Jennifer Mead

Math 436 – Math History

Final Paper

May 1, 2017

A Brief History of Cryptosystems Through World War II and the Enigma Machine

Cryptography did not start out as the encryption of messages. In fact, it started out as something little more than message hiding, or steganography, around the fifth century BC (Singh, 1999). Various forms of steganography include hiding the message behind a physical barrier, such as on a piece of wood covered in wax or beneath someone's hair, or with invisible inks. However, with steganography, the message is immediately readable should someone uncover it. Thus, cryptography was born. The purpose of cryptography is to, rather than simply hide the message, scramble it through a process known as encryption such that even if found, the message is unreadable unless the exact decryption key is known (Singh, 1999).

In cryptography, both historically and contemporarily, letters are assigned numbers. Doing so enables us to encode messages using complex mathematical formulas. The following is the typical numbering of the English alphabet:

a	b	c	d	e	f	g	h	i	j	k	l	m
00	01	02	03	04	05	06	07	08	09	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

One of the earliest known forms of cryptography dates all the way back to the time of Julius Caesar around 100 BC (Singh, 1999). This particular cryptosystem is known as the shift cipher. Shift ciphers hold fixed a set of ordered plaintext letters, and shift ciphered letters that are ordered in the same way. The following is an example using a shift of 3 ($\kappa = 3$).

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

This particular shift ($\kappa = 3$) is known as the Caesar shift, as Julius Caesar typically used a shift of 3 when encrypting his messages (Trappe & Washington, 2006). The general encryption function for a shift cipher is:

$$x \rightarrow x + \kappa \ (\text{mod } 26)$$

where κ is the shift |number of ciphered letter - number of plaintext letter|. A variation of the shift cipher is the affine cipher. However, instead of simply shifting the letters in one direction or another, a linear function can be applied. By choosing α and β, where gcd(α,26)=1, the affine function is:

$$x \to \alpha x + \beta \ (\text{mod } 26)$$

Note that when α is 1, this is the same as the shift cipher.

This basic form of cryptography was used up until the sixteenth century, when another more complex variation of the shift cipher was developed. The Vigenère cipher, so named after Blaise de Vigenère, was thought to be a secure version of the shift cipher, and a secure cryptosystem in general, well into the 20th century (Trappe and Washington, 2006). The idea behind the Vigenère cipher is to use different substitution alphabets (it is a polyalphabetic cipher) for each character in a message.

In order to create a Vigenère cipher, a key word needs to be chosen to represent the cycle of shifts that will be used. That is, the same pattern of shifts will be used, but this means that a particular plaintext letter will not always shift to the same ciphered letter, depending on where in the cycle of shifts it falls. For example, if we chose the key word "math", then the cycle of shifts would be 12 00 19 07 and would repeat until the end of the message. Thus, if the index of a character is 1 *mod* 4, then it is shifted by $\kappa=12$. If the index of a character is 2 *mod* 4, then the shift is $\kappa=0$ and so on. For example:

(plaintext)	m	a	t	h	h	i	s	t	o	r	y	r	o	c	k	s
(key)	12	00	19	07	12	00	19	07	12	00	19	07	12	00	19	07
(ciphertext)	Y	A	M	O	T	I	L	A	A	R	R	Y	A	C	D	Z

For a long time, the Vigenère cipher was thought to be secure. However, in the 19th century, Charles Babbage and Friedrich Kasiski developed an attack on this cryptosystem and in the 20th century, William Friedman developed an additional method of attack on this cryptosystem that relied on nothing more than simple letter frequencies (Trappe and Washington, 2006). As with all frequency analysis, the message must be substantially long enough to obtain frequencies that are representative of those that occur in the English language.

A similar but more complex form of the Vigenère cipher was used in developing the Enigma machine that the Germans used during World War II. Shortly after the first world war came to an end, electric coding machines came into being, spurred on by the invention of typewriters. The first version of this "electric coding machine" to use a rotor was patented by Edward Hebern in 1921 (Davies, 1997). A rotor is a disk consisting of "26 electrical contacts in a circle on each side and scrambled connections between them". Hebern's electric coding machine used four of these, producing 26^4 different alphabets. The Enigma machine itself was developed by Arthur Scherbius around 1923 using the same idea as Hebern did in his machine (Davies, 1997).

The Enigma machine was made up of three variable-position rotors, a fixed reflecting rotor and entry drum, as well as a key board, plugboard, and a panel of blubs. Below is a diagram of the Enigma machine (Gaj and Orlowski, 2003). According to Gaj and Orlowski

(2003), the Enigma machine functions by using a polyalphabetic cipher, that is, by changing the substitution settings for each letter of a message according to a key. As we see from the diagram, each time a key is pressed on the keyboard, it goes to the corresponding letter in the plugboard. However, the plugboard consists of connections from the original letter to a different letter, thereby switching the input letter before it goes into the rotors. However, there were only about 10 of these connections, so not all letters were given a substitution in the plugboard. From the plugboard, the new letter goes through a fixed entry drum. Each of the right, middle and left rotors were made up of 26 fixed contacts on one side, and 26 spring-loaded contacts on the other, which were used as the input and output to the next rotor respectively. When the original key was pressed, the right rotor turned 1/26th of a full turn (to the letter listed after the one it was on, these were not necessarily in order). Once the right rotor had completed its turn, the middle rotor rotated 1/26th of a full turn. Once the middle rotor completed its turn, both the middle and left rotors rotated 1/26th of a full turn. Using this method, each letter was encrypted using different rotor settings.

Once a letter has traveled through the right, middle, and left rotors, it goes through a fixed reflecting rotor and back through the left, middle, and right rotors, through the letter on the rotor that is opposite the one that it came in as. Upon exiting the rotors, the new letter goes through the plugboard a second time, again switching this letter. This process has all been completed by using an electrical current through the rotors. Once this current leaves the plugboard with the new letter, it travels to a panel consisting of 26 bulbs to represent each letter. The final letter lights up on this plugboard, giving the ciphered letter. Using this complex process means that letter frequency distributions are nearly uniform across all 26 letters, thereby rendering useless attacks such as the Friedman attack that is based on frequency analysis (Gaj and Orlowski, 2003).

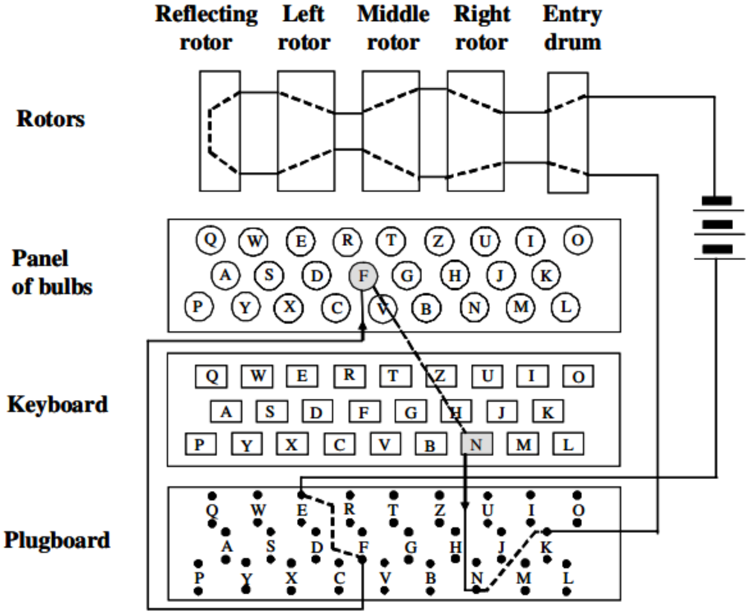

Fig. 1. Functional diagram and the dataflow of the military Enigma.

This machine is clearly similar to the Vigenère cipher in that it uses a key (or in this case the rotor settings) that creates a polyalphabetic cipher. Of course, rather than doing a simple shift for each letter of the message as the Vigenère cipher does, several such substitutions are done. Adding to the security of the Vigenère cipher and Enigma machine is the fact that instead of needing to keep secret an entire codebook of substitutions that were likely to change relatively often, only the key or rotor settings needed to be kept secret.

The Germans began using the Enigma machine several years before the start of World War II. According to Slawo Wesolkowski (2009), the Germans only changed the rotor settings once every three months up until 1935, every month until October of 1936, and then daily from then through the start of World War II until 1943, about two-thirds of the way through the war, at which point they began changing the rotor settings every eight hours.

Due to the obvious complexity of this machine, it is clear why many believed it to be unbreakable. To add to this complexity, the German Navy Enigma used four main rotors, whereas the German Army Enigma used three main rotors (Wesolkowski, 2009). However, contrary to popular history, and the portrayal of the breaking of the Enigma machine by the movie, The Imitation Game, Alan Turing and the British were not the first to crack the Enigma machine. The first to crack the Enigma machine were the Polish.

Marian Rejewski, Henryk Zygalski, and Jerzy Rozycki began working for the Polish Cipher Bureau in 1932. They were recruited through a cryptography course offered at the University of Poznań in 1929 where they were given real German cipher messages to solve. The Cipher Bureau had begun collecting these messages in 1928 (Wesolkowski, 2009).

Rejewski left the university before the course was finished to attend the University of Göttingen, but upon his return in 1930, he joined the other two decrypting German messages at the University of Poznań. This post was closed in 1932 upon the discovery of a German cipher that could not be broken, at which time the three began working for the Polish Cipher Bureau. It was then that the Germans had begun to use the Enigma machine. While Rejewski had determined equations that would allow him to crack Enigma, he could not solve these without knowing the internal wiring of the military Enigma (as opposed to the commercial version) (Wesolkowski, 2009). Recall, that at this point, the Germans were only changing the Enigma machine's settings once every three months.

According to Wesolkowski (2009), after having obtained a schematic to the inner workings of the Enigma machine from the French, and making the stunning realization that the letters on the rings were listed in alphabetical order, the Poles were able to reconstruct a version of the military Enigma machine. They also discovered that the reflecting rotor did not allow letters to be ciphered as themselves, which eliminated a vast number of possible rotor settings. However, at this point, the Germans began to change their rotor settings daily, in addition to making several modifications to Enigma such as adding a fourth and fifth rotor, and increasing the number of connections in the plugboard.

It was soon after in 1939 that the Poles began to collaborate with the French and British governments, and history as many now know it, began to play out. What is rarely mentioned is the early contributions to breaking the Enigma machine by the Polish, and how many of the ideas that Alan Turning and the cryptologists at Bletchley Park were largely based on the technological methods that the Poles had used. While it is the British who are often lauded for cracking the Enigma machine, shortening the war by many years, and lowering the death count, and while their accomplishments are by no means trivial, their work would not have been possible if not for the initial Polish contributions towards breaking the Enigma machine.

Cryptography has long since moved past many of these basic cryptosystems, and even more complex cryptosystems such as Enigma due to the introduction of computers. Many cryptosystems today use public key, zero-knowledge, digital, and even quantum techniques to encrypt and decrypt messages, making it virtually impossible for outside listeners to break these codes, at least for now. Of course, once technology has advanced to the point where we have created quantum computers, many of these techniques we use today will become breakable and will have played their role in the evolution of cryptography.

References

Davies, D. (1997). A Brief History of Cryptography. *Information Security Technical Report*, *2*(2), 14–17. http://doi.org/10.1016/S1363-4127(97)81323-4

Gaj, K., & Orlowski, A. (2003). Facts and Myths of Enigma: Breaking Stereotypes. In *Advances in Cryptology-Eurocrypt 2003* (Vol. 2656, pp. 106–122). http://doi.org/10.1007/3-540-39200-9_7

Singh, S. (1999). The Code Book: The Evolution of Secrecy from May, Queen of Scots to Quantum Cryptography. New York, NY: Doubleday.

Trappe, W., & Washington, L. C. (2006). Introduction to Cryptography: with Coding Theory (2nd ed.). Upper Saddle River, NJ: Pearson Education.

Wesolkowski, S. (2009). The Invention of Enigma and How the Polish Broke It Before the Start of WWII.