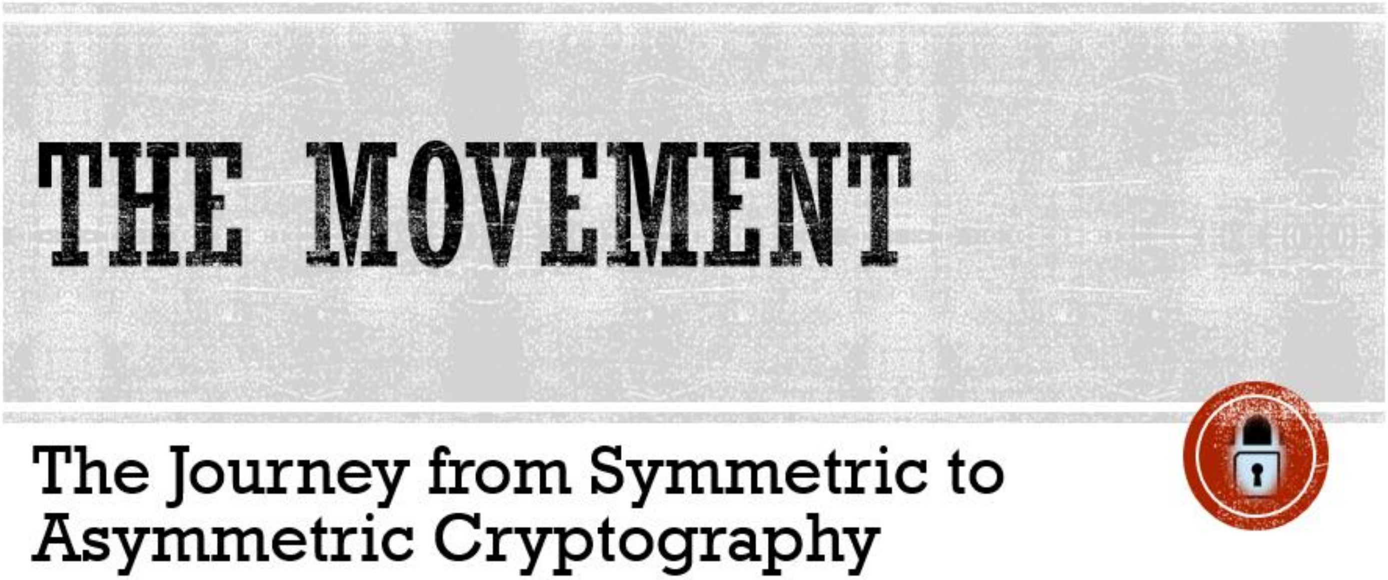
University of Guyana

CSE2203 (2017 – 2018)



THE MOVEMENT

The Journey from Symmetric to Asymmetric Cryptography

Farnaz Baksh (*usi n#*)

Kim Shing Chong (*usi n#*)

Shemar Brandon Austin (*usi n#*)

Shomari Williams (*usi n#*)

Dwight Ferguson (*usi n#*)

Group E

3/9/2018

1. Introduction

In order for us to understand how we reach to this present stage in the field of cryptography, we must know a bit of its history. This essay will highlight important events along the way of this amazing journey of *code making and breaking*.

Protecting the information that humans exchange has been extremely important for a long time; this can be dated back to the *Stone Age*. Over 30,000 years ago, humans began to communicate using language. During that time, written language was considered an art so the people of that era used to communicate with simple drawings; examples of such can be found on cave walls and clay accounting tablets. The evolution took place over the years and from this we can say steganography and cryptography emerged since it was around the *Bronze Age* (3500 to 1200 BC) when the Egyptian would have carved hieroglyphic symbols into rocks at their tombs.

Steganography and Cryptography has a distinct meaning even though both terms were derived from the Greek. In steganography, persons should not detect the existence of the message but the message itself may not be difficult to decode; whereas in cryptography, persons should be able to tell that the message has been encrypted but they cannot decode the message without knowing the key itself.

Early documentation of steganography are dated back during the first century A.D, when the substance from the *tithymalus* plant was used as an invisible ink. Herodotus was a Greek historian and recorded the evolution of steganography in his book: *The Histories*. The father of history mentioned the conflict between Greece and Persia in the year 480 B.C. The story goes that a loyal Greek send a hidden message from Persia to Greece by scraping the wax off a pair of wooden folding tablets, wrote the message warning the Greeks about the ‘Persian military attack buildup’ on the wood of the tablet and then cover the message over with wax again. The other incident of simple message hiding that Herodotus recorded was *the story of Histaiaeus*; where they shaved the head of a messenger, wrote the message on his scalp, and then waited for the messenger hair to regrow.

The ancient Chinese also have a history in the field of "hiding the existence of a message" whereby they would write their message on fine silks and make them into a tiny ball where they then would covered it in wax and swallow it. By intuition, you can only imagine which end they would regurgitate or pass out the hidden message.

Cryptography began to develop with the aim of not to hide the existence of a message, but rather to hide its meaning; that process is now called *encryption*. The field of cryptography has two branches, namely: *transposition* and *substitution*. We will explain each branches more in-depth along with the two types of encryption namely: Symmetric (also called “secret key” encryption) and Asymmetric (also called “public key encryption”) in this essay.

2. Cryptanalysis

Cryptanalysis aims to understand how ciphers, ciphertext and cryptosystems works and while improving techniques for defeating or weakening them. Cryptanalysis sees its origins going as far back as the ninth (9th) century Arabs, more specifically, a mathematician by the name Al-Kindi, who would’ve developed a method for breaking ciphers at the time.

Cryptanalysts over the years with the gradual development of cryptography, have been tasked with ensuring that ciphers and algorithms are capable of protecting sensitive data from being compromised. Notable instances in which cryptanalysts were able to come in “clutch” as it were, include: during World War I when the British intercepted the German Zimmerman telegram, which when decoded revealed the German plan to go back on their policy of unrestricted submarine warfare, which was the only thing keeping the US neutral in the war. Another instance again, was in World War II where deciphering of enemy ciphers, was quoted as being “decisive” to the Allies securing victory.

Cryptanalyst methods have come a long way since the first frequency attack designed by Al-Kindi. The most common attacks currently used include, the **ciphertext attack**, where the analyst is able to intercept an already ciphered message and then begin attempting to break the cipher. The second attack, is the known **plaintext attack.** This attack is the opposite of the ciphertext attack, in which this attack has the analyst being able to intercept the original deciphered text from which they then attempt to recreate the cipher. Another attack, the chosen plaintext attack, the analyst either knows the encryption algorithm or has access to the device used to do the encryption. The analyst can encrypt the chosen plaintext with the targeted algorithm to derive information about the key.

Other attacks include, the **dictionary attack** which is used for password protected files, by running a wordlist consisting of common word combinations against the algorithm to try and access the data. The **man in the middle attack**, which as the name suggests operates by having an attacker exist between the two communicating parties, after which they begin either intercepting messages or altering messages between the parties. The final attack being mentioned, is the **differential cryptanalysis attack**. This attack involves analyzing multiple plaintexts in order to notice patterns present within them, to help with breaking block ciphers.

Cryptanalysis will always be necessary, once cryptography exists. This is so, since cryptanalysts can exist on both sides of the coin as it were. With different means of encryption being developed, developers would want white hat analysts to be able to find exploits, in order for them to be corrected, before they are exploited by the wrong persons, and compromising information.

3. Symmetric Cryptography

Symmetric Cryptography (also known as the symmetric-key algorithm) works by having both the sender and recipient use the same key that was used to encrypt the message, to decrypt it. This key does not necessarily have to be a word or a number it can also be a physical object as we will talk about later. One of Symmetric Cryptography's biggest issue has always been how to get the same key to all the receiving parties without any unwanted interference.

Cryptography can be broken down into two major parts which are transposition and substitution; both of which falls under symmetric cryptography. The transposition method works by switching the places of letters while substitution works by changing the value of the letters. The usage of these methods date back as far as the *Spartans* (around 404 B.C) and have been used for military purposes ever since.

An easy example of transposition is changing the word "crypt" to "tyrpc". The letters of the word still retain their value but they have changed their position. This however can present some obvious problems for one word will only have a small limited amount of places the letters can go. Three letter words can only be switched by six places and five letter words such as the word "crypt" can only be switched so many places. However as words or the sentences get larger and larger it becomes increasingly difficult to even think about going through all the possible combinations and get the right one. **A simple sentence such as this one in bold**, has literally over 50 x 10^25 or (50,000,000,000…) different combinations. Without knowing the exact way to rearrange the letters to get back the plain text, it is impossible to force your way through deciphering long messages. In order for transposition to be effective the scrambling protocol needs to follow a specific algorithm which only the sender and recipient should know. One method of doing this is by the Rail Fence cipher where the words alternate either by superseding or superseding the letters by a few lines. For example the Phase “Facts are Irrelevant” will read as “FCSRIRIVNATAEREEAT”. This happened because every other letter was placed on the line above and then rewritten as if they were one word. This is as simple as this method gets and to get back the plain text simple count the amount of letters, cut them in half and rewrite them with one have superseding the other

Another method of transposition is called the Route Cipher which works by putting the words in a grid with specific rows and columns then re-write in the line. For example the phrase “Facts are irrelevant” would be written as “FTRRLAASERENCAIEVT”. Without knowing that the phrase was written in a matrix of 3 rows by 6 columns you would have to randomly place that cipher text in grids that is if you know it was encrypted by a grid and not another method.

One of the most popular and earliest uses of the Transposition method is in the fifth century when the Spartans used what was known as a Scytale. This was a piece of wood with a specified diameter. The way this was used as a key to encrypt messages was by wrapping a paper around the wood and writing the message alongside the wood so when unwrapped the paper will contain what seems to be just a bunch of random letters. To get back the original message you would need a wood of similar diameter and wrap the message around and read it alongside the wood.

Substitution is the method of changing the value of the letters of a word or message and the earliest known recording of this type of encryption appears in the Kama-Sutra. It recommends that women learn the art of substitution cryptography to assist their “liaisons” in concealing messages. The way they did this is by pairing the letters of the alphabet with other letters so that when encrypting a message you would just replace the letters with their partners. However, one of the most famous form of substitution is known as the Shift Cipher or the Caesar Cipher. This Cipher works by *Shifting* the letter by the letter a specified number down in the alphabet. For example shifting our alphabet by 1 space would change **A** to **B** and **B** to **C**, similarly a shift of 3 spaces would change **A** to **D** and **B** to **E**. This is a very popular form of substitution and was used by *Julius Caesar* who it got its name from because of his frequent use of it. Julius first used ciphers by replacing the Roman letters with Greek letters to make the message illegible to the enemy however this method was not his only form of encryption. Of course you are not restricted to using just three shifts there are twenty-six letters so you have twenty-five shifts to choose from. But if you decide not to restrict yourself to just the plain alphabet you can generate generally any amount of ciphers or about "400,000,000,000,000,000,000,000,000"; according to "The Code Book" by Simon Singh.

Any one of those ciphers can be considered a different method of encryption and have a key that specifies how it is encrypted. The key can also specify the exact kind of cipher alphabet to be used. Any person looking at the cipher text may be able to tell what kind of algorithm was used and that the letters were replaced by a different cipher alphabet but would not be able to know exactly what cipher alphabet was used. This is why keeping the key a secret between the sender and receiver is important even if the algorithm is known, because anyone who does not know the key may not be able to decipher the ciphertext if they happen to intercept the message. It would be a lot more practical to use an algorithm with lots of potential keys for increased security. For example the Caesar Shift Cipher only has 25 possible key combinations so anyone who really wants to decipher the message would be able to. Therefore using a substitution method that has a lot more possible combinations will have a lot more key combinations and will be increasingly difficult for unwanted parties to break. It is efficient to make sure the sender and the receiver have no misunderstanding about what the key is or else the encryption would be useless. A method to avoid this understanding is to use a KeyWord or Phrase. The way this would work is to remove all the spaces or letters that would be in the keyword/phrase then use it as the beginning of the cipher alphabet, then place the remaining letters of the alphabet at the end of the keyword/phase. Using this is convenient because the key in this case will be a lot easier to memorize and would be much more difficult to misunderstand. One advantage of this in history is that the code would no longer have to be written on a paper that the enemy can easily find and read, it can just be committed to memory.

4. War Driven Cryptography

To understand why it was necessary to develop asymmetric cryptography we must first understand the anomaly that directly influenced the paradigm shift. A model described by Thomas Kuhn in 1962 in his seminal work *The Structure of Scientific Revolutions* does well to explain how a model crisis will lead to a better developed model. In the case of symmetric cryptography the model crisis that lead to the development of asymmetric cryptography was the key exchange problem and how secure the key exchange processes was. One of the greatest examples that exemplify this anomaly is that of the breaking of the enigma code and the subsequent ending of World War II. World War II began on September 1, 1939 when Germany invaded Poland, Britain and France responded by declaring war on Germany on September 3. As time progressed more countries got involved. With many rival nations engaged in war secure communication between nation and allies was of great importance and as such cryptography was used extensively. The most significant display of cryptanalysis during the war was the first full successful break of the enigma code. The Enigma was invented by German engineer Arthur Scherbius at the end of World War I. It was in 1932 when the Polish government was successful in “cracking” the enigma code, seven years before the start World War II .This event triggered the German’s need to develop a more secure chipper, during World War II the German’s had what is said to be the most secure cipher at the time, the enigma cipher. They achieved this by changing the chipper system daily. When the Polish cracked the enigma code the main codebreakers who joined the Polish General Staff’s Cipher Bureau in Warsaw were Jerzy Rozycki, Henryk Zygalski, and Marian Rejewski. At this time the British were also trying to crack the enigma using linguists. However, the Poles realized it was imperative to use mathematics to determine code patterns. Building some electro-mechanical machines to make calculations for solutions (called “bombes”) helped them greatly. Later on, A British mathematician named Alan Turing visited the Polish code breakers personally. It was this visit that helped him build his own electro-mechanical “bombe,” which worked by simulating the operations of the Enigma machine. Alan Turning studied at both Cambridge and Princeton universities. He was already working part-time for the British Government’s Code and Cypher School before the Second World War broke out. In 1939, Turing took up a full-time role at Bletchley Park in Buckinghamshire – where top secret work was carried out to decipher the military codes used by Germany and its allies. The main focus of Turing’s work at Bletchley was in cracking the ‘Enigma’ code. He along with fellow code-breaker Gordon Welchman invented what is now known as the Bombe machine, the machine was built by the British Tabulating Machine Company in Letchworth, Hertfordshire under supervision of Harold Keen. A machine that was capable of recovering the key settings even if the Germans would drop the double encryption of the message key at the beginning of each message. Turning’s approach was based on the assumption that a known (or guessed) plaintext, a so-called crib, is present at a certain position in the message. The Bombe was further enhanced with the diagonal board that greatly reduced the number of steps needed for the codebreaking effort. From mid-1940, German Air Force signals were being read at Bletchley and the intelligence gained from them was helping the war effort. Because it is possible to intercept a symmetrically keyed text and infer the key was the main reason that the Enigma code was cracked and this is evidence of the model crisis that exists in symmetric cryptography.

5. Asymmetric Cryptography

During the 1960s, computers were powerful, and they were affordable for businesses and organizations. Computers were used to encrypt important communications and transactions within the businesses. As businesses bought computers, encryption spread between the businesses, and cryptographers were confronted with a major problem known as key distribution. The key distribution problem was discovered using Symmetric Cryptography.

According to Lecturer Tom Roeder, in 1969, the Government Communications Headquarters(GCHQ), an intelligence and security organization responsible for providing signals intelligence and information assurance to the Government and armed forces of the United Kingdom in Great Britain had tasked James Ellis (24 September 1924- 25 November 1997), a British engineer and cryptographer to look at the key distribution problem. Ellis in 1970, proposed using Asymmetric Cryptography with a pair of keys, one key is used to encrypt (public key) the message and the other key (private key) is used to decrypt the message. Ellis's proposal was reviewed and to deploy his idea, he had to derive at an algorithm in order for the idea to become successful. In 1973, Clifford Cox (British mathematician and cryptographer) teamed up with James Ellis in order to assist him in finding a solution to the key distribution problem. Cox had recently started working at the GCHQ at that time, and it was not long after that he finished his studies he decided to work with Ellis on the proposal. Cox believed that he could contribute to Ellis's proposal since he was good with prime numbers and factoring. After Cox did his research and progressed with his work, Malcolm Williamson in 1974, discovered Whitfield Diffie attempting to find a way to break Cox's work.

Bailey Whitfield Diffie (born in 1944 in Washington DC), an American cryptographer and one of the pioneers of public key encryption, was captivated by the problem of key distribution that it became the most important entry in his notebook entitled "Problems for an Ambitious Theory of Cryptography". Diffie's idea was similar to that of James Ellis. According to the Code Book, Diffie was fearful that the necessity of key distribution would prevent the public from having access to digital privacy, and he became obsessed with the idea of finding a solution to the problem. In 1974, Diffie visited the IBM's Thomas J. Watson Laboratory where he was invited to give a talk. After his speech, he was told that Martin Hellman (a professor from Stanford University in California) also addressed the issue of key distribution. Diffie had hooked up with Martin Hellman in order for them to solve the key distribution issue.

Martin Hellman, born in 1945, grew up in a Jewish Neighborhood in the Bronx. He was also interested in the issue of key distribution as Diffie was. From 1974 onwards, together the duo tackled the problem of key distribution, but in order to be successful, they had to derive an algorithm in order for the solution to work the way they projected it to. The duo published a paper popularly known as "New Directions in Cryptography" describing the public key encryption in 1975. The Diffie-Hellman key exchange scheme was similar to that of James Ellis's using the public key and the private key. Diffie and Hellman published the Diffie-Hellman Key-Exchange in 1976. The Key Exchange became successful with the help of Ron Rivest, Adi Shamir and

Leonard Adleman in 1977 when the RSA Algorithm was published. By 1975, James Ellis, Clifford Cocks and Malcolm Williamson had discovered all the fundamental aspects of public-key cryptography, yet they all had to remain silent. Ellis and Cocks watched their discoveries rediscovered by Diffie, Hellman, Rivest, Shamir and Adleman. Cocks in 1973, had described an equivalent system in an internal document to the RSA Algorithm.

According to the Open Secret, in 1977, the British cryptographers were upset to learn that both Stanford University and MIT were planning to patent, respectively, the Diffie-Hellman and RSA algorithms. "I tried to get them to block the US patent," Williamson says. "We could have done that, but in fact the people higher up didn't want to. Patents are complicated." Specifically, there was a question as to whether one could obtain a patent under British law for what was essentially a mathematical algorithm. "The advice we received was, 'Don't bother,'" says Cocks.

In 1979, there was a Computer Conference hosted by the National Security Agency (NSA). At that time, Bobby Inman (born in 1931), a retired United States Admiral was the Director. Inman hailed Diffie and Hellman for their publishing. After he would have given his speech, a reporter asked him, “Do you think that Diffie-Hellman Key Exchange will make it harder for the NSA to accomplish its mission?” Inman responded, “We knew about that 10 years ago.” Inman’s response baffled Diffie, and cause him to question the audience. Someone whispered that it was James Ellis who came up with the idea of the public key cryptography. Diffie travelled to Britain to meet with James Ellis. Ellis said to Diffie, “You did more with it than we would have.”

It was in the 1990s, the British GCHQ had decided to declassify the reports produced by James Ellis, but he passed away and received no credit for the work he had done with the help of Clifford Cox. Diffie and Hellman won Turing Awards for their work.

To this date, after lecturers and researchers would have conducted research on the topic of Asymmetric Cryptography, they came up with the conclusion that it was James Ellis who deserved the credit for his invention. Whitfield Diffie and Martin Hellman are known to be the pioneers of the Public Key Invention, but James Ellis is the inventor behind the Public Key Encryption.

Asymmetric Cryptography, also known as public key encryption, uses a pair of keys: one for encrypting the message (public key) and the other to decrypt the message (private key). Public Key Encryption was invented to solve the key distribution issue in Symmetric Cryptography. Usually, in symmetric cryptography, one key is used to encrypt the message and to decrypt the message. Public Key cryptography systems rely on cryptographic algorithms based on mathematical problems.

6. Reference

Alderman, R. (2015, December 22). *Cryptology, Cryptography, and Cryptanalysis*. [Web log post]

Retrieved March 9, 2018 from http://mil-embedded.com/guest-blogs/cryptology-cryptography-and-cryptanalysis/

AskHON (n.d.). *What Event started World War 2?*

Retrieved from https://www.historyonthenet.com/what-event-started-world-war-2/

Bombe – Breaking the Enigma cipher. (n.d.)

Retrieved from http://www.cryptomuseum.com/crypto/bombe/

Caesar Cipher. (n.d.).

Retrieved from https://learncryptography.com/classical-encryption/caesar-cipher

IWM Staff (2018, January 5). *How Alana Turing cracked the Enigma Code.*

Retrieved from https://www.iwm.org.uk/history/how-alan-turing-cracked-the-enigma-code

James H. Ellis. (n.d.) In *Wikipedia*.

Retrieved March 15, 2018, from https://en.wikipedia.org/wiki/James_H._Ellis

Levy, S. (1999, April 1). *The Open Secret.*

Retrieved from https://www.wired.com/1999/04/crypto/

Origins of written language / Journey into Information Theory / *Khan Academy*.

Retrieved (8 March 2018) from https://www.khanacademy.org/computing/computer-science/informationtheory/info-theory/v/language-of-coins-2-8-proto-writing

Public key Encryption. (n.d.).

Retrieved from http://www.convolo.co.uk/history.htm

Roeder, T. (n.d.). *Asymmetric-Key Cryptography*.

Retrieved from https://www.cs.cornell.edu/courses/cs5430/2013sp/TL04.asymmetric.html

Rosencrance, L., Pawliw, B. (n.d.). *Cryptanalysis*.

Retrieved from http://searchsecurity.techtarget.com/definition/cryptanalysis

Simmons, G.J (n.d.). *Substitution Cipher.*

Retrieved from https://www.britannica.com/topic/substitution-cipher

Simmons, G.J (n.d.). *Transposition Cipher*.

Retrieved from https://www.britannica.com/topic/transposition-cipher

Singh, S. (2001). *The code book: how to make it, break it, hack it, crack it.* New York: Delacorte Press

The Alternative History of Public-Key Cryptography. (n.d.)

Retrieved from http://cryptome.org/ukpk-alt.htm

The Kuhn Cycle. (2014).

Retrieved from http://www.thwink.org/sustain/glossary/KuhnCycle.htm

Winston, G. (2017, May 14) *Polish Codebreakers cracked Enigma in 1932 – Long Before Alan Turing*.

Retrieved from https://www.warhistoryonline.com/world-war-ii/polish-mathematicians-role-in-cracking-germans-wwii-code-system-xb.html

World War II Cryptography. (n.d.). In *Wikipedia*. Retrieved March 15, 2018, from https://en.wikipedia.org/wiki/World_War_II_cryptography