITAR).[34] While never specifically naming any papers, Meyer referenced the same issues of *Transactions* that contained Diffie and Hellman's work. Meyer warned that these publications were disseminating "weapons technologies [that] could have more than an academic affect."[35] The interpretation dictated in Meyer's letter was of immediate concern to the intellectual community. The accuracy of his claims was unclear, but the potential repercussions were severe, both for Diffie and Hellman and academia as a whole.[36] Meyer essentially compared publishing a paper in cryptography to exporting information on nuclear weaponry and was insinuating that any publications in cryptography were restricted under ITAR. Members of the academic community feared that if Meyer's interpretation held

[32] David Burnham, "The Silent Power of the NSA," March 27, 1983
[33] Duncan Campbell, "Whose Eyes on Secret Data?," *New Scientist* 77, no. 1092 (March 2, 1978): 594-595, accessed December 19, 2016, https://books.google.com/; Diffie, e-mail interview by the author.
[34] Stephen H. Unger, "Privacy, Cryptography, and Free Research," *IEEE: Technology and Society* 20 (December 1977): 8-9, accessed December 19, 2016, http://ewh.ieee.org/soc/ssit/Newsletter%20Archive/1972-1981/TS5-20-77.pdf; Malcolm W. Browne, "Senate Panel Asks Role for Security Agency in Cryptography Grants," *The New York Times*, April 13, 1978, B8, http://search.proquest.com.ezaccess.libraries.psu.edu/hnpnewyorktimes/docview/123749364/1A4825D7FDE0484EPQ/10?accountid=13158.
[35] J. A. Meyer to E. K. Gannet, July 7, 1977, accessed December 16, 2016, https://cryptome.org/hellman/1977-0707-Meyer-letter.pdf.
[36] Hellman, telephone interview by the author.

true, their freedom to publish research in areas of remote government interest could be restricted.[37]

Around the same time Meyer's letter came out, Martin Hellman was getting ready to present more research with students on public key encryption at a symposium hosted by Cornell. Uncertain about how serious he should take Meyer's supposition, Hellman consulted Stanford lawyer John Schwartz. Schwartz held the opinion that it was constitutional to publish research about cryptography, though warned Hellman, "If you are prosecuted, Stanford will defend you. But if you're found guilty, we can't pay your fine and we can't go to jail for you."[38] After WWII and the dawn of the Cold War, cryptography's status was unclear, considered a munition by some and a dual-use export by others.[39] Depending on how its status was perceived in a potential confrontation, those involved faced hefty fines and possible jail sentences.

In the end, the only repercussion of Hellman's stand at Cornell was signaling the end of the U.S. government's monopoly on cryptographic research. Alongside his students, Hellman stood against the restriction of research despite the threat of legal retaliation and presented their ground-breaking cryptographic work. Of this decision, Hellman said, "It's interesting people have…talked about how courageous I was to do this…It's one of those things where it's not courage. You're confronted with a situation where it's so clearly right to do it and you find the courage in yourself. It's just no question."[40]

---

[37] Unger, "Privacy, Cryptography," 8-9.
[38] Henry Corrigan-Gibbs, "Keeping Secrets," *Stanford Alumni*, November/December 2014, accessed October 24, 2016, http://alumni.stanford.edu/get/page/magazine/article/?article_id=74801; Hellman, telephone interview by the author.
[39] Whitfield Diffie and Susan Landau, "The Export of Cryptography in the 20th Century and the 21st," in *The History of Information Security: A Comprehensive Handbook*, by Karl Maria Michael de Leeuw and Jan Bergstra Elsevier (Amsterdam: Elsevier, 2007), 4-6, accessed December 15, 2016, http://privacyink.org/pdf/export_control.pdf.
[40] Hellman, "Oral History," interview, University of Minnesota Digital Conservancy.

That same summer, Admiral Bobby Inman became director of the NSA, walking directly into the uproar caused by the Meyer letter, written on the first day of his tenure.[41] Inman was concerned about the potential impact Diffie and Hellman's publication could have on the government's foreign eavesdropping abilities, and even more perplexed about why they were researching cryptography.[42] Until the 1970's, the primary consumers of cryptographic equipment were governments and drug dealers. Since the bulk of cryptographic research was done by the NSA for the purposes of the government, Inman wanted to find out why Diffie and Hellman were focusing on cryptography.[43] What he discovered was that the pair had set out to solve a problem that was not on the NSA's radar—the growing need for securing commercial computer systems. Both Diffie and Hellman believed computers were growing into an aspect of everyday life, requiring greater unclassified knowledge of cryptography to be secure. Given the NSA had not even begun to think about this issue, Diffie and Hellman were solving a problem they felt was not going to be solved by the government.[44]

Inman was still concerned about the increased availability of high-grade encryption: "We were worried that foreign countries would pick up and use cryptography that would make it exceedingly hard to decrypt and read their traffic."[45] As public interest in cryptography began to grow, Inman convened an internal panel to determine a course of action that would protect

---

[41] National Security Agency, *American Cryptology during the Cold War, 1945-1989, Book III: Retrenchment and Reform, 1972-1980*, by Thomas R. Johnson, research report no. CCH-S54-98-01, United States Cryptologic History 6 (n.p.: Center for Cryptological History, 1995), 189, 235, accessed December 18, 2016, http://nsarchive.gwu.edu /NSAEBB/NSAEBB260/nsa-6.pdf; Stephen Budiansky, *Code Warriors: NSA's Codebreakers and the Secret Intelligence War Against the Soviet Union* 1st ed. (New York: Knopf Doubleday Publishing Group, 2016), 295.
[42] Corrigan-Gibbs, "Keeping Secrets."
[43] Christopher Paine, "Admiral Inman's Tidal Wave," *The Bulletin of the Atomic Scientists* 38, no. 3 (March 1982): 3-4, accessed December 19, 2016, https://books.google.com/.
[44] Corrigan-Gibbs, "Keeping Secrets."
[45] *Ibid*; *Foreign Applied Sciences Assessment Center Technical Assessment Report, Soviet Computer Science Research*. United States: Central Intelligence Agency, 31 July 1984. *U.S. Declassified Documents Online* (accessed January 12, 2017). http://tinyurl.galegroup.com.ezaccess.libraries.psu.edu /tinyurl/4Aref0; National Security Agency, *American Cryptology*, 236.

national security interests and avoid controversy. Initially, he sought to pass legislation to impose government control on cryptographic research, but Inman's proposed bill was "dead on arrival," standing no chance of moving through Congress. Inman then moved to craft a voluntary review system that would fall apart within a decade. With the press on their side and the world undergoing a digital revolution, it was nearly impossible to halt the cryptographic progress Diffie and Hellman's stand had set into motion.[46]

In some ways, history has vindicated Whitfield Diffie and Martin Hellman. One year after the publication of *New Directions in Cryptography*, three MIT researchers refined Diffie-Hellman key exchange to an applicable system, known as RSA.[47] In 1991, Phil Zimmermann wrote the Pretty Good Privacy program, a widely available implementation of public key cryptography for e-mail communications.[48] Just as Diffie predicted, ordinary people are using personal computers for communication and commerce, and Admiral Inman is just as concerned with protecting these nongovernmental computer systems today as Diffie and Hellman were in the 1970's.[49] However, in other ways, what Diffie and Hellman stood against persists with the ongoing debate between privacy and security.[50] Since taking their initial stand, multiple other altercations between the government and the research community have ensued, now collectively

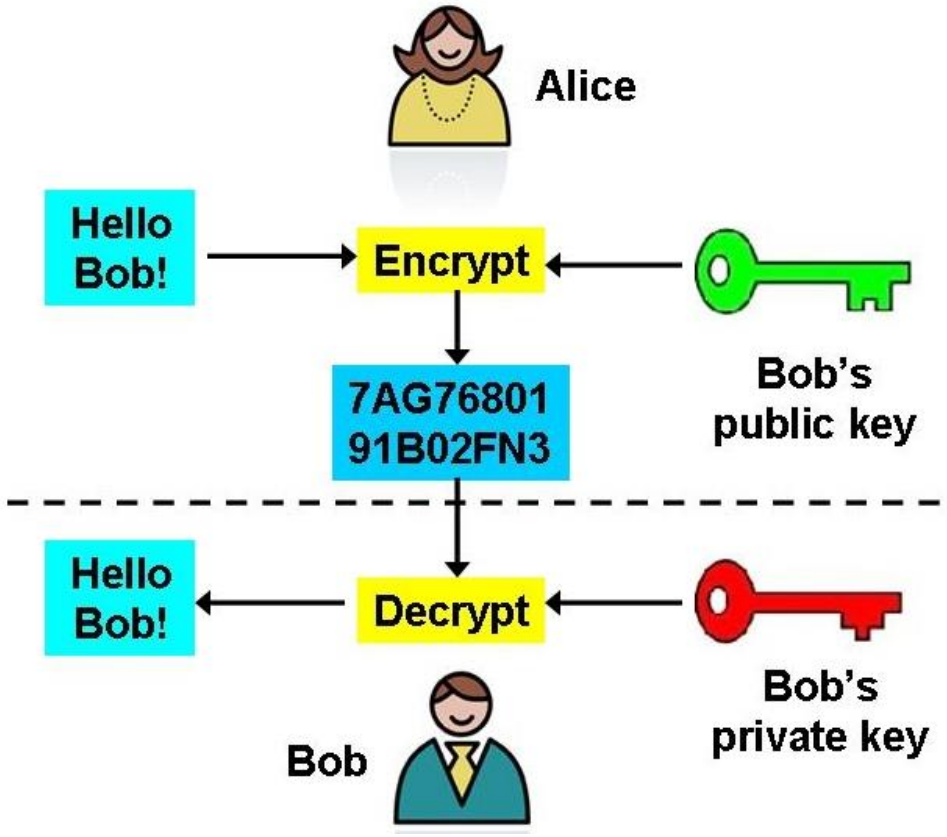
[46] *Ibid;* Paine, "Admiral Inman's," 3-4.
[47] Burt Kaliski, "The Mathematics of the RSA Public-Key Cryptosystem," *RSA Laboratories*, April 2006, 2-5, accessed December 5, 2016, http://www.ams.org/samplings/math-awareness-month/06-Kaliski.pdf; Susan Landau, "Primes, Codes, and the National Security Agency," *Notices of the American Mathematical Society*, January 1983, 7-10, accessed December 15, 2016, http://www.privacyink.org/pdf/PrimesCodesNSA.pdf.
[48] Philip R. Zimmermann, "Cryptography for the Internet," *Scientific American*279, no. 4 (October 1998): 111-112, accessed January 12, 2017, https://www.philzimmermann.com/docs/SciAmPRZ.pdf.
[49] Hellman, telephone interview by the author; Amy Nordum, "Forty Years Later, Turing Prize Winners Devoted to Digital Privacy and Nuclear Activism," IEEE Spectrum, last Modified March 4, 2016, accessed May 14, 2017, http://spectrum.ieee.org/tech-talk/computing netwroks/forty-years-later-turing-prize-winners-devoted-to-personal-privacy-and-nuclear-activism
[50] Corrigan-Gibbs, "Keeping Secrets."

referred to as the Crypto Wars.[51] From the standoff between Apple and the FBI to allegations of Russian interference in the 2016 election, cryptography continues to be a vital aspect of U.S. politics.[52] And with no knowledge of how American policy may evolve, Diffie and Hellman's stand may be more consequential now than ever before.

While nowhere in the Constitution is there a specific "right to privacy," there is a right to free speech. Standing against both the ideas of their colleagues, who believed the key distribution problem could not be solved, and the policies of the government, who believed they should be the ones to solve the problem, Whitfield Diffie and Martin Hellman jump-started a revolution in cryptography. By exercising their right to freely publish their work, the pair's stand set the stage for the birth of modern encryption, leading to a society dependent on secure digital communication in every facet of life. While many saw them as foolish for attempting to solve a problem that "could not be solved," for researching in a field dominated by the government, and for publishing despite threats of lawsuits, fines, and jail time, it seems Martin Hellman may have been right; perhaps God does reward fools.

[51] Sean Sposito, "General' Martin Hellman Recalls Decades-Long Wars over Encryption," *San Francisco Chronicle,* March 24, 2016, accessed December 20, 2016, http://www.sfchronicle.com/24hrsale/article/General-Martin-Hellman-recalls-decades-long-6933394.php.
[52] Darrell M. West and Jack Karsten, "A Brief History of U.S. Encryption Policy," Brookings. Last modified April 19, 2016, accessed December 8, 2016, https://www.brookings .edu/blog/techtank/2016/04/19/a-brief-history-of-u-s-encryption-policy/.

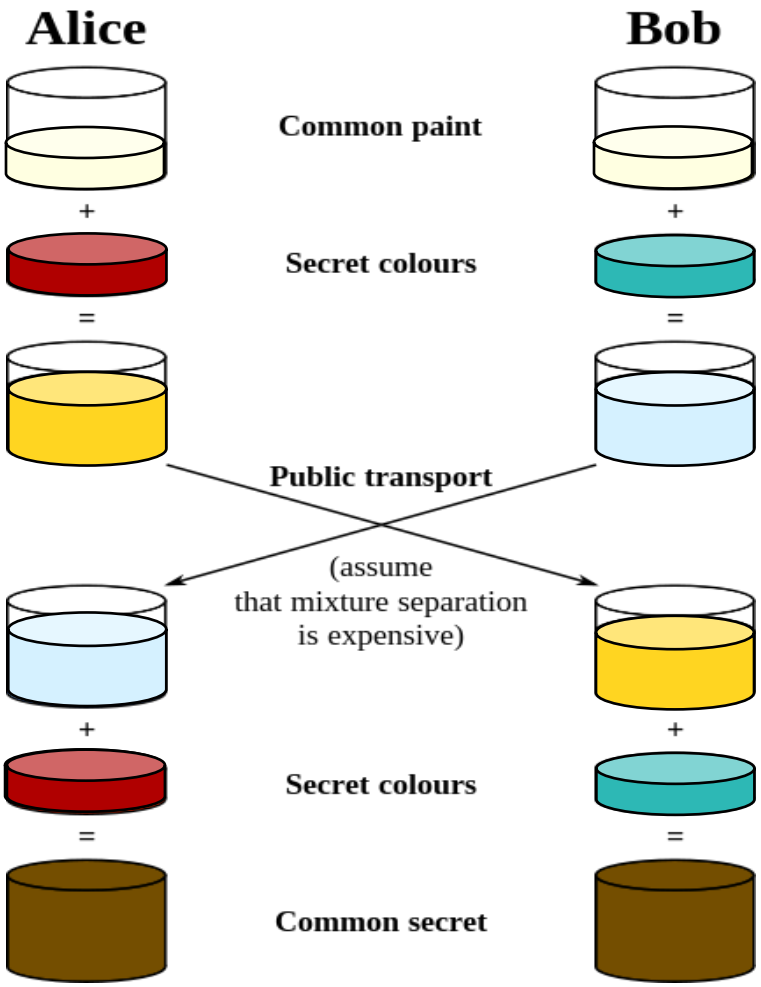
Appendix A



Above is a simplified diagram of how public key encryption works. Alice would encrypt her message to Bob using Bob's public key and then send the message. The only way to decrypt the message would be to use Bob's private key, to which only Bob has access.

Wellesley College. "Encryption and Security." Computer Science 110. Accessed December 20, 2016. http://cs110.wellesley.edu/reading/cryptography-files/handout.html.

Appendix B



A common analogy for how public key encryption works is one using paint, as mixing paint works the same way as a successful one-way function: it is easy to do, but nearly impossible to undo. Both parties, commonly referred to as Alice and Bob, start with a common base color of paint. They then each add their respective secret, or private, colors and send the mixture to the other person. Since Alice now has a paint that is a mixture of the common base color and Bob's secret color and Bob has a mixture of the common base color and Alice's secret color, each of them needs to add their respective secret colors to the mixture they received. This would result in both Alice and Bob having the same color paint. Assuming Eve intercepts the paint Alice sent to Bob and the paint Bob sent to Alice, she would be unable to derive either secret color or the common secret since she would be able to 'unmix' either paint to determine the common color or either secret color.

Zamaria, Elias. "'Diffie-Hellman Key Exchange' in Plain English." Information Security. Last modified November 24, 2013. Accessed December 20, 2016. http://security .stackexchange.com/questions/45963/diffie-hellman-key-exchange-in-plain-english.

ANOTATED BIBLIOGRAPHY
PRIMARY SOURCES

Browne, Malcom W. "Cryptography Is Too Good for Anyone's Comfort." *The New York Times*, June 4, 1978, E7. http://search.proquest.com.ezaccess.libraries.psu.edu/hnpnewyorktimes /docview /123682978/1A4825D7FDE0484EPQ/8?accountid=13158.

Browne's article details how, by the 1970's, the United States had developed incredibly secure methods of encryption after their experiences in World Wars I and II and the growth of computer technology. When writing my paper, this helped me to understand how strong the United States really was when it came to cryptography and how it developed its prominence in the field.

Browne, Malcolm W. "Senate Panel Asks Role for Security Agency in Cryptography Grants." *The New York Times*, April 13, 1978, B8. http://search.proquest.com.ezaccess.libraries .psu.edu/hnpnewyorktimes/docview/123749364/1A4825D7FDE0484EPQ/10?accountid= 13158.

This article details the interactions between the NSA and cryptography researchers and how the Senate settled these issues. I learned more about the arguments from both sides of the issue and started to understand how the debate between researchers, including Hellman, and the NSA were settled. Browne also went into more detail about how the J. A. Meyer letter was perceived by people and groups outside of academia.

Burnham, David. "The Silent Power of the NSA." *The New York Times*, March 27, 1983. Accessed December 20, 2016. http://www.nytimes.com/1983/03/27/magazine/the-silent-power-of-the-nsa.html?pagewanted=all.

Burnham's article informed me about who strong and powerful the NSA's knowledge of cryptography was. Burnham also discussed the attitudes of the NSA as well as the lawmakers and the public towards the NSA, including an analysis of the findings of a Senate select committee study of the NSA. It helped me to better understand the NSA's role in cryptography and the different ways it was perceived in the context of the time period of my paper.

Campbell, Duncan. "Whose Eyes on Secret Data?" *New Scientist* 77, no. 1092 (March 2, 1978): 593-95.Accessed December 19, 2016. https://books.google.com/.

Campbell's *New Scientist* article details the effects of the discovery of public key cryptography. He discussed the controversy surrounding Diffie and Hellman's work as well as the applications of it. This was helpful for me in understanding more of what resulted from the publication of *New Directions in Cryptography.*

Diffie, Whitfield. E-mail interview by the author. December 9, 2016.

I reached out to Diffie over email, and almost immediately he graciously agreed to answer some of my questions. We discussed everything from how he became interested in cryptography to the development of public key encryption to the government's role in the field and more. This interview was an invaluable source for me as it was not only conducted with someone very knowledgeable about my topic, but it was conducted about one of the very people that I am writing about.

Diffie, Whitfield. "Interview with Whitfield Diffie on the Development of Public Key Cryptography." By Franco Furger. Institute for Technology Assessment and Systems Analysis. Last modified January 16, 2002. Accessed December 14, 2016. http://www.itas.kit.edu/pub/m/2002 /wedi02a.htm.

Furger's interview with Whitfield Diffie provided a comprehensive look at Diffie's career and how public key cryptography was developed. While the entire interview was informative and useful in writing my paper, it specifically helped me to understand how Diffie developed an interest in cryptography, as a formative amount of time was spent focused on Diffie's early life and career.

Diffie, Whitfield, and Martin E. Hellman. "New Directions in Cryptography." *IEEE Transactions on Information Theory* IT-22, no. 6 (November 1976): 644-54. Accessed October 24, 2016. https://www-ee.stanford.edu/~hellman/publications/24.pdf.

New Directions in Cryptography was the very publication that sparked Diffie and Hellman's stand against the NSA and restrictive policies on encryption. After reading it multiple times, I could understand how public key encryption works and why it is so secure so I explain it in my paper. It also detailed the problems that Diffie-Hellman key exchange solved, including authentication and key-distribution. Additionally, Diffie and Hellman gave some remarks putting Diffie-Hellman key exchange into a historical perspective.

Diffie, Whitfield, and Martin E. Hellman. "Exhaustive Cryptanalysis of the NBS Data Encryption Standard." *Computer* 67 (June 1977): 74-85. https://doi.org/10.1109/C-M.1977.217750.

Diffie and Hellman were skeptical of the Data Encryption Standard because they believed the key size was so small that a reasonably powerful computer could break it. They describe why they think that DES is too weak in this article, which helped me to understand what Diffie and Hellman believed and more of the underlying reasons behind their stand against the NSA.

Foreign Applied Sciences Assessment Center Technical Assessment Report, Soviet Computer Science Research. United States: Central Intelligence Agency, 31 July 1984. *U.S. Declassified Documents Online* (accessed January 12, 2017). http://tinyurl .galegroup.com.ezaccess.libraries.psu.edu/tinyurl/4Aref0.

Soviet Union's capabilities in computer science are assessed in this declassified CIA report. Towards the end of the document, cryptography, and where the research was coming from in the Soviet Union is discussed. It mentions that most of the citations of public-key cryptography in Soviet papers and reports were of American publications, in some ways affirming the NSA's suspicions that freedom in cryptography publications in the United States would lead to foreign countries improving their own cryptography. This helped me to better understand the gravity of the NSA's concerns when Diffie and Hellman had published.

Hellman, Martin. "Oral History Interview with Martin Hellman." By Jeffrey R. Yost. University of Minnesota Digital Conservancy. Last modified November 22, 2004. Accessed October 19, 2016. https://conservancy.umn.edu/handle/11299/107353.

This transcript of Jeffrey Yost's interview with Martin Hellman detailed his entire career in this interview, starting with how he entered the field of cryptography and continuing onto his encounters with the government after publishing his research. I used this throughout my paper for insight into Hellman's and Diffie's careers and into how they stood up against NSA policy.

Hellman, Martin. Telephone interview by the author. December 15, 2016.

Dr. Hellman generously allowed me to interview him the development and repercussions of public key encryption. His firsthand knowledge of my topic provided me with inspiration as to what direction I wanted my paper to go, and he brought to light the details and success of his stand for privacy rights and against the NSA. I was also able to discuss some of the current issues in cryptography and threats to individual privacy that persist today, helping me connect what he and Diffie accomplished in the 1970's to modern society. Hellman also briefly talked with me about his current work in trying to avert nuclear war.

Hellman, Martin E. "An Overview of Public Key Cryptography." *IEEE Communications Society Magazine* 16, no. 6 (November 1978): 24-32. https://doi.org/10.1109/MCOM.1978 .1089772.

Hellman's paper details the benefits that public key cryptography provided, from decreased cost of encryption to satisfying a growing commercial need. This helped me to understand Hellman's perspective of what his work would do in contrast to the fears the NSA had about it.

Holmes, Edith. "Senate: DES More than Adequate." *Computerworld* (Boston), April 17, 1978. Accessed December 19, 2016. https://books.google.com/.

In this article from the news publication *Computerworld*, Edith Holmes covers the Senate's response to criticism of DES and the NSA's involvement in the development of the standard. It also mentions that the Meyer letter was not sent on behalf of the entire NSA, but rather on Meyer's own initiative. Both the discussion of DES from the government's perspective and the revelation on the Meyer letter were helpful to me while writing my paper.

The Impact of a Secret Cryptographic Standard on Encryption, Privacy, Law Enforcement and Technology: Hearings Before the Committee on Energy and Commerce, 103d Cong. (1993) (statement of Whitfield Diffie). Accessed November 29, 2016. https://epic.org/crypto/clipper/ diffie_testimony.html.

In his testimony before the Subcommittee on Telecommunications and Finance of the Committee on Energy and Commerce, Whitfield Diffie addressed both perspective of some of the most prevalent ethical dilemmas that arise through determining the proper course of legislation regarding cryptography. This allowed me to understand the perspectives of legislatures and how it contrasted with those who were developing new cryptographic systems. I used a quote from this source to begin my paper as well as referencing it on multiple other occasions.

McGraw, Gary. "The History of Public Key Cryptography with Whitfield Diffie." *Silver Bullet Security Podcast*. Podcast audio. December 31, 2014. Accessed December 5, 2016. https://www.cigital.com/podcasts/show-105/.

In the form of a podcast, this interview by Gary McGraw with Whitfield Diffie discusses what led Diffie to the discovering public key encryption, from gaining an interest in cryptography to meeting Martin Hellman to developing Diffie-Hellman Key Exchange. Among other topics discussed in the interview, Diffie also talks about his opinion on the concept of backdoors in encryption systems for law enforcement and the dispute between Apple and the FBI. The first-hand account given by Diffie about his experiences help provide inspiration for the direction I wanted to take my paper.

Meyer, J. A. Letter to E. K. Gannet, July 7, 1977. Accessed December 16, 2016. https://cryptome.org/hellman/1977-0707-Meyer-letter.pdf.

In response to the publication of numerous works concerning encryption and cryptography, NSA employee J. A. Meyer sent a letter to the Institute of Electrical and Electronic Engineers (IEEE) arguing that these publications were in violation of the International Traffic in Arms Regulations (ITAR). While he never mentions any authors by name, it was clear that this message was intended for Diffie and Hellman to see, as Meyer references the publications that included papers authored by them about cryptography. This letter helped me to understand the potential implications of Diffie and Hellman's stand.

The New York Times. "A Cryptic Ploy in Cryptography." October 29, 1977, 17. http://search.proquest.com.ezaccess.libraries.psu.edu/hnpnewyorktimes/docview/123289015/1A4825D7FDE0484EPQ/12?accountid=13158.

In this *New York Times* article, the dilemma between cryptographic researchers and the government is explored. It discusses both the government's perspective of wanting to protect Americans during peacetime and wartime by ensuring that potential enemies did not get hold of such powerful encryption as public key cryptography and researchers' perspective of wanting to open the door to private communications at home.

The New York Times. "Hearings Involve Secret Codes; 'Cracking' a Major Peril in War." May 13, 1951, 59. http://search.proquest.com.ezaccess.libraries.psu.edu/hnpnewyorktimes/docview/112238579/fulltextPDF/42107E5953004D5FPQ/1?accountid=13158.

As soon as the early 1950's, the government was concerned with protecting American cryptographic secrets from foreign powers and placed tight security protocol around research in cryptography. This source helped me to understand how the government viewed cryptography before computers became an aspect of everyday life for civilians.

Paine, Christopher. "Admiral Inman's Tidal Wave." *The Bulletin of the Atomic Scientists* 38, no. 3 (March 1982): 3-6. Accessed December 19, 2016. https://books.google.com/.

Paine's article on Admiral Bobby Inman, who was the director of the NSA at the time *New Directions in Cryptography* was published, discusses Inman's view on the relationship between scientific research and national security. This article depicts Inman as "the archetype of what a modern intelligence officer should be" due his stance that the government's needs and the research field's needs have a symbiotic relationship. This helped me to see how Inman's views has changed since his initial reaction to the publication of work in the field of cryptography.

Presidential Directive No. PD-24 (Nov. 16, 1977). Accessed December 18, 2016. https://www.jimmycarterlibrary.gov/documents/pddirectives/pd24.pdf.

This previously classified Presidential Directive from the Carter Administration detailed a new Telecommunications Protection Policy concerning how research in the communication field like cryptography should be treated. It helped me to understand how the Carter Administration responded differently from the NSA to non-government research in fields that were classified by the government.

Shaffer, Richard A. "Cryptic Reaction: Companies Use Codes to Ward off Thieves and Safeguard Secrets." *The New York Times*, June 16, 1978, 1. http://ezaccess.libraries.psu.edu/login?url=http://search.proquest.com.ezaccess.libraries.psu.edu/docview/134245990?accountid=13158.

Shaffer's article detailed the use of cryptography in business and in banking, providing yet another important consequence of Diffie and Hellman's stand. When writing my paper, this helped me to understand how improvements in cryptography resulted in more efficient transactions and communications in the business world in addition to how I already knew they affected personal communications.

Unger, Stephen H. "Privacy, Cryptography, and Free Research." *IEEE: Technology and Society* 20 (December 1977): 8-10. Accessed December 19, 2016. http://ewh.ieee.org/soc/ssit/Newsletter%20Archive/1972-1981/TS5-20-77.pdf.

In response to several articles concerning encryption being published by the IEEE and various other publications, J. A. Meyer of the NSA sent a letter to E.K. Gannet wearing the IEEE and the authors of these works about potential repercussions that could result from interpreting laws like the ITAR in a certain manner. Unger outlines the IEEE's response to this incident and defends the free publication of cryptography research. This source helped me to understand the response to Meyer's letter and more about what the potential implications on the field of cryptography if Meyer's interpretation of the law was correct.

SECONDARY SOURCES

Association for Computing Machinery. "Cryptography Pioneers Receive ACM A.M. Turing Award." Communications of the ACM. Accessed October 24, 2016. https://www.acm.org/awards/2015-turing.

Whitfield Diffie and Martin Hellman were the recipients of the 2015 Turing Award, commonly referred to as the "Nobel Prize of Computing," presented by Association for Computing Machinery. This website provided an explanation of what prompted the award to be given to Diffie and Hellman from more of a technical perspective, helping me to better understand the concept of public key cryptography and what made it groundbreaking.

Bellovin, Steven M., Matt Blaze, Whitfield Diffie, Susan Landau, Peter G. Neumann, and Jennifer Rexford. "Risking Communications Security: Potential Hazards of the Protect America Act." IEEE Security and Privacy, January/February 2008, 24-32. Accessed October 19, 2016. http://privacyink.org/pdf/PAA.pdf

While not directly related to Whitfield Diffie's work on Public Key Cryptography, this journal article in which he is a coauthor helped me to understand the full extent to which he believes in privacy rights and dissents NSA policy. Specifically, this article expressed distrust for and NSA wiretapping policy concerning situations where one party is outside of the United States.

Budiansky, Stephen. *Code Warriors: NSA's Codebreakers and the Secret Intelligence War Against the Soviet Union.* 1st ed. New York: Knopf Doubleday Publishing Group, 2016.

Budiansky's book covers the history of the NSA in the Cold War era and the importance of cryptography in the conflicts of the time period. While it never explicitly discussed Whitfield Diffie and Martin Hellman or their confrontation with the NSA, I learned about the strengths, weaknesses, and development of the NSA's abilities in cryptography, giving me some broader knowledge about the time period of my topic and what cryptography was like in the preceding years.

Calderbank, Michael. "The RSA Cryptosystem: History, Algorithm, Primes." Unpublished manuscript, University of Chicago, August 20, 2007. Accessed December 19, 2016. http://www.math.uchicago.edu/~may/VIGRE/VIGRE2007/REUPapers/FINAL APP/Calderbank.pdf.

Calderbank's paper gave me both a brief historical background on public key encryption as well as a view into how it works and how Diffie and Hellman's work influenced future applications, such as the RSA cryptosystem. In writing my paper, this source was helpful for me in explaining the process and importance of public key encryption.

Corrigan-Gibbs, Henry. "Keeping Secrets." *Stanford Alumni*, November/December 2014. Accessed October 24, 2016. http://alumni.stanford.edu/get/page/magazine/article/?article_id=74801.

Corrigan-Gibbs's article from the Stanford Alumni magazine provided a comprehensive history of the interactions between the NSA and Martin Hellman and his colleagues following the publication of *New Directions in Cryptography*. It helped me to piece together the chronology and impact of specific events I had researched earlier, and was also a resource that Hellman recommended I consult.

Diffie, Whitfield, and Susan Landau. "The Export of Cryptography in the 20th Century and the 21st." In *The History of Information Security: A Comprehensive Handbook*, by Karl Maria Michael de Leeuw and Jan Bergstra Elsevier, 725-36. Amsterdam: Elsevier, 2007. Accessed December 15, 2016. http://privacyink.org/pdf/export_control.pdf.

In this chapter of de Leeuw and Elsevier's *The History of Information Security*, Diffie and Landau discuss the history of the export status of cryptography. I learned about how cryptography was first classified as a munition and then evolved into a dual-use status and how the continued debate over how to classify it impacted how the export of cryptography was controlled. All of this helped me to understand the basis of some of J.A. Meyer's claims as well as some context for the NSA's concerns.

Diffie, Whitfield, and Susan Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption.* Cambridge, MA: MIT Press, 1998.

In their book, Diffie and Landau provide a comprehensive analysis of the politics that influence the regulation and development of cryptography and the public's access to it. While it clearly had a civil libertarian perspective, it helped me to better understand the issue of personal privacy and the government's role in both protecting and regulating those rights throughout the Information Age. Given that Diffie was an author, I was also able to gain insight into what he had stood against while advocating for privacy rights and how it has impacted legislation concerning privacy.

Fyffe, Steve, and Tom Abate. "Stanford cryptography pioneers Whitfield Diffie and Martin Hellman win ACM 2015 A.M. Turing Award." Stanford News. Last modified March 1, 2016. Accessed October 24, 2016. http://news.stanford.edu/2016/03/01/turing-hellman-diffie-030116/.

Stanford News recognized alumni Martin Hellman and Whitfield Diffie for being awarded the 2015 Turing Award in this article, which provided both an explanation of why the pair received the award and the repercussions of their publication. It detailed the careers of Diffie and Hellman and helped me to piece together a timeline of Diffie and Hellman's stand for privacy rights. Fyffe and Abate also remarked on Diffie and Hellman's perspective of the dispute between Apple and the FBI.

Kaliski, Burt. "The Mathematics of the RSA Public-Key Cryptosystem." *RSA Laboratories*, April 2006, 1-9. Accessed December 5, 2016 http://www.ams.org/samplings/math-awareness-month /06-Kaliski.pdf.

Dr. Burt Kaliski's paper on public key encryption explained the underlying mathematics that allows it to function, such as modular arithmetic, prime factors, and one-way functions. It also explained how Diffie and Hellman's theory is applied, and how cryptography needs to continue to progress in order to remain secure. In writing my paper, I used this to understand and explain public key encryption.

Landau, Susan. "Primes, Codes, and the National Security Agency." *Notices of the American Mathematical Society* 30, no. 1 (January 1983): 7-10. Accessed December 15, 2016. http://www.privacyink.org/pdf/PrimesCodesNSA.pdf.

Landau's article detailed how the government was beginning to meddle in the research of mathematicians due to the applications of math in cryptography as it had physicists and biologists in the past due to the applications of their work. Landau explains how this could be of detriment to research in the United States, an important point that I noted while writing my paper.

Landau, Susan. E-mail interview by the author. December 12, 2016.

Dr. Susan Landau is a Professor of Social Science and Policy Studies at Worcester Institute of Technology and Visiting Professor in Computer Science at the University of London. Due to her expertise of the intersection between cybersecurity, national security, law and policy, I interviewed her to gain a better understanding of United States' law concerning encryption.

National Security Agency. *American Cryptology during the Cold War, 1945-1989, Book III: Retrenchment and Reform, 1972-1980*. By Thomas R. Johnson. Research report no. CCH-S54-98-01. United States Cryptologic History 6. N.p.: Center for Cryptological History, 1995. Accessed December 18, 2016. http://nsarchive.gwu.edu/NSAEBB /NSAEBB260/nsa-6.pdf.

Johnson's previously classified report on the history of encryption in the United States, specifically in the NSA, provided me with ample information for my paper. It discussed everything from the NSA's perspective of the publication of *New Directions in Cryptography* to the importance of cryptography and cryptanalysis for the United States in the context of the Cold War. It helped me to understand my topic from a new perspective as well as providing me with historical context in which to place Diffie and Hellman's major academic achievement.

Nordum, Amy. “Forty Years Later, Turing Prize Winners Devoted to Digital Privacy and Nuclear Activism.” IEEE Spectrum. Last Modified March 4, 2016. Accessed May 14, 2017. http://spectrum.ieee.org/tech-talk/computing netwroks/forty-years-later-turing-prize-winners-devoted-to-personal-privacy-and-nuclear-activism

Nordum briefly discusses Diffie and Hellman’s past achievements in cryptography and how they are used today, but most of her article is centered on Diffie and Hellman’s views of current issues. Hellman still spends some of his time on cryptography and related research, though most of his time is spent advocating to try to prevent nuclear war, whereas Diffie now champions personal security and is concerned about political and governmental abuse of power. In sum, Nordum gave me greater knowledge of the present endeavors of Diffie and Hellman.

NSA. "National Cryptologic Museum Exhibit Information." National Cryptologic Museum. Last modified May 3, 2016. Accessed December 17, 2016. https://www.nsa.gov/about /cryptologic-heritage/museum/exhibits/.

This website, published by the National Cryptologic Museum which is operated by the NSA, gives a brief description of the events depicted in the museum’s exhibits. This helped me to put Diffie and Hellman’s work into a broader context of cryptographic history.

Singh, Simon. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. 22nd ed. New York: Anchor Books, 1999.

It was in this book by Simon Singh that I was first introduced to the work Whitfield Diffie and Martin Hellman. Singh’s book provided a comprehensive history of all cryptography and encrypted communication, helping me to place Diffie and Hellman’s work in the context of all work concerning encryption and examine what lead to and from this discovery.

Sposito, Sean. "'General' Martin Hellman Recalls Decades-Long Wars over Encryption." *San Francisco Chronicle* (San Francisco, CA), March 24, 2016. Accessed December 20, 2016. http://www.sfchronicle.com/24hrsale/article/General-Martin-Hellman-recalls-decades-long-6933394.php.

Sposito’s article from the *San Francisco Chronicle* detailed Martin Hellman’s perspective of the series of “Crypto Wars” that have been occurring since the 1970’s. It offered me a clear and concise timeline of the details of the events during each “war,” which was useful for me in writing my paper. Sposito also included some of Martin Hellman’s opinions on current issues concerning cryptography and privacy as well as Hellman reflecting on his initial perspective and conflict with the NSA.

U.S. Const. amend. IV. Accessed December 14, 2016. http://constitutionus.com/.

The Fourth Amendment of the United States protects citizens from “unreasonable searches and seizures,” and requires “probable cause” for warrants to be issued. This amendment is seen by many as the basis for privacy rights, and I used it to understand where this basis comes from.

Wellesley College. "Encryption and Security." Computer Science 110. Accessed December 20, 2016. http://cs110.wellesley.edu/reading/cryptography-files/handout.html.

This website was a digital version of a lesson used in Wellesley College’s Computer Science 110 class. I used a diagram from this website in my appendix materials to help explain public key encryption visually.

West, Darrell M., and Jack Karsten. "A Brief History of U.S. Encryption Policy." Brookings. Last modified April 19, 2016. Accessed December 8, 2016. https://www.brookings.edu/blog/techtank/2016/04/19/a-brief-history-of-u-s-encryption-policy/.

West and Karsten’s online article provided, as the title implies, a brief history of United States encryption policy. While the period that I discuss in my paper is only briefly mentioned in the article, it nonetheless allowed me to put into context the policies of the 1970’s with the policies of today and how they differ.

Zamaria, Elias. "’Diffie-Hellman Key Exchange’ in Plain English." Information Security. Last modified November 24, 2013. Accessed December 20, 2016. http://security.stackexchange.com/questions/45963/diffie-hellman-key-exchange-in-plain-english.

Diffie-Hellman Key Exchange can be quite complicated to explain in terms of mathematics to a lay-person, so I looked for a way to explain it that could be easily understood. On this website, I found a diagram of public key encryption showing how it would work we use paint instead of prime numbers and modular arithmetic. I referenced this diagram in my appendix materials.

Zimmermann, Philip R. "Cryptography for the Internet." *Scientific American* 279, no. 4 (October 1998): 110-15. Accessed January 12, 2017. https://www.philzimmermann.com/docs/SciAmPRZ.pdf.

Phil Zimmermann utilized public-key cryptography in his program, Pretty Good Privacy, and had his own confrontation with the United States government concerning his distribution of the Pretty Good Privacy program. This article showed me how Diffie and Hellman’s work impacted the future of cryptography, how it was perceived, and how it was applied by Zimmermann.