Cryptography: A Journey to WWII and Beyond

Final Paper

CSC 321

4/16/2021

Ryan Morganti

**Abstract**

Billions of highly personal messages are exchanged daily and can result in severe consequences if they are read by the wrong person. So how is it possible to ensure that these messages stay confidential when these messages are sent through the public domain where theoretically anyone can read them? The answer to that is the mathematical field of cryptography. Cryptography simply is “enciphering and deciphering of messages in secret code or cipher”[[1]](#footnote-1). While studying this field, this paper will focus largely on its evolution and ultimate culmination of the classical portion in systems used during WWII. The following topics are to be discussed: a history of ciphers and cryptography focusing on specific system designs, the invention of the enigma machine, failures of enigma, the Allies decoding of the enigma, the contributions of cryptography to WWII, and the movement to modern cryptosystems and what that entails.

**Methodologies**

The questions that drove this paper were: how does cryptography work? What kind of systems were used previously? How did the enigma machine work, and how did the Germans utilize it? How were people able to break the enigma code? And how have modern systems moved away from those of the past? To achieve each of these, sources were found that pertained to cryptography in general or to the more specific questions. From there, an evolution of systems and their inner workings were compiled and explained in this paper.

**History of Cryptography**

From the dawn of civilization to modern day, keeping secrets has been integral to life. Whether it be a small secret between siblings or something major like a secret military operation, keeping this information private is a necessity. Often, messages need to be transmitted between parties to coordinate efforts, and sometimes they need to go through “enemy” territory where they need to stay confidential even if they are intercepted. This paper is going to focus on a few of the more famous systems that were used to accomplish this confidentiality. Throughout the paper, names like Alice will refer to the sender of the message, Bob, the recipient of the message, and Eve, a third-party intent on knowing Alice and Bob’s secrets for simplicity’s sake. At the most basic level, the goal of a cipher is to confuse Eve to the point that she does not know what the original message was but allow Alice and Bob to communicate knowing a certain key. What follows is the evolution from simple systems, which at the time were secure, to systems that are much more complex and harder for Eve to break. The systems that are discussed are classical cryptography since they rely on alphabets and encoding rather than encryption using mathematical properties. The first major system to emerge was used by Julius Caesar and is aptly called the Caesar Cipher.

Caesar and Affine Ciphers

The most basic and oldest ciphers rely on shifting each letter to another letter using a single alphabet. For example, A becomes D, B becomes E, Z becomes C, etc. The earliest form of this to be widely used in domestic and military affairs is named the Caesar Cipher, aptly named after Julius Caesar who pioneered the system. In his biography, it is noted that “…if there was occasion of secrecy, he wrote in cyphers”[[2]](#footnote-2). Ciphers like this one were easy to use and would confuse anyone merely glimpsing at the message during the era in which they were used. The cipher works as a special case of the Affine Cipher, which, mathematically speaking is defined as . Each character (M) is encrypted with some factor (a) and some additive (k) with respect to modulus 26 to keep the cipher text (C) within the alphabet. The Caesar Cipher is a special case where and . For the receiver to decrypt this, the formula is used. The inverse of a () is calculated by solving the equation . There are only 12 possibilities for to produce an inverse and 26 values of k, which leaves a total of total combinations of this type of cipher. Using modern technology, each of these combinations can be tried in a trivial amount of time, making the use of this type of cipher relegated to trivia and puzzles. Since the keyspace is so small, a better solution was needed that made it harder for Eve to crack the code and read the original message. This leads to a more general form of substitution ciphers.

Substitution Cipher

Since the problem with the shift ciphers is the small keyspace, a full substitution cipher can be utilized to give more possible combinations. Instead of using a mathematical equation to calculate the cipher text, the cipher text is constructed by using key words or known substitutions. This means that A can be swapped with any of the 26 letters, B can be swapped with any of the remaining 25 letters, and so on. This creates a keyspace of combinations. Since Eve does not know the key, the message, in her opinion, can produce anything using different keys. For example, given the cipher text of “grrd”, it can translate to room, doom, soon, jeep, etc. However, using different statistical and frequency attacks, the contents of the message can be determined. Using the fact that the word “the” is the most common word in the English language and that the letter “e” is the most common letter, it follows that the most common occurrence of a letter in the cipher text is probably “e” in the real message. This can be done with each letter with a varying degree of success and interpretation done on Eve’s part. To protect against these kind of attacks, new systems were created that utilize multiple alphabets, the most famous of which is the Vigenère cipher.

Vigenère Cipher

In the 16th century, a French cryptographer Blaise de Vigenère invented a system known as the Vigenère cipher. The credit of this system cannot be entirely given to Vigenère since many mathematicians proposed parts of the system before him. This includes Leon Battista Alberti who suggested rotating the shift in a shift cipher every few words, Johannes Trithemius who proposed changing the alphabet used each time, and Giovanni Battista Porta who combined the previous ideas. Vigenère took Porta’s ideas and published them, making them famous[[3]](#footnote-3).

The basic premise of the Vigenère cipher is that a repeating keyword is used to make the substitutions. A key decided upon beforehand by both the sender and receiver is used repeatedly for the entire message. Instead of utilizing one alphabet, like previous systems had, this makes use of multiple alphabets, meaning that a substitution can be distributed over varying alphabets, changing the cipher depending on the location. In this system each of the alphabets start with the letter of the key at that position. For example, the key CIPHER would produce 6 alphabets with the first being CDEF…, the second being IJKL…, and so forth. Then to encrypt a message, HELLOWORLD for example, the first letter would be lined up to the first alphabet and found where it intersects, the second lined up with the second alphabet and so forth. This would produce the cipher text jmassnqzak. Notice that the two L’s in the plain-text message encrypted to different values based on the key. This defeats the statistical analysis attacks used on previous substitution attempts.

Even though this solved the problem of basic statistical analysis, there are still weaknesses and downfalls of using this system. The failure lies within the key used. Since it is a repeating key, patterns emerge that allow a few different tests to be conducted. The Kasiki test, invented by Friedrich Kasiki and published in 1863, looks for these patterns. Ironically, the test was also independently discovered by Charles Babbage about 10 years prior.[[4]](#footnote-4) By calculating the distance between repeating groups of letters, and comparing all distances of repeats, the key size can be guessed to a good percentage of accuracy. This only works due to accidental lining up of key and plain text multiple times and is not found in every message. The other test to calculate key size was invented about 60 years later by William Friedman. This works by calculating the Index of Coincidence (IC) of two letters appearing next to each other. Then by guessing key sizes and calculating the IC based on the guess and comparing it to known values, the key size can be guessed. After determining the key length, statistical analysis used to break monoalphabetic ciphers can be applied for each alphabet to break the message. Also, using modern technology, brute forcing the key using a dictionary attack, one where a large list of words is used as possible keys, can work to decipher this system.

Running Key Cipher

Since the Vigenère cipher’s weakness is due to the repeating key, choosing a non-repeating key solves some of its issues. Both the Kasiki test and IC become useless since the key size is irrelevant as it is the length of the entire message. In his writings, Blaise de Vigenère described the method that is referred to as the autokey cipher. By deciding on a primer key, either a single letter, or word, the rest of the message is enciphered using a combined key of the primer and the plain-text message. For example, the message MATHISFUN with initial key PI, would have the full key of PIMATHISF. Another version that evolved out of this system is using a book, speech, or some other long series of words as the key. Both cases suffer from the same weakness and downsides. Since the key is likely to be made up of proper words, since the key is found in a written work, then regular statistical analysis can apply to the key. Once again, William Friedman, invented an attack against this system. By taking each cipher text letter, certain combinations of the message and key is more likely than others. For example, the cipher letter A is most commonly a combination of letters H and T.[[5]](#footnote-5) By taking each of these likely pairings and forming words out of both message and key combinations, and many attempts, the original message can be decoded.

Since these methods suffer from recognizable text, the next logical step would be to mix up, or randomly generate the key. This method, known either as the one-time pad or the Vernam cipher, was proposed by Gilbert Vernam and Major Joseph Mauborgne around year 1918[[6]](#footnote-6). If the system is truly random and the key is never repeated, then it is impossible to crack. The issue though is the number of pages that are needed to be produced and distributed. If millions of messages are being sent, then millions of pages of these random keys need to be produced and distributed beforehand. This is nearly impossible to do and maintain. The other issue is constructing truly random data and not data driven by pseudo randomness that can be reverse engineered.

**Cryptography in World War II**

During times of war, sending messages to different troops and keeping troop movement secret is a necessity. Opponents will have dedicated teams trying to crack the encryption that their enemies use and will dedicate resources implementing their own encryption schemes. Since there is so much scrutiny to these codes, systems can change relatively fast as old ones are broken and new ones are necessary to implement. In World War II (WWII) especially, there were numerous systems that evolved and were implemented at some point during the war. The two most famous systems to emerge that the Germans used were the enigma machine and the Lorenz Cipher. This paper will focus on the enigma and not the Lorenz cipher.

How the Enigma Works

The creation of the enigma machine predated WWII by decades and was relatively simple at first. What allowed the enigma to come into existence was the invention of a rotor, which is an electrical device that does letter substitutions by sending electrical input from one letter to a different letter. Between 1917 and 1923 this device was independently invented by four separate men in four different countries.[[7]](#footnote-7) In the Netherlands in 1919, Hugo Koch filed for a patent on his encryption machine. This was the precursor to the enigma machine, but ultimately Koch did little with that machine until he sold the patent to Arthur Scherbius. Scherbius took the machine to mass market and is credited with the invention of the modern enigma machine[[8]](#footnote-8). Scherbius brought his machine to the German navy for use, and they found no issue with his machine. However, until the rise of Hitler, the machine was relatively unused for military purposes.

The machine has a keyboard that, when a letter is pressed, completes a circuit. The circuit first goes through a plug board that performs initial substitutions and then through a series of rotors, which act as the different alphabets found in the Vigenère cipher. Finally, it hits a reflector that sends the electric signal back through the same rotors, performing more substitutions, until it reaches the output side where it lights up the corresponding cipher character. To introduce a running-key cipher, the first rotor would rotate a spot after each character, and the second and third would be turned over by the preceding rotor when it hit a certain spot. In the original schematics, the machine worked with exactly six wires in the plug board and three rotors with a specific reflector design. Later this would be updated to include different reflectors and number and design of the rotors. It was also originally marketed in both a commercial and military design with only slight differences in wiring between those versions.

German Enigma Usage

The Germans suffered from an overconfidence in their machine which led them to create flaws in the transmission protocol. Since the keyspace of the enigma machine has more than 3x10^114 possibilities and combinations, the Germans believed that whatever they sent using it was impossible to decode and that the code was unbreakable[[9]](#footnote-9). However, the Germans never actually utilized the entirety of this keyspace and limited themselves by using common rotor patterns and plug board settings quite often. When the Germans wanted to send a message, the operator would use the daily code given to them by high command. They would set the rotors to that initial setting and choose a random session key. They would then type that session key in twice and set the rotors to the positions dictated by the session key. This was to help further randomize the message in case the daily key was ever leaked. The receive end would also have set the rotors to the daily key and would type the duplicate session keys out to recover the session key. From there, the operator would then set the rotors to the session key and then proceed to decode the rest of the following message.

Enigma Flaws

The German implementation of the enigma machine suffered from a few key design and operation failures that led the allies to ultimately be able to crack the “unbreakable” code. The only flaw that the machine itself held was that it would never be able to encipher a character back into itself, meaning that the cipher text “a” could never have corresponded to the plain text letter “a”. This makes it slightly easier to decode a message since the possible input letters are only 25 instead of 26. The rest of the flaws lay with the operators of the machine. The redundant typing of the session key twice, although implemented to lower transmission errors of that key, led to a decreased key space since it is repetitive of a word in the cipher message. Also, operators were told to come up with the session keys independently and randomly, but coming up with true randomness is very difficult for human nature. Just as people use common passwords or passwords that relate to them personally, the German operators would use simple keyboard patterns like abc, aaa, qwe, etc. If they were not using these patterns, they would probably be using the name of a girlfriend or pet. By knowing these habits and layouts of the keyboard being used, a decryption machine can cycle through common possibilities to help aid the decryption process. This did not work in every scenario, but a large portion of the session keys could be broken by these simple tricks, just as passwords are cracked today. Furthermore, another flaw lays with re-transmitting. Sometimes the message would transmit incorrectly, so the operator would need to retransmit that same message and use a different key. This meant the Allied forces would be able to take both messages and compare their differences and have a better idea as to what the message contained. Another problem was that the Germans would use repetitive words, like ending the messages with “Hail Hitler” or sending a daily weather report that always had the word weather in it. This led to what the English referred to as message cribs, which significantly reduces the amount of test cases they would need to check to decipher the message.

Initial Polish Decryption

Before WWII started, the Poles were able to acquire a commercial grade enigma machine and break the encryption scheme. Led by Marian Rejewski, the Poles were able to lay the groundwork on mathematical permutations in calculating the rotor positions. They came up with a method of calculating permutations and comparing them with key sequences that would commonly appear on the keyboard being used. By adopting this method, the cryptography team would only need to test some few thousand different permutations instead of millions[[10]](#footnote-10). By using that data, the Poles were able to calculate the key used for the day and came up with formulas to find the rotor positions. They invented a machine called the Bomba that was able to run through all these combinations and find one that would successfully work. The machine was able to decode almost every enigma encrypted message in about 2 hours[[11]](#footnote-11). When the Germans introduced 2 new rotors to make the machine more secure in 1938, the Poles had little resources to continue their calculations. They turned their resources over to the English in 1939 so the English could continue their work.

Cracking and Allied Force Decryption

The Allies took the Poles’ work and were able to expand on it with new resources. At the English cryptography center at Bletchley Park, the team of hut 6, which included Alan Turing and Gordon Welchman, were able to reconstruct and expand on the Polish Bomba machine. Their machine became known as the Turing Bombe. By studying and testing different common permutations for the messages, they were successfully able to decipher messages sent from the 3-rotor enigma at a rate of about 50,000 per month.[[12]](#footnote-12) When the Germans increased the rotor count to 4, the rate went drastically down.

Contributions to the War

The English kept their decryption efforts top secret and classified to everyone outside of Bletchley Park. This operation was called Ultra, and it was a complete success. By keeping their decryption findings secret, the Germans never figured out that their encryption scheme was broken, and that let the English have an advantage over them. This project was also very careful on what was allowed out to be used by military intelligence and was often covered secretly by false reports of new sonar or long-range scanning equipment.[[13]](#footnote-13) The full release of the details of this project were not released until the 1970s.

World War II saw the onset of some of the most complex classical cryptosystems emerge, and many brilliant mathematicians were stumped by them. Ultimately human blunders, pressures of war, and relentless mathematical attacks brought these systems to their knees and changed the course of the war and history. An apt description of moderns wars, taken by Craig Bauer: “World War I is referred to as ‘The Chemists’ War’ due to the major role of chemical warfare, and World War II is called ‘The Physicists’ War’ because of the atomic bomb. It has been claimed that, if it occurs, World War III will be ‘The Mathematicians’ War’”[[14]](#footnote-14). As important as cracking codes was in WWII, it has only gotten that much more so in modern day cryptosystems.

**Modern Day Cryptosystems**

Modern day cryptosystems began to emerge in the 1970s and later and have replaced all earlier systems. Instead of deciding on a substitution or rotation scheme, a mathematical system is used. That means that each letter needs to be represented in a numeric format. This is accomplished in a few ways, either by using a hashing algorithm or using the hex representation for ascii letters (a = 61, b = 62, etc.). Then the message is combined into one numeric string. For example, “hello” would become “68656C6C6F”. Then finally that number would be converted into decimal which would be 448378203247. This is practically impossible to compute by hand, but with the onset of computers, mathematical encryption becomes trivially easy to use and is far more practical. Depending on the system used, all that is necessary is for both parties to know a public number that is available to everyone. There are two main methods of this in use today: asymmetric key systems and symmetric key system. Generally, the symmetric key systems are much faster, but transferring the key over a line is problematic, which is why asymmetric key systems are generally used to transport the key for symmetric systems.

Asymmetric System (El Gamal)

One of the earlier forms of asymmetric key systems is the ElGamal system. It was invented by Taher ElGamal in 1985, and although cryptographically secure, remained relatively unimplemented due to the RSA algorithm written just 8 years prior.[[15]](#footnote-15) The system is based on the earlier Diffie-Hellman key exchange algorithm that provided a method for two separate parties to conduct mathematical operations using separate private keys to create a shared private key between them. This key exchange did not however provide how to enable secure messages to be sent between the parties once the key was generated. This led to the ElGamal system to be created. The system starts with two publicly known pieces of information, a large prime, p, and a primitive root of p, g. A primitive root is a number that generates the entire finite set, or, mathematically speaking, the first occurrence where is at x = p. After deciding upon these public values, Alice computes some private exponent, a, and Bob computes his own private exponent, b. Then for Bob to send a message to Alice, Alice first needs to send Bob . He receives that and calculates and sends that to Alice. in this case is the plain-text message he wishes to send, in numeric format. Alice can then recover the plain-text message by computing . Ultimately, this system is cryptographically secure which means it is possible to break it, but would involve intense, time consuming computation power. Eve can break the system by calculating the discrete log problem and solving for .

Asymmetric System (RSA)

The RSA system was invented in Ron Rivest, Adi Shamir, and Leonard Adleman in 1977 while they were at MIT. RSA works by publishing two pieces of information that are accessible to all who want it. These are a large composite number N that is the product of two primes () and an encryption exponent, e (where ). Alice then also calculates a private key d, such that . For Bob to send Alice a message, he takes her published N and e values and calculates . He then proceeds to send that encoded message c to Alice. All Alice needs to do to decrypt the message is to take . Using modern computers, this process is quite easy to compute and does not take up that much processing power in either the encryption or decryption process. Although this seems insecure, it is cryptographically secure, since the ability to factor numbers increases tremendously for large numbers N. For Eve to calculate the decrypting exponent, she must first factor N, which becomes nearly impossible even using modern computers as N grows larger. A 1024-bit number produced using two primes is not able to be cracked without taking millions of years with modern day systems. With the onset of quantum computing, factorization will become significantly faster, and the security of the system is called into question. But for now, using sufficiently large numbers will ensure a protected RSA cryptosystem.

Symmetric System (AES)

The Advanced Encryption Standard is the most commonly used symmetric key today. It was invented in 1998 by Vincent Rijmen and Joan Daemen who were from Belgium.[[16]](#footnote-16) Unlike the other ciphers mentioned before, AES is a block cipher and not a stream cipher. This means that it encodes blocks of data instead of lines of code. The inner workings of the algorithm are complex, but it mainly takes the entered data block and mixes the columns and rows up. It adds the private key to the block matrix and performs a substitution based on a predefined table. It then undergoes 14 total passes for the 256-bit key size and less total passes for smaller keys. The passes take a key schedule and mix the keys appropriately using a special algorithm. Unlike ElGamal and RSA, there are no known attacks or ways to break this algorithm using mathematical principles besides brute force, which is impossible considering the massive key space AES has.

**Conclusion**

Cryptography, over the span of thousands of years, has grown considerably more complex. Using methods of cryptoanalysis, most forms of classical systems can be broken. Although by jumping through multiple different alphabets to substitute letters, it becomes much more difficult for an outside user to be able to break the system. After WWII and with computers being more largely used in the 1970s, new systems were invented that rely on mathematical concepts and cannot be broken unless a mathematical problem can be solved. These problems become increasingly difficult and approach an impossibility for being cracked when sufficiently large numbers are used to encode. Although the process of encryption has changed drastically from the first known systems, the entire concept has remained consistent as people will always want to hide their secrets from prying eyes. As one system is broken, another new system will crop up and take its place, and that cycle will seemingly continue forever, at least for the foreseeable future.

References

Bauer, C. P. (2021). *Secret history: The story of cryptology*. Boca Raton: Chapman & Hall/CRC.

Cryptography. (n.d.). Retrieved April 11, 2021, from <https://www.merriam-webster.com/dictionary/cryptography>

Diffie-Hellman Protocol. (n.d.). Retrieved from <https://mathworld.wolfram.com/Diffie-HellmanProtocol.html>

Diffie, W., & Hellman, M. E. (n.d.). New Directions in Cryptography. Retrieved April 11, 2021, from <https://www.cs.jhu.edu/~rubin/courses/sp03/papers/diffie.hellman.pdf>

Enigma History. (n.d.). Retrieved April 11, 2021, from <https://cryptomuseum.com/crypto/enigma/hist.htm>

Hardy, D. W., Richman, F., & Walker, C. L. (2009). *Applied algebra: Codes, ciphers, and discrete algorithms*. Boca Raton, FL: CRC Press

Hoffstein, J., Pipher, J., & Silverman, J. H. (2014). *An introduction to mathematical cryptography*. New York: Springer.

Klima, R. E., & Sigmon, N. P. (2019). *Cryptology: Classical and modern*. Boca Raton: CRC Press, Taylor & Francis Group.

Kraft, J. R., & Washington, L. C. (2018). *An introduction to number theory with cryptography*. Boca Raton: CRC Press.

Lapienytė, J. (2021, February 13). What is AES Encryption and How Does It Work? Retrieved April 11, 2021, from <https://cybernews.com/resources/what-is-aes-encryption/>

Mollin, R. A. (2007). *An introduction to cryptography*. Boca Raton: Chapman & Hall/CRC.

Mollin, R. A. (2019). *RSA and Public -Key Cryptography*. S.l.: CRC PRESS.

Padhye, Sahadeo. Sahu, Rajeev A.. Saraswat, Vishal. (2021). *Introduction to Cryptography*. S.l.: CRC Press

Tranquillus, C. (n.d.). The Lives of the Twelve Caesars. Retrieved April 11, 2021, from <https://www.gutenberg.org/files/6400/6400-h/6400-h.htm>

Ultra. (n.d.). Retrieved April 11, 2021, from <https://www.britannica.com/topic/Ultra-Allied-intelligence-project>

Vernam-Vigenère cipher. (n.d.). Retrieved April 11, 2021, from <https://www.britannica.com/topic/Vernam-Vigenere-cipher>

1. Meriam Webster Dictionary [↑](#footnote-ref-1)
2. The Lives of The Twelve Caesars [↑](#footnote-ref-2)
3. Secret History; The Story of Cryptography pg 61-62 [↑](#footnote-ref-3)
4. Cryptology Classical and Modern pg 224 [↑](#footnote-ref-4)
5. Secret History; The Story of Cryptography pg 82 [↑](#footnote-ref-5)
6. Britannica: Vernam-Vigenère cipher [↑](#footnote-ref-6)
7. Secret History; The Story of Cryptography pg 217 [↑](#footnote-ref-7)
8. Crypto Museum [↑](#footnote-ref-8)
9. Cryptography Classical and Modern pg 75 [↑](#footnote-ref-9)
10. Secret History; The Story of Cryptography pg 236 [↑](#footnote-ref-10)
11. Cryptology Classical and Modern pg 79 [↑](#footnote-ref-11)
12. Secret History; The Story of Cryptography pg 251 [↑](#footnote-ref-12)
13. Britannica: Project Ultra [↑](#footnote-ref-13)
14. Secret History; The Story of Cryptography pg 166 [↑](#footnote-ref-14)
15. An Introduction to Cryptography pg 181 [↑](#footnote-ref-15)
16. CyberNews [↑](#footnote-ref-16)