John Hunt

Professor Derek Bruff

FYWS Cryptography

28 October 2010

Most people familiar with codes and cryptography have at least heard of the German Enigma Machines. However, very few people have heard of the Lorenz Cipher Machine. The Lorenz Schlüsselzusatz 43, also known as the Lorenz SZ 43, was the successor of the enigma machines and was used throughout World War II by the Hitler and his commanding officers. The SZ 43 is notable not only for the advancements that it created in the field of cryptography but also the advancements made by cryptanalysis in order to counter the innovation, specifically the invention of Colossus, the predecessor of the modern computer.

The German Enigma machines offered the strongest form of encryption available to the Germans for quite a while. Unfortunately those machines had their flaws, namely the difficulty and amount of time needed to send a message. When an enigma machine was used one person would type the message in plaintext, for each letter struck, a different letter of cipher text would be flashed on a bulb and an assistant would record whatever letter appeared in the ciphertext. Then a radio operator would take the encrypted message and, using Morse code, send the message to the receiver. The entire process would then have to be reversed in order for the original message to be read (Copeland 36). This process required six people and obviously took a substantial amount of time to do. The SZ 43 simplified the process by requiring only one person to type in the original message. The machine would then automatically encrypt the message and send the encryption to the intended recipient (Kippenhahn 203). Upon arrival, the receiving machine would decrypt the message and print out the original (Kippenhahn 201).

While the SZ 43 had rotors and wheels like the Enigma, the two machines operated in entirely different ways. The enigma had six wheels, each of which lead to a different letter ("The Machines"). Whereas the SZ 43 had twelve wheels, two motor wheels, five chi wheels, and five psi wheels. Each wheel had a different number of pins with which to poke holes into a piece of tape. The pins could either be up or down so that the settings of the wheels could be changed. This meant that the wheels could be changed significantly more frequently on the Enigma where an electrician was needed in order to move all of the wires around (Tutte). The ten psi and chi wheels worked together to create one key letter, while the motor wheels worked together to determine when the psi wheels moved. The chi wheels would all turn every time a letter was pushed. The psi wheel would move when the pin on the first motor wheel was up, the first motor wheel would move when the pin on the second motor wheel was up, the second motor wheel would move with the chi wheels. (Copeland 47)

The innovation that made this new form of encryption possible was the Vernam method. Named after the man who created it, the Vernam method assigned each letter with five characters, either a dot or a cross. For example a "T" was represented by "●●●●+" and an "S" was represented by "+●+●●●". According to the Vernam method one of the letters would be the key and the other would be user inputted. The other two letters would then be added together so that two of the same yielded a cross but if the letters would different they would be represented by a dot. So + + = +, ● ● = +, + ● = ●, and ● +=●, so using this principle the two letters would be added together to create a new letter. For example "T" plus "S" would yield

+ ● = ● , ● ●= + , +●=● , ●●=+ , +●=● , this gives us ●+ ●+● which corresponds to the letter "R". Therefore T+S=R. (Kippenhahn 202)

The Lorenz took the Vernam method a step further by adding another letter into the equation. When the pin was up on one of the wheels it would poke a hole in the tape running through the machine, this would register as a cross in the Vernam method, when the pin was down no hole was made and this would be represented as a dot in the Vernam method (Copeland 38). So the five chi wheels would create one series of dots and crosses, while the five psi wheels would create another series of dots and crosses. These two series would both represent a different letter. Those two letters were added creating a key letter, and then the inputted letter would be added to the key letter creating the cipher letter. It was a fairly complicated process. However, to unscramble all one would have to do is know what the key letter created by the psi's and the chi's was (Copeland 48). The genius of the method used by Vernam is that no matter which order the characters are read in, they produce the same thing. So there were no difficult calculations to be done, all one had to do was subtract the ciphertext letter from the key letter, and the plaintext letter is once again revealed (Kippenhahn 202). This method also allowed the plain text to appear in the form of dots and spaces so that it was easily readable by the receiving machine, and transmitted via radio waves without the need of Morse code.

Because the SZ 43 has about $4x10^{131}$ different possible sequences the Germans decided that it was the closest possible code to unbreakable (Hinsley 153) and therefore it could be used amongst the most prominent officials in the military, it was in fact the encryption device used by Adolf Hitler to communicate with his commanding officers. The men and women at Bletchley Park immediately recognized the significance of these encryptions. If one would be able to decipher what the most prominent military minds in Germany were planning then one would have an immensely strong grasp on the condition and plans of the German military as a whole (Hinsley 167) For several months it appeared as if the code would prove to be unbreakable. There were glimpses of hope mainly in the first twelve letters of every encryption. The cryptanalysts noticed that sometimes the same letters repeated themselves in the first twelve letters of each encryption. This was called a having a depth of two. (Copeland 50). Unfortunately, while it became apparent that the first twelve letters were significant, no one at Bletchley Park knew what the SZ 43 looked like so it was really no help. (Copeland 56)

Britain's big break came when a German officer made a lazy mistake that essentially handed the British the answer to the inner workings of the machine. One officer tried to send an encrypted message, comprised of roughly four thousand words to another. Unfortunately for the Germans the receiving officer didn't receive the entire message so he sent back a message in plaintext asking for the initial officer to resend the message. Then the initial officer broke protocol and sent the message over using the same wheel settings. The crew at Bletchley had picked up on the request to resend, and picked up both messages. Both messages started with the same twelve letters so it was safe to assume that they had both been encrypted with the same wheel settings, and the nail in the coffin for the German machine was that the officer had made a few slight changes in wording and abbreviating but had otherwise kept the text the same. (Copeland 56) These mistakes were enough to give British cryptanalyst John Tiltman enough of a crib to not only read both messages, but to infer what the design of the machine was. (Copeland 57). Soon after the crib was found, the British built their own Lorenz which they called "Tunny" (Hinsley 161)

As quickly as the success came for the British it was lost just as fast. Only a few months after Tiltman's breakthrough, the Germans realized that having the wheel settings be represented by the first twelve numbers of the code was a severe breach of security so, instead of the twelve significant characters, one three digit number started out the beginning of every message, which corresponded to settings laid forth in a code book. (Copeland 58)

If it hadn't been for Bill Tutte's intervention, all of the work done thus far by John Tiltman would have been done in vain. Luckily for the British, Tutte recognized a pattern that played on the fact that the psi wheels moved less frequently than the chi wheels. By shifting the ciphertext over and computing some advanced mathematics Tutte was able to recognize that he could get a rough interpretation of what the chi wheel was generating. (Copeland 58). However, even with this method it was still too much for any human, or team of humans, to work out by hand. It was then that Dr. Max Newman was assigned to create a machine that would be able to test the multiple different possibilities, he called this machine Colossus. (Copeland 59)

Colossus is now considered the predecessor of all computers, primarily created by Max Newman and Tommy Flowers. The processing machine was created in order to counter the new complications brought on by the Tunny machine. (Copeland 74) "Colossus could read paper tape at 5,000 characters per second and the paper tape in its wheels travelled at 30 miles per hour". ("The Machines") Colossus was able to do in hours what it once took teams weeks to do. The machine was effectively built entirely by Flowers. It was Newman's idea to bring Flowers in, but his plan of using electricity seemed too farfetched for Newman, so Newman gave Flowers free reign to do whatever he wanted in the creation of Colossus. The rest of Newman's team worked on the machine they called Heath Robinson. Colossus was created late in 1943 and everyone at

Bletchley was in awe of the power that Colossus exhumed. It was faster and more accurate than not only humans, but all of the machines that Newman and his team had created. (Copeland 74)

By the end of the war there were ten Colossi in Bletchley Park, all capable of deciphering messages sent by the Lorenz machine, even though no one in England had ever seen one. The cracking of the Lorenz was a huge feat in cryptanalysis and was a devastating blow to German security. The Germans had created a code that was unbreakable, and yet, because of one officer's mistake the code was broken.

Works Cited

Copeland, B. Jack. *Colossus: the Secrets of Bletchley Park's Codebreaking Computers*. Oxford: Oxford UP, 2006. Print.

Hinsley, F. H., and Alan Stripp. *Codebreakers: the inside Story of Bletchley Park*. Oxford: Oxford UP, 1993. Print.

Kippenhahn, Rudolf. *Code Breaking: a History and Exploration*. Woodstock, NY: Overlook, 1999. Print.

"The Machines." *Bletchley Park*. Web. 28 Oct. 2010. <http://www.bletchleypark.org.uk/content/machines.rhtm>.

Tutte, W. T. "FISH and I." Lecture. University of Waterloo, Waterloo. 19 June 1998. *FISH and I*. Web. 28 Oct. 2010. <http://frode.home.cern.ch/frode/crypto/tutte.pdf>.