ANNOTATED BIBLIOGRAPHY

The Importance of Encryption in the Modern World

Jonathan O’Donnell, Xingyu (Tim) Xiang, Joshua Brest

NHD Annotated Bibliography

Primary Sources

Artifacts

Carpenter v. United STATES. 2017, www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf.

This case established that under the Fourth Amendment, any information that is obtained illegally isn't allowed to be used in court. In addition, after the court case, the government could no longer access CSLI records containing the physical locations of cell phones without a search warrant.

"Riley v. California." Oyez, https://www.oyez.org/cases/2013/13-132. Accessed 8 Dec. 2022.

This case is another example of the Fourth Amendment being used as a defense, where the police searched Riley's phone, which was protected by encryption. However, the police won this case as he was arrested before the phone was searched. However, police now require a search warrant before being able to search someone's phone.

"United States v. Chatrie, CRIMINAL 3:19cr130 | Casetext Search + Citator." Casetext.com, 3 Mar. 2022, casetext.com/case/united-states-v-chatrie. Accessed 8 Dec. 2022.

This is yet another case that involves technology and the Fourth Amendment. Information that was supposed to be protected under encryption was accessed by the government in order to be used as evidence against Chatrie. However, he changed his mind at the end due to the police having sufficient evidence.

The Constitution of the United States: A Transcription. National Archives, U.S. National

Archives and Records Administration, 4 May 2020, https://constitution.congress.gov/constitution/amendment-4/.

The fourth amendment states that people have the rights to be safe from unreasonable searches. This applies to their homes, documents and other artifacts that they may have.

Books

Fred Cohen &Associates Specializing in Information Protection since 1977 2.1 -A Short History of Cryptography

This book was really informational and went really in depth into cryptography history. It really helped us understand the different types of cryptography all around the world. It also helped our group understand the general development of cryptography, as this book really laid it out. In addition, it also talked in depth about the discovery of RSA.

Smart, Nigel. Cryptography: An Introduction (3rd Edition).

This book really goes into depth about every kind of cypher and how they work. It really helped us understand how people's understanding of encryption evolved over time and more about the basics of the more simple encryptions. In addition, it really goes into RSA security and how to prevent hacking/MIDM (Man In The Middle).

Inc, Thawte. History of Cryptography an EASY to UNDERSTAND HISTORY of CRYPTOGRAPHY 2. 2013.

This short book really talked about the start of encryption and also the future of encryption, for example when quantum computers were invented and quantum cryptography would be a thing. It also helped us better understand the use of encryption and how it will affect the future.

Christensen, Chris. Introduction to RSA and to Authentication. 2006.

This book helped us understand the process that the MIT team went through to discover RSA. According to this book, Rivest had a dream about three hypothetical people. Alice, Bob, and Eve. Alice wants to send Bob a message, but Eve wants to intercept the message. This is where an asymmetrical key comes into play; if Alice locks it using a lock and Bob has the key, they could send messages.

Jean-Philippe Aumasson. Serious Cryptography : A Practical Introduction to Modern Encryption. San Francisco, No Starch Press, 2018.

This RSA book helped us understand how RSA works by using prime numbers, and is really complicated to crack. So people can easily impediment this on the early email systems. This gave us the specifics of how RSA works and also a brief history of what happened before and after the invention of RSA.

Zwicke, Andrew. An Introduction to Modern Cryptosystems. SANS Institute, 2003, www.giac.org/paper/gsec/2604/introduction-modern-cryptosystems/104482. Accessed 8 Dec. 2022.

This cryptosystem really gave the context of what cryptography is. The history of it, the uses of it, and the definition of it, in addition to giving a brief introduction to every kind of modern encryption, such as Blowfish, SkipJack, and Elliptic Curves, are really information on different cryptography as of now.

E-Books

Cook, T. “Customer Letter - Apple”. Apple, 16 Feb. 2016, https://www.apple.com/customer-letter/.

This source helps us understand how important encryption is to our current society. It helped our group understand how having backdoors into encryption and software can be dangerous. It also helped us understand how encryption is used in our everyday lives.

Zimmermann, Philip. “Why I Wrote PGP.” Philip Zimmermann, June 1999, https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html.

This source helped us understand the idea behind asymmetric encryption and, more importantly, how it allows businesses to protect their data. This article also explains how encryption, even though it could be used for malicious purposes, is still a good thing to have because it does more good than harm. PGP was meant to protect our privacy.

A. M. Turing Award Oral History Interview With Whitfield Diffie. Interview by Hugh Williams, 15 Sept. 2017, amturing.acm.org/pdf/DiffieTuringTranscript.pdf.

This interview with Whitefield Diffie (one of the creators of public key encryption) helped us understand the thought process behind an encryption method and why it was created. It also helped us understand the importance of asymmetric encryption and DES (Data Encryption Standard) and how it changed the world of encryption, being the first block cipher.

“GCHQ Pioneers on Birth of Public Key Crypto.” ZDNET, interview by Tom Espiner, 26 Oct. 2010, www.zdnet.com/article/gchq-pioneers-on-birth-of-public-key-crypto.

This interview with Whitfield Diffie and Martin Hellman (two of the creators of public key encryption) helped us understand the process of creating a one way encryption method. It also explained why RSA was hidden from the public for so long and how it was used, rather than just left to collect dust.

“Interview With Peter Shor.” EP News, interview by Panos Charitos, 10 Mar. 2021, ep-news.web.cern.ch/content/interview-peter-shor.

This interview with Peter Shor (the creator of Shor’s algorithm) helped us understand how quantum computers work and how they can be used to break encryption (specifically RSA and Diffie-Hellman). It also helped us understand the mathematical side of encryption and how every encryption method is just a mathematical problem.

Interviews

Sky News [Sky News]. “Home Secretary Amber Rudd on #Ridge.” YouTube, 26 Mar. 2017, www.youtube.com/watch?v=0r9tDQx_lhM. Accessed 8 Dec. 2022.

This video between 3:51 to 6:15 tells us about terrorist attack using WhatsApp. The home secretary Amber Rudd tells us about how it is important for law enforcement to be able to access data relative to cases encrypted and whatnot. She states that it could be possible to let law enforcement access data while allowing end-to-end encryption.

Journals

Andrew Cohen. “Could Better Technology Lead to Stronger 4th Amendment Privacy Protections?” Brennan Center for Justice, 7 Dec. 2022, www.brennancenter.org/our-work/analysis-opinion/could-better-technology-lead-stronger-4th-amendment-privacy-protections. Accessed 8 Dec. 2022.

This article is a transcript of an interview with a professor that specializes in the fourth amendment and cases such as Riley v. California and Carpenter v. United States. Where the fourth amendment was infringed by law enforcement. This explores the limits and the loopholes in the fourth amendment that the government might use and really strengthened my understanding of the fourth amendment.

Newspaper Articles

Jamshidi, Sean. “In Conversation With Clifford Cocks.” Chalkdust, 23 Oct. 2019, chalkdustmagazine.com/interviews/clifford-cocks.

This interview explains how Clifford Cocks did invent RSA asymmetric encryption; however, at the time, computers were not powerful enough to run this algorithm. He also says that cryptanalysis not only requires brains, but also a lot of collaboration skills.

The Tablet. “The Babington Plot - From the Tablet Archive.” Tablet Archive, 3 Mar. 1923, web.archive.org/web/20160817162835/http://archive.thetablet.co.uk/article/3rd-march-1923/5/the-babington-plot-i1. Accessed 8 Dec. 2022.

This article tells us about the Babington Plot, a plot to assassinate Queen Elizabeth I. Former Queen Elizabeth I was almost assassinated by The Queen of Scots, who happened to be detained in Britain. The Queen of Scots was able to communicate with a priest. It was assumed that the priest created the plot himself. It also highlights the importance of encryption and how it can change the course of history.

Magazine, Stanford. “Keeping Secrets - Stanford Magazine.” Medium, 8 May 2018, stanfordmag.medium.com/keeping-secrets-84a7697bf89f.

This magazine tells us about how researchers at Stanford University were "tantamount to treason." They were trying to solve a "national problem that they had been looking for years." The NSA believed that if this research was released, it would make intelligence operations more difficult. This article is important because it shows how the NSA makes a decision that lots of people would disagree with.

“Documents Reveal N.S.A. Campaign Against Encryption.” Document - NYTimes.com, 5 Sept. 2013, archive.nytimes.com/www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html.

This article shows how the NSA was trying to prevent the use of encryption by the public. The NSA believed that if the public used encryption, it would make catching criminals and terrorists more difficult. They purposely hampered the strength of encryption standards like DES in order for them to be able to decrypt it easily.

Bernstein V. US DOJ (9th Cir. May 6, 1999). archive.epic.org/crypto/export_controls/bernstein_decision_9_cir.html.

In this article, it shows that the government wants to control the export of encryption source code. They argued that Bernstein's Snuffle crypto-system was a military weapon. The court ruled that the Snuffle crypto-system was not a military weapon and that the government could not control the export of encryption source code. This article is important because it shows how the government tried to control the export of encryption source code.

Documents

“FIPS 74 - Guidelines for Implementing and Using the NBS Data.” Archive.org, 2022, web.archive.org/web/20140103013152/www.itl.nist.gov/fipspubs/fip74.htm. Accessed 31 Oct. 2022.

This source taught us the fundamentals of data encryption, which assisted us in learning the fundamentals of encryption. Additionally, it taught us what a block cipher was. Additionally, it discloses to code which keys are used to decrypt an equation. They employed K, the key, which may be used to encrypt or decrypt an equation.

Data Encryption Standard, Federal Information Processing Standards Publication (FIPS PUB) 46, National Bureau of Standards, Washington, DC (1977).

According to this source, DES mandates that the algorithm be used internally by computers to safeguard their cryptographic security. It also taught us that each member of the group needs a key to encrypt the data, and that the 56 bits the method uses directly are randomized.

Whitfield Diffie and Martin E. Hellman, Exhaustive Cryptanalysis of the NBS Data Encryption Standard, Computer 10 (6), 74-84 (1977).

Our group learned how to use encryption and how it's created on this site. It creates a code that could be used for encryption by using a variety of letter combinations. It included a segment where it discussed how useless encryption is.

National Institution of Standards and Technology. (2001). NIST Planning Report 01-2, The Economic Impacts of NIST’s Data Encryption Standard (DES) Program. *National Institution of Standards and Technology*.

We learnt from this source that the NIST's first goal was to develop an encryption system safe enough to guard sensitive data. The Data Encryption Standard's conformance tests were created and put into use by the NIST.

National Bureau of Standards. “Data Encryption Standard.” *National Institution of*

***Standards and Technology*, Jan. 1977.**

The Data Encryption Standard (DES) defines an algorithm to be used for the cryptographic security of computer data and implemented in electronic hardware devices. The mathematical algorithm for encrypting and decrypting information that has been encoded in binary is fully described in this paper.

NIST Computer Security Division (CSD). "FIPS 140-1, Security Requirements For Cryptographic Modules (Superseded)." *National Institution of Standards and Technology*, Jan. 1994.

Our group learnt about the security requirements for protecting letters being transmitted in transit and the various degrees of letter protection from this source. This also told us about the additional security levels that are being introduced.

National Institution of Standards and Technology. "Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures." *National Institution of Standards and Technology*, Oct. 1999.

This source explained the creation of encryption and showed us the various methods for encrypting equipment. It also showed us how to use all the code that was used for encryption. Modes of Operation Validation System (MOVS): Requirements and Procedures, NIST Special Publication 800-17, 1998. This source outlines the creation and applications of the Data Encryption Standards. Additionally, it described the operation of encryption and its applications in government.

NIST Computer Security Division (CSD). "FIPS 46-3, Data Encryption Standard (DES) (Withdrawn May 19, 2005)." *NIST*, Oct. 1999.

Our group learned about encryption from this source, and I also mentioned two more sources about it. It also showed us how to utilize the primary and secondary encryption codes and the processes necessary to complete encryption.

E. Burr, William. "A New Hash Competition." *NIST*, 20 May 2008, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=152084.

This source taught us that there are many different kinds of encryption and methods for encrypting them. It also demonstrated to us the workings of encryption. It informed us that there was a NIST hash competition that was ongoing at the time.

“Online Security through Strong Encryption.” *NIST*, 6 Apr. 2017, https://www.nist.gov/industry-impacts/online-security-through-strong-encryption.

This source outlined the purposes for which encryption is utilized online. NIST collaborates with stakeholders all across the world to provide reliable, robust cryptography standards and guidelines, according to the statement.

National Security Agency. *American Cryptology during the Cold War*. NSA, 7 Sept. 2007, http://web.archive.org/web/20130918020036/www.nsa.gov/public_info/_files/cryptologic_histories/cold_war_iii.pdf.

Our group discovered from this source that before American troops left South Vietnam, cryptology was used during the Vietnam War and evacuated to Thailand. As stated on page 91, cryptology essentially played a supporting role in the conflict. Additionally, it discussed the role the NSA played in 1966.

Rivest, R. L., et al. “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.” Communications of the ACM, vol. 21, no. 2, 1978, pp. 120–126, people.csail.mit.edu/rivest/Rsapaper.pdf, 10.1145/359340.359342.

Our group was able to determine from the RSA literature that the equations utilized in the document had been developed as they were beginning to develop a formula for securing a public encryption. It also gave us in-depth justifications for when, how, and why the equation was created and how it came to be.

Rivest, Ronald. The Early Days of RSA -- History and Lessons ACM Turing Award Lecture. https://people.csail.mit.edu/rivest/pubs/ARS03.rivest-slides.pdf.

This RSA bibliography made it clear to us that the world could create sophisticated algorithms and a theory consumer that could be utilized to create prime-finding, multiplication, and factorization for the good guys using computer science theory. It also provided us with thorough explanations on the history and operation of the RSA algorithm.

Secondary Sources

Books

Turing, Alan, and Jack Copeland. The Essential Turing: Seminal Writings in Computing, Logic, Philosophy, Artificial Intelligence, and Artificial Life Plus the Secrets of Enigma. 1st ed., Clarendon Press, 2004.

This book is all about encryption used by the German army during the second world war. One of the highlights and reasons why this book is crucial is because it discusses how the Germans used the Enigma Encryption to coordinate its army of U-boats In fact, this book tells us that the Germans used encryption combined with U-boats to create unexpected attacks on the British navy. This book is important because it shows how the Germans blindly trusted their encryption; that was their downfall.

Morris, Edmund. Theodore Rex. New York: Modern Library, 2001.

This biography of Theodore Roosevelt helped us understand the way in which Philippe Bunau Varilla was able to get President Roosevelt to recognize the revolutionary government of Panama. It also gave us details regarding the specific treaties signed between the two nations that gave the U.S. control of the canal zone.

Singh, Simon. The Code Book: The Science of Secrecy From Ancient Egypt to Quantum Cryptography. Reprint, Anchor, 2000.

This book covers all the basics about encryption. It covers all the way back to the first monoalph described in the Jewish bible to the latest encryption technology that we use now! It really drew a clear picture in my mind about how and which ciphers were cracked. Furthermore, it also gave us insights about the significance of these ciphers in different wars, for example, the use of Enigma in WWII and how the Polish and Brits cracked it.

E-Books

“Code Talkers.” National Archives, 4 Oct. 2016, www.archives.gov/research/native-americans/military/code-talkers.html.

This article shows how much the US military relied on the Navajo language to communicate with each other. In both world wars, people from traditional tribes used their native languages that only they understood to communicate with each other. They then translated it into English. In this case, it was more of a code than encryption.

GeeksforGeeks. “Cryptanalysis and Types of Attacks.” GeeksforGeeks, 5 Jan. 2021, www.geeksforgeeks.org/cryptanalysis-and-types-of-attacks.

This article tells us about how cryptanalysis works and different methods that Cryptanalysts use to break encryption. One example is Known Plaintext Analysis (KPA) or CRIB. If we use that to guess part of the key. This will only work well if the key is 2-3x shorter than the plaintext. This article is important because it shows how cryptanalysis works and how it can be used to break encryption.

Mirza, Fauzan. “Block Ciphers and Cryptanalysis.” ResearchGate, July 1999, www.researchgate.net/publication/2582364_Block_Ciphers_and_Cryptanalysis. Accessed 8 Dec. 2022.

This article explains how people use cryptanalysis to break block ciphers, mainly DES. DES was broken a long time ago and is no-longer secure because each key can only be a max of 56 bits. This is equivalent to a 7 character password or `2^56` possible keys. This article is important because it shows how cryptanalysis works and different ways to break encryption. On modern computers, it is possible to brute force DES in a matter of hours.

“Timeline: A History of Encryption and Government Backdoors (Pictures).” CNET, www.cnet.com/pictures/timeline-a-history-of-encryption-and-government-backdoors-pictures/2.

This shows the brief history of modern encryption. Starting from the 1789 "All Writs Act" that allowed US courts to order anything they wanted to the rise of encrypted messaging apps like WhatsApp. This article is important because it shows how encryption has evolved over the years and how it has been used by governments.

Stubbs, Jack, and Andrey Ostroukh. "Yahoo Is Part of the Yahoo Family of Brands." Yahoo, 13 Apr. 2018, https://finance.yahoo.com/news/russian-court-rules-block-access-084401128.html.

This article explains how the Russian Government banned Telegram because of its encryption. This helped us understand how important encryption is, as it allows people to plan secret attacks against the government. This article also helped us understand how encryption can be used for good and bad purposes.

Levy, S. "Cypher Wars | WIRED". WIRED, 1 Nov. 1994, https://www.wired.com/1994/11/cypher-wars/.

This article shows how PGP was made using a patented mathematical process. This helped us understand how much law enforcement hated PGP and how they wanted to stop it. Because of that, they tried to make it illegal to use PGP.

McCullagh, Declan. "FBI: We Need Wiretap-ready Websites - Now." CNET, 4 May 2012, https://www.cnet.com/news/privacy/fbi-we-need-wiretap-ready-web-sites-now.

This article shines light on the FBI / Government's idea of backdoor encryption. In further re\ading, we can see that the U.S. government proposed the idea of a rewrite of the "CALEA" act, which in itself allows the government and law enforcement to wiretap and 'intercept communications in order to extend this to the web and private communications'.

Inc, Thawte. History of Cryptography an EASY to UNDERSTAND HISTORY of CRYPTOGRAPHY 2. 2013.

This book really helped us understand the use of cryptography in a history view. For example using it to keep the Egyptian Pharaoh’s script secret. It also gave us even more insight into different types of ciphers, their strengths and weaknesses and how to decode them.

Kotas, William. A Brief History of Cryptography. May 8AD, trace.tennessee.edu/cgi/viewcontent.cgi?article=1398&context=utk_chanhonoproj. Accessed 26 Oct. 2022.

This book helped us gain an even deeper understanding into the beginnings of cryptosystems, and the purpose of always innovating new ones. It also informed us of what happened to later develop into RSA how it was implemented into the internet and the asymmetrical cryptosystems.

Kak, Avi. Lecture 12: Public-Key Cryptography and the RSA Algorithm Lecture Notes on “Computer and Network Security.” 2019.

These notes really help us understand the concept of asymmetrical encryption as it really breaks it up into simple chunks for readers to understand. It also went into the backstory of encryption, which was really interesting as they brought some new insight. For example how RSA was really important as a war was going on when it was discovered.

Boneh, Dan, and Victor Shoup. A Graduate Course in Applied Cryptography. 2015.

This book gives a lot of insight into the vulnerabilities of encryption. It really taught us how something might be intercepted, but it also gave an example of how people have overcome this and patched the exploit. It also really informed about how encryption makes sure that the message wasn’t altered in any way or the key or whatnot was leaked.

Paar, Christof, and Jan Pelzl. Understanding Cryptography. Springer Berlin Heidelberg, 2010,

https://swarm.cs.pub.ro/~mbarbulescu/cripto/Understanding%20Cryptography%20by%20Christof%20Paar%20.pdf.

This book provided numerous illustrations of how encryption works, which greatly aided our understanding of how they are actually implemented and what happens behind the scenes, such as who a computer is computing. LIke other books it also gave a indepent of the issues with each encryption and how they can be solved.

Cozzens, Margaret B, and Steven J Miller. The Mathematics of Encryption : An Elementary Introduction. Providence, Rhode Island, American Mathematical Society, 2013.

This book provided a thorough historical overview of why encryption was required and how it was used in warfare. It also has a lot to say about Enigma, and what it did. This has really helped give us insight into why encryption was invented and how it was used to fight wars. It also gave more insight into how this is vulnerable to attacks.

Journal Articles

Lim, Matt. "RSA Encryption - the Startup - Medium." Medium, The Startup, 22 July 2020, medium.com/swlh/rsa-encryption-bdd80a3177. Accessed 6 Nov. 2022.

Reading this article really helped us visualize the mechanics of RSA. As there was a simple model of how the encryption works on the website. It provided a story into how RSA was first thought up in a dream. It also clarified our thinking into how RSA worked.

Claudio Di Giuseppe. "RSA Cryptography: History and Uses - Telsy." Telsy, 26 May 2021, www.telsy.com/rsa-encryption-cryptography-history-and-uses/#:~:text=The%20RSA%20encryption%20is%20a,project%20remained%20secret%20until%201997.. Accessed 27 Oct. 2022.

This article helped us understand the specific history about RSA better, as it talked about where and how RSA discovered and what caused them to discover it. It also gave us a brief introduction about how the RSA worked, and even provided a small snippet of code that could be implemented.

“Encryption Technology.” Www.rpc.senate.gov, www.rpc.senate.gov/policy-papers/encryption-technology#:~:text=Fourth%20amendment%20considerations&text=There%20is%20no%20exception%20for. Accessed 4 Dec. 2022.

This article has given us a new direction for research as the fourth amendment is enforced by encryption for personal use. But at the same time criminals can use this technology to protect themselves. However, when police gain this information in illegal ways it can’t even be used in court.

Sanchez, Julian. “Encryption Originalism.” Just Security, 16 July 2021, www.justsecurity.org/77383/encryption-originalism/. Accessed 4 Dec. 2022.

This article not only talked about the fourth amendment but also how the first amendment was also tied into this. In addition, it also gave a lot of court cases which I will research later. This talked about the FBI wanting to mandate backdoors in encryption which effectively lets them invade everyone's privacy.

Wong, David. “How to Backdoor Diffie-Hellman.” Cryptology EPrint Archive, 1 Jan. 1970, eprint.iacr.org/2016/644.

This article aided our understanding of a similar key exchange system called Diffie-Hellman. It also gave us a brief breakdown on what its flaws were. In this case, it was a bad and broken implementation of Diffie-Hellman, not an issue in Diffie-Hellman itself.

Wiener, Michael. “Cryptanalysis of Short RSA Secret Exponents.”, 3 Aug. 1989, https://www.cits.ruhr-uni-bochum.de/imperia/md/content/may/krypto2ss08/shortsecretexponents.pdf.

This article helped us realize that even an encryption like RSA that seems impossible to crack can still be cracked. It also somewhat explains the war between encryption and cryptanalysis.

Washington University. *The RSA Algorithm*. Washington University, 3 June 2009, https://sites.math.washington.edu/~morrow/336_09/papers/Yevgeny.pdf.

Our group was able to understand from the source that when someone wants to encrypt something, they utilize this technique. C = Ea(M) When someone wants to send another email to another person, they would get a public key encoded at M. This source also gave us a thorough understanding of what occurs when you send a message, email, or other communication to someone or to yourself.

Washington University. *The RSA Algorithm*. Washington University, 3 June 2009, https://sites.math.washington.edu/~morrow/336_09/papers/Yevgeny.pdf.

Our group was able to deduce from the discussion of switching keys that many nations use various keys, such as the Washington-Moscow hotline. The paragraph claims that a key is difficult to examine using cryptanalysis because it changes every hour. It also clarified how certain aspects of cryptology operate.

NIST. (1980). *FIPS 81 - Des Modes of Operation*. Federal Information Processing Standards Publications . https://csrc.nist.gov/csrc/media/publications/fips/81/archive/1980-12-02/documents/fips81.pdf

Our group learned from this source how binary data was employed to prevent the export of cryptography to other nations. To create a key, a combination of binary and cryptography were utilized. Furthermore, a hexadecimal cryptography key was employed. As stated on page 4, it appears that the meanings of the codes used in cryptography exist.

National Institution of Standards and Technology. *Data Encryption Standard*. Accessed 28 Nov. 2022.

Our group learned about the development of encryption from this source, which helped us with my data chronology. It discussed how encryption was adopted in 1972 as a long-term kind of defense against external threats. It also helped us fully comprehend how encryption is still utilized today, albeit for different purposes.

Wiener, M.J. “Cryptanalysis of Short RSA Secret Exponents.” IEEE Transactions on Information Theory, vol. 36, no. 3, May 1990, pp. 553–558, pdfs.semanticscholar.org/87ec/5b7f37a10669d6567659a3804f0fd29ed548.pdf, 10.1109/18.54902.

Our group can use the encryption code with the aid of this source. as stated on pages 1 through 14. Additionally, it provides a thorough argument for how we could use this code to advance our project.

Data Encryption Algorithm (DEA), ANSI X3.92-1981, American National Standards Institute, New York.

Our group learned from this source that encryption uses a 56-bit key to convert 64 bits of plain information into 64 bits of cipher text. We also learned that there are several equivalence transformations.

Horst Feistel, Cryptography and Computer Privacy, Sci. Am. 228 (5), 15-23 (1973).

Our group learned that there are two distinct types of encryption from this source. Code or cipher. It also explains what a code and a cipher are. A cipher replaces one set of alphabetic letters with another set of symbols. A code, however. For the persona, this is fundamentally semantic. Only predetermined meanings can be communicated by a code, which also allows for a private list like a code book.

Horst Feistel, Block Cypher Cryptographic System, US Patent 3,798,359, March 19, 1974.

Our group discovered that using encryption in a data processing center assures the total privacy of any data and information stored in or processed by a computing system. It also taught us how cryptography functions.

“What Is Data Encryption?" Definition, Best Practices & More.” *Digital Guardian*, https://digitalguardian.com/blog/what-data-encryption. Accessed 8 Dec. 2022.

Our group discovered from this source that the main purpose of encryption is to safeguard data when it is stored on your computer and delivered over the internet. It also informed us that contemporary encryption had taken the place of the

antiquated DES.

“What Is Encryption?" "Data Encryption Defined .” *IBM*, https://www.ibm.com/topics/encryption. Accessed on December 8, 2022.

This site taught us that encryption is safe because your computer manages and stores it. Additionally, it informed us that encryption uses cybersecurity to protect your data. There are two different kinds of encryption, which it also informed us about.

“What Is Data Encryption?” *Forcepoint*, 4 Dec. 2018, https://www.forcepoint.com/cyber-edu/data-encryption.

Our group learned from this source that encryption is one of the most crucial ways to protect your data and that very few trustworthy security programs are complete without it. It also informed us that there where two different kinds of encryption

Team, Tresorit. “The History of Encryption: The Roots of Modern-Day Cyber-Security.” *Tresorit Blog*, 14 Jan. 2022, https://tresorit.com/blog/the-history-of-encryption-the-roots-of-modern-day-cyber-security/#:~:text=Encryption%20can%20be%20traced%20back,of%20the%20World%20Wide%20Web.

We learned about the development of encryption from this source, including how it was utilized in battles as far back as the Roman Empire. We also learned about the popularity of encryption in the 1970s thanks to this site. Today, it also informed us about encryption.

“A Brief History of Encryption (and Cryptography).” *Thales Group*, https://www.thalesgroup.com/en/markets/digital-identity-and-security/magazine/brief-history-encryption. Accessed 8 Dec. 2022.

Our group learned about the history of encryption and how it was used in battles as early as the Roman Empire from this source. Our group discovered that a company called IBM was founded in 1970. It resulted in the development of the RSA.

Document

TüftelAkademie. “Quantum Key Distribution, BB84 - Simply Explained | Quantum 1x1.” YouTube, 3 May 2022, www.youtube.com/watch?v=8hNQyTdNil4. Accessed 2 Mar. 2023.

From this video, I learned the basics of the Quantum Key Exchange algorithm “BB84”. It uses 4 polarizations of photons in order to use the randomness of measurement to their advantage to detect whether there is an attacker eavesdropping on their communications.