Cryptology, the Secret Battlefield of World War I:

Dawn of the Crypto Arms Race

Ralph Simpson

World War I was the first war in which the new invention of the radio played a starring role. The radio gave battlefield commanders more timely military intelligence and the ability to execute a coordinated war strategy, with direct control of their army, navy, and air force. But use of radio also meant all military messages were easily intercepted by the enemy. Unfortunately, the cipher technology of the time did not keep pace with the rapid adoption of radio, so the secret messages of every country were broken!

This failure to secure radio messages had a huge impact on the progression of the war and was directly responsible for the outcome of some of the major battles. Also, the British decryption of the German ambassador's telegram to Mexico, called the Zimmermann telegram, was the impetus for the US entry into the war. So at the time of WWI, the code breakers had the upper hand in the burgeoning field that would later be called the crypto arms race.

The main cipher technologies used at the beginning of WWI were the Vigenère disk, code books, and various manual methods of transposition ciphers. All of these ciphers were hundreds of years old and were susceptible to being broken, especially when dozens or hundreds of messages are sent each day, using the same key. These manual ciphers were also very slow, tedious to use, and error-prone in battlefield conditions.

In the final years of WWI, four inventors from four countries invented the electric rotor cipher, of which the Enigma machine was the most infamous. This represents the first machine cipher, which was also the first time electricity was used to encipher a message. The teletype one-time tape cipher was also invented, which provided automatic and instant encryption and decryption, without human intervention. The NSA would later call the invention of the one-time tape cipher, "perhaps one of the most important in the history of cryptography."

Other new cipher technologies in WWI included the use of Native American languages, presaging the later use of the Navajo code talkers in WW2. The invention of burst encoders gave the capability to rapidly send Morse code signals so that anyone intercepting the message would not be able to distinguish the dots and dashes, or have time to locate the enemy by radio direction finding. The cipher wheel was also invented just prior to WWI.

Most of these new cipher inventions came too late to be of much use during WWI, but the resulting technological explosion propelled a worldwide crypto arms race. This arms race would go on to have a major influence on world history, especially in WW2 and the beginning of the computer revolution. That influence extends to the events occurring today, with the surveillance and cyber attacks that continue to shape world events today.

Cipher Technologies Used in WWI

The Vigenère disk, code books, and various methods of transposition ciphers were the most widely used ciphers of WWI. All of these cipher methods were many hundreds of years old and had known solutions.

The Vigenère disk consists of 2 rings of the alphabet that spin on a central axis. This cipher disk was named for Blaise de Vigenère, even though it was invented in 1467 by Leon Battista Alberti, 56 years before Vigenère was born! This was the beginning of a long tradition of cipher devices being credited to the wrong inventor.

Because of the secrecy surrounding cipher technology, many inventions are not made public and then are named for a later inventor. This has been the case, for example, with the infamous German Enigma machine, the Jefferson Cypher Wheel, the one-time pad, the Playfair Cipher, the Wheatstone Cipher, and even modern public key encryption.

Vigenere disk, invented in 1467

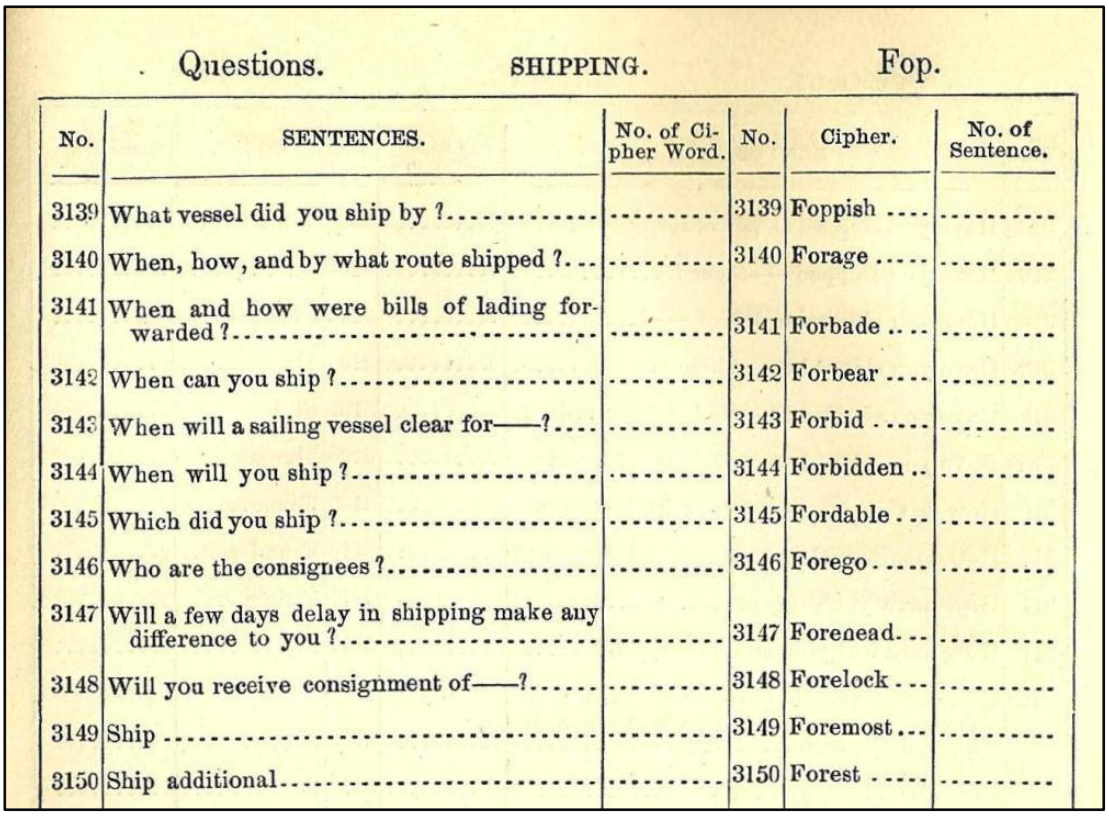
Leon Battista Alberti

Alberti proclaimed his cipher disk to be unbreakable and "worthy of kings." This is another tradition in cryptology, claiming a cipher invention to be unbreakable, only to be proven wrong at a later date. In 1917, exactly 450 years after its invention, the Vigenère cipher was declared to be unbreakable by *Scientific American* magazine. Apparently, *Scientific American* was not aware of the published solution to the Vigenère cipher, written by a German military officer, Friedrich Kasiski, in 1863.

To use the Vigenère cipher disk, the user would successively align the "A" on the outer disk with each of the letters of a keyword on the inner disk. After spinning the disk for each letter of the keyword, he would find each letter of his message on the outer disk and then select the letter from the inner disk aligned with that letter to be the encrypted letter. For longer messages, the keyword is repeated as often as needed. It is, in fact, this repetition of the keyword that makes this cipher vulnerable. Also, by finding several messages with the same keyword, the enemy can easily break the cipher using letter frequency analysis.

Code books were in common use in WWI, which is another technology used for over 500 years. Code books can successfully be used when the number of messages and users are kept to a minimum. The

widespread use of code books in times of war exposes the books to capture or compromise without the user aware of the breech in security. In times of war, printing and distributing new code books can be very dangerous and time-consuming. The Zimmermann telegram, which was deciphered by the British code breakers, used a code book. This gave proof of German war intentions that forced the US to enter the war.



Questions. SHIPPING. Fop.

No.	SENTENCES.	No. of Cipher Word.	No.	Cipher.	No. of Sentence.
3139	What vessel did you ship by ?		3139	Foppish	
3140	When, how, and by what route shipped ?		3140	Forage	
3141	When and how were bills of lading forwarded ?		3141	Forbade	
3142	When can you ship ?		3142	Forbear	
3143	When will a sailing vessel clear for——?		3143	Forbid	
3144	When will you ship ?		3144	Forbidden	
3145	Which did you ship ?		3145	Fordable	
3146	Who are the consignees ?		3146	Forego	
3147	Will a few days delay in shipping make any difference to you ?		3147	Forenead	
3148	Will you receive consignment of——?		3148	Forelock	
3149	Ship		3149	Foremost	
3150	Ship additional		3150	Forest	

Code book published in 1888

Various transposition ciphers were also used in WWI. These ciphers are very manual and error-prone. Unfortunately, they are also among the easiest ciphers to break, so these ciphers provided added reason to pursue newer technology to encrypt radio messages.

One of the more sophisticated battlefield ciphers in WWI is the Playfair cipher, which is a diagraphic cipher. This means that the encipherment is performed on pairs of letters instead of one letter at a time. The advantage is that frequently used letters are thus hidden from decryption using letter frequency analysis. For instance “TE” may encipher to “HN” and “TH” may encipher to “JZ”, so the frequently used letter “T” is coded into two different letters.

The Playfair cipher can still be broken by using frequency analysis on pairs of letters, but there are 600 pairs of letters to analyze instead of the 26 letters of the alphabet. A book was written in 1914 by Lt. Joseph O. Maubourgne of the US Army on the method to decrypt the Playfair cipher. This was the first book published by the US military on cryptology. Mauborgne would go on to fame as the US Chief Signals Officer and a Major General.

Another cipher technology used in WWI was the burst encoder. The Germans used the new invention of the magnetic wire recorder in their submarines to record Morse coded messages, which were sent via radio at high speed. The receiver would record the message and play it back at a slower speed in order to read the message. In fact, the German submarine attack on the Lusitania was ordered by the German command by sending such a burst message to the German submarine, which simply said, "Get Lucy!"

New Cipher Technologies Invented during WWI

Because of the obvious need for a more robust cipher technology which could withstand the demands of war, the race was on to develop that new technology. In a two year period, from 1917-1919, four inventors from four countries would invent the electric rotor cipher. The most famous of these inventions was the German Enigma machine, thought to be invented by Arthur Scherbius in 1918.

In 2003, it was discovered that the electric rotor cipher machine was actually invented prior to the four inventions mentioned above. In 1915, two Dutch naval officers, Theo van Hengel and Rudolf Spengler came up with the idea while working in the Dutch East Indies. They built a prototype in the summer of 1915 but the Dutch navy decided not to adopt the cipher. Hengel and Spengler tried to patent the device but were prohibited by the Dutch navy from publicizing their invention for fear of this technology being used by the enemy. The patent attorney they hired was the brother-in-law of one of the other 4 electric rotor inventors, Hugo Koch of the Netherlands, who gave this information to Arthur Scherbius! Now Hengel and Spengler are recognized as the original inventors of the Enigma machine.

German Enigma machine

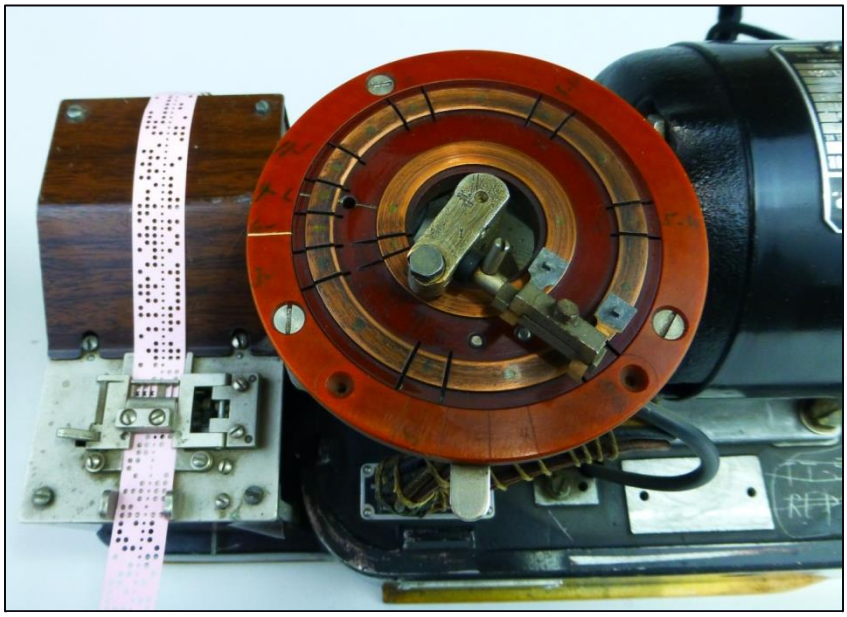
So, deception and intrigue surrounded the Enigma machine invention, even before it was patented and manufactured. This was the first electric, machine cipher and breaking this cipher required ingenuity and determination for several decades in order to be able to decode these messages in WW2.

A US inventor, Edward Hebern, was another of the inventors of the electric rotor cipher. The US Navy bought several of these machines just after WWI and tried to convince the US Army to adopt this same technology so they could exchange messages. The US Army premier code breaker, William F. Freedman, was able to break the Hebern because of its use of odometer-style rotor movements. This was the same rotor movements used in the

Enigma, so Freedman invented a more complex cipher called the SIGABA, which had irregular rotor movements. The SIGABA was used in WW2 and was never broken by the enemy. The US military did not tell Hebern why they did not adopt his cipher machine and he went out of business after manufacturing only about 100 machines.

Another brand new technology invented during WWI was the one-time tape teletype system. This was invented in 1917 by Gilbert S. Vernam, an engineer at Bell Telephone Laboratories. He invented a teletype-based cipher system in which a reel of perforated paper tape representing random letters was added to a plaintext message to create the ciphertext. On the receiving end, a duplicate reel of random letters was used to subtract from the ciphertext to re-create the plaintext message. The elegance of this system was the encipherment and decipherment was handled automatically by the teletype system without human intervention, delay, or error.

Vernam was awarded US Patent #1,310,719 in 1919 for a "Secret Signaling System", which describes this automated teletype cipher. Many other cipher inventors have claimed their inventions were unbreakable, but the invincibility of the one-time pad has the advantage of being mathematically provable. It is also mathematically provable that ANY unbreakable cipher system must include the features of a random and non-reused key which is as long as the message. Claude Shannon proved the one-time pad was unbreakable during WW2, saying it has the property of perfect secrecy. His results were published in a seminal article in the *Bell Labs Technical Journal* in 1949.



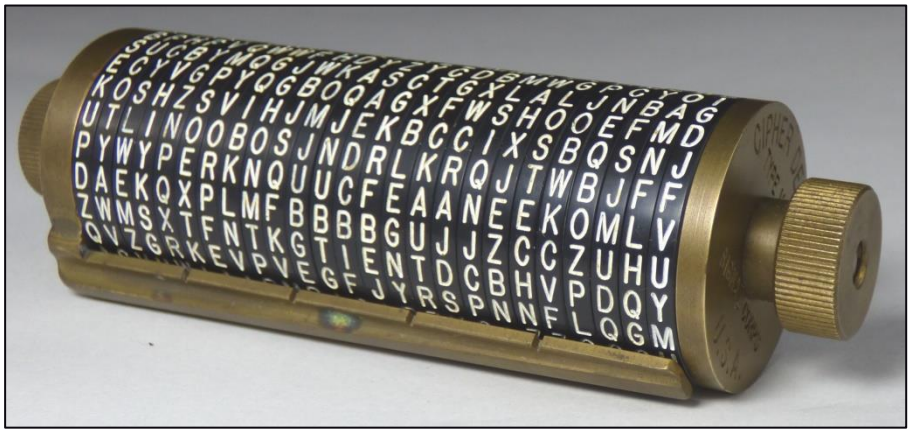
US SIGTOT one-time tape cipher - invented in 1917

The Vernam patent was first introduced in the teletype machine. A plaintext message is punched on tape and a second tape of random letters is added by the Boolean "exclusive or" function. This is an elegant solution since the enciphering and deciphering logic is identical and performed in the electro-mechanical relays. This one-time tape system is automatic, without human intervention or delay, and has the benefit of being a perfect cipher. The reason it was not more widely used was because of the cumbersome distribution and destruction of the reels of random letters required.

Another invention just before WWI was the cipher wheel, invented by French Lt. Etienne Bazeries in 1891 and then independently by US Army Lt. Parker Hitt in 1912. Neither inventor realized that the original inventor of this technology was our third president, Thomas Jefferson, who invented this in c.1795! He called his invention the Wheel Cypher and the only remaining example is in the NSA museum in Ft. Meade, Maryland.

Parker Hitt transformed his cipher wheel into a tablet form with sliding strips of the mixed alphabet to

replace the wheels. Joseph Mauborgne pursued the wheel version, which likely saw limited use by the military attachés in WWI. It was finally officially accepted into the military in 1922 and was used until 1943. The only known prototype of this wheel is shown below, from the author's collection.

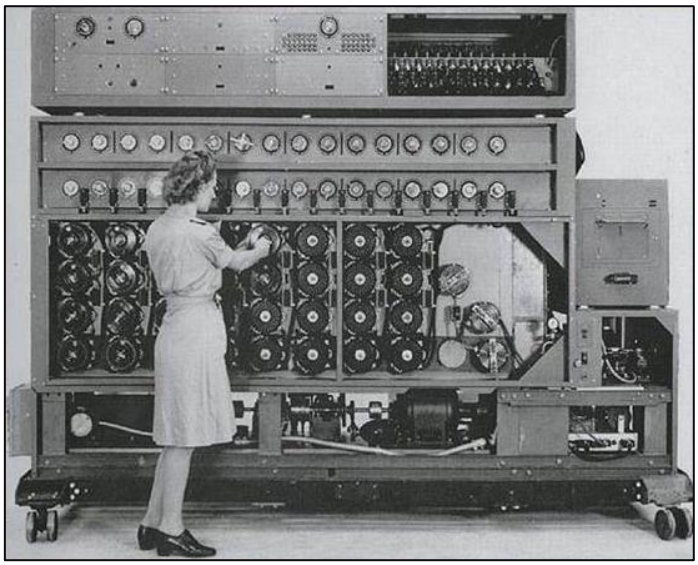


US M-94 prototype cipher wheel from 1917

The use of Native American Indian languages was first used in WWI, but on a very limited basis. This was greatly expanded in WW2 when 400 Navajo Indians were deployed in the Pacific theater to quickly send and receive messages in a mixture of Navajo language and code words. The Japanese were never able to decipher the Navajo messages, despite capturing a non-code talker Navajo Indian.

The Genesis of Crypto Wars

The explosion of new cipher technology during WWI was the cause of another explosion, the technology to break these new cipher methods. The new cipher machines required a machine in order to break the code. The old method of using linguists and crossword puzzle enthusiasts would no longer work. Mathematics and number theory was the new requirements to break these cipher technologies.



US Navy Bombe

The Polish and later UK and US bombes, built to break the German Enigma machines, were electro-mechanical computers. The strength of the Enigma, before considering the use of Bombes, was formidable and considered unbreakable by the Germans. The investment in resources required to break the Enigma was beyond the comprehension of the times. For instance, in order to break the Enigma machine, assuming you captured a machine and knew all the wiring of the machine and each rotor can be described in an example.

If you have 100,000 Enigma machines, each with an operator capable of testing out a new setting every second, 24X7, it would take twice the age of the universe to break the code! The Germans changed the settings every day and used many different settings for the different networks of users.

Prior to WWI, the only cipher technologies used were in place for hundreds of years. So the disproportionate advantage enjoyed by the codebreakers during WWI was the impetus to generate many new and innovative cipher technologies during WWI. Those new technologies ignited a crypto war after WWI for the first time in history. The result of that crypto war was the computer and information revolution, which is continuing to this day.