Chapter 5
Crypto and the War to End All Wars: 1914–1918

Abstract The use of wireless telegraphy—radio—during World War I marked the advent of modern cryptology. For the first time, commanders were sending enciphered messages to front line troops and for the first time, the enemy had an enormous amount of ciphertext to work with. This spurred the development of more complicated codes and ciphers and eventually led to the development of machine cryptography. World War I is the first time that the Americans had a formal cryptanalytic organization. It is the beginning, in all the nations involved in the conflict, of the bureaucracy of secrecy. In the United States it marks the first appearance of the two founding fathers of modern American cryptology, Herbert O. Yardley and William F. Friedman. This chapter introduces Herbert Yardley and William Friedman and examines some of the cryptographic systems used during World War I.

5.1 The Americans Start from Behind

At the beginning of the 20th century there was no organized cryptologic effort in either of the military services of the United States—and there never had been. In all the conflicts in which the United States had been involved since it's founding, it had always had the occasional code, cipher, and cryptanalyst. And they had all been strictly ad hoc. In particular there had never been an official cryptanalytic organization in either the Army or the Navy. This was in sharp contrast to the Black Chambers of the European powers, which had been in existence since at least the 16th century.

The first real American cryptanalytic effort began in 1911 at the Army Signal School in Fort Leavenworth, Kansas. It was there that a few Army officers received initial training in cryptanalysis at a series of technical workshops. The students included Lt. Joseph Mauborgne who would one day head the Signal Corps and who, in 1914 published the first systematic solution of the Playfair cipher. Also trained at Leavenworth was Captain Parker Hitt who went on to write,

J. F. Dooley, *A Brief History of Cryptology and Cryptographic Algorithms*,
SpringerBriefs in Computer Science, DOI: 10.1007/978-3-319-01628-3_5,

in 1916, *Manual for the Solution of Military Ciphers* that was to be the handbook for Army cryptanalysts for nearly a generation.

At America's entry into World War I in 1917, these two officers constituted about half of the trained cryptanalysts in the American military.

5.2 America Catches Up

In April 1917 Herbert O. Yardley (1889–1958) was 28 years old, a code clerk for the State Department in Washington, D.C. ambitious, and bored silly. Yardley had been with the State Department since 1912 and had pulled too many night shifts, waiting for diplomatic telegrams to come across his desk for encryption and decryption. At one point he decided to while away some time by trying to decode the personal correspondence between President Woodrow Wilson and his close aide Colonel House. Much to Yardley's surprise, it took him just a few hours to break the cryptosystem that Wilson and House were using [7]. Fascinated by the work of cryptology and appalled by how insecure many of the State Department cryptosystems were Yardley spent several months producing a 100-odd-page memorandum on the codes and ciphers then in use at State. Once war was declared, Yardley set about trying to get the Army to put him in charge of a cryptanalytic bureau. He finally convinced Major Ralph Van Deman of Military Intelligence and in June 1917 Yardley was commissioned a second lieutenant and placed in charge of Military Intelligence, Section 8—MI-8—the new cryptologic section—and the first official one the Army had ever created. What Yardley lacked in real cryptanalytic experience he made up for in energy and in innate organizational ability. Before the year was out MI-8 grew from Yardley and one clerk to six sub-sections, Instruction, Communications, Code and Cipher Compilation, Shorthand, Secret Inks, and Code and Cipher Solution and by the end of the war had 165 personnel. Yardley's second-in-command was Dr. (later Captain) John M. Manly, head of the English Department at the University of Chicago. Manly started in MI-8 as the chief of the Instruction section, but later became Yardley's best cryptanalyst. Manly brought with him several colleagues from Chicago including Dr. Edith Rickert, with whom Manly would write several textbooks and spend 14 years after the war creating the definitive set of volumes on Chaucer's *Canterbury Tales*.

MI-8 solved cryptograms from a number of nations, but focused its attentions on Germany, Mexico, and later, Japan. The high point of MI-8's cryptanalysis during the war was the case of the German spy, Pablo Waberski. Yardley tells the tale, suitably embellished, in his best-selling and controversial tell-all book, *The American Black Chamber* [7]. Waberski was arrested crossing the U.S.-Mexico border in January 1918. In Waberski's luggage was found a letter in cipher, which was forwarded on to MI-8 in Washington. After several MI-8 cryptanalysts failed to solve the cryptogram, Manly began working on it with Dr. Rickert assisting him. The accounts vary, but either after a brief two-days or a long several weeks Manly broke the cryptogram, which was a variation of a route transposition

cipher. The message itself was a letter of introduction that plainly named Waberski as a German spy and laid out the sabotage that he was to attempt while in the United States. In August 1918, Yardley and Manly traveled to Fort Sam Houston in San Antonio, Texas where Manly testified on the exact nature of his cryptanalysis and the contents of the cryptogram. Waberski was convicted and sentenced to death; the only German spy given the death sentence during World War I. In the end, President Wilson commuted Waberski's sentence and he was released and sent back to Germany in 1923 [7].

Yardley was sent to England and France in August 1918 to establish closer relations with the cryptologic organizations there, leaving Manly in charge of MI-8. The English were very reticent about sharing anything with Yardley, and he was never given entrance into Room 40, the main Admiralty cryptologic organization (and the group that deciphered the Zimmermann Telegram that helped bring the United States into the war). The French were more cordial and Yardley met many of the cryptanalysts in their organization including Georges Painvin, the best French cryptanalyst of the war. The French, however, would not talk to Yardley about diplomatic codes and ciphers. After the Armistice, Yardley, now a major, was ordered to head the cryptologic section of the American delegation to the Versailles Peace Conference, and did not return to the United States until April 1919 at which point most of MI-8 had already been demobilized as the Army prepared for peace [3, pp. 354–355].

5.3 The A.E.F in France

While MI-8 in Washington focused on more strategic and diplomatic cryptologic systems, the American Expeditionary Force in France had it's own cryptologic organization that focused on tactical codes and ciphers. In the summer of 1917 as American forces were beginning to arrive in France, the cryptologic functions of the American Army were divided between Military Intelligence and the Army Signal Corps. The Radio Intelligence Section of Military Intelligence, designated as G.2 A.6 was organized under Major (later Colonel) Frank Moorman, one of the few Army officers trained in cryptanalysis. G.2 A.6 was primarily charged with code and cipher cryptanalysis, but also had sub-sections for traffic analysis, enemy telephone interception (via wiretaps), and monitoring of American communications to ensure security rules were followed. The Signal Corps had two sections devoted to codes and ciphers: the Code Compilation Section under Captain Howard Barnes, [3, p. 326] and the radio interception section that grabbed German cryptograms out of the air and passed them on to G.2 A.6. These organizations mirrored in many ways the cryptologic organizations of the British and French.

Many of the cryptologic personnel in France were trained by Yardley's organization in Washington and then shipped to American headquarters in Chaumont, to become either part of the Signal Corps, or Military Intelligence, section G.2 A.6. Among the cryptanalysts assigned to G.2 A.6 was Lieutenant William F.

Friedman, who arrived in France in July 1918. Friedman had trained cryptanalysts early in the war at Riverbank Laboratories before Yardley's organization was set up. Friedman was assigned at his own request to the code cryptanalytic section and spent the remaining five months of the war deciphering German *Satzbuch* and *Schlüsselheft* code messages. The Germans and the Allies both had decided that ciphers were too difficult to use near the front lines and so had reverted to 1-part and 2-part codes with anywhere from 800, to about 2,000 code groups for these *trench codes*. The Satzbuch codes were changed once a month and so the Americans had to break the codes quickly in order to be able to gain intelligence from the German secret messages. Friedman gained much experience with codes, something he had not had before, and went on to write the official monograph on *Field Codes Used by the German Army during the World War*, and also the history of the Code and Cipher Solving branch of G.2 A.6 [2, p. 69].

One of the first assignments of the Code Compilation Section of the Signal Corps was to create a trench code for the American Army. Barnes' organization had no experience with creating these types of codes, so they began with an obsolete British trench code and modified it for the American sector of the Western Front. The result was the American Trench Code of 1,600 codewords. It was a 1-part code and was designed to be *superenciphered*—the code message was enciphered using a monoalphabetic cipher—before any messages were sent. Because the Americans had no experience with this type of code before, Parker Hitt, then the chief of the Signal Corps for the A.E.F asked Lt. J. Rives Childs to see if he could recover the encipherment alphabet. If Childs could undo the superencipherment it would severely weaken the code. Childs sat down with 44 relatively short superenciphered messages in the American Trench Code and within 5 h had recovered the entire cipher alphabet.

Barnes scrapped the American Trench Code and proceeded to create one of the best series of trench codes in the war. The so-called *River Series* trench codes—all were named after American rivers—were 2-part codes with about 1,800 code words, nulls, and specific codewords for tactical use. The first code, *Potomac*, was released 24 June 1918 and Barnes' organization released a new code on the average of every two weeks for the rest of the war. In October, when the American 2nd Army was formed, a new series, the *Lake Series*, was begun and those codes were issued at the same rate as the River Series codes [3, p. 327].

5.4 Ciphers in the Great War: The Playfair

While all the combatants in World War I reverted to trench codes for much of their tactical communications, ciphers were not totally forgotten. In particular, the British used a field cipher as their tactical communications system for at least the first two years of the war, and the Germans used a complex field cipher for their high-level communications till the end of the war.

Sir Charles Wheatstone, the physicist, mathematician, and engineer, invented the British system, known as the Playfair cipher, in 1854. It acquired its name from Baron Lyon Playfair, who spent years popularizing the cipher and attempting to get the British government to adopt it. The British Army finally adopted the Playfair in the 1890s as their field cipher. It saw its first use during the Boer War (1899–1902) and was still used as the field cipher down to the company level during the first years of World War I [3, pp. 198–202, 1, pp. 166–178].

The Playfair cipher is a *digraphic substitution cipher* that encrypts two letters at a time. Every plaintext digraph is encrypted into a ciphertext digraph. It is based on a five by five Polybius square that uses a keyword to map 25 of the 26 letters of the Latin alphabet (I and J are either mapped together in a single cell, or J is just dropped). The keyword is dropped in row-by-row, deleting any repeated letters, and then the rest of the alphabet is filled into complete the square. For example, if the keyword is MONARCHY, then the Playfair square looks like Fig. 5.1.

Messages are enciphered according to the following rules:

1. The plaintext message is broken up into two-letter groups. Any double letters (like SS or LL) are broken up by inserting a null letter (like Q or X or Z) between the repeated letters. If the message has an odd number of letters, just add a null to the end.
2. Each two-letter group is enciphered separately.
3. If the two letters in a group are in the same row, then the group is enciphered by taking the letter immediately to the right of each letter in the group. So if the square in Fig. 5.1 is used and the plaintext pair is HY, then the ciphertext is YB. If you run off the right side of the square, just loop around to the beginning of the row.
4. If the two letters in a group are in the same column, then the group is enciphered by taking the letter immediately below each letter in the group. So in Fig. 5.1, if our plaintext is CL, then the ciphertext is EU. If you run off the bottom of the square, just loop around to the top of the column.
5. If the two letters are in different rows and columns then you "complete the rectangle" by first going across the row where the first letter is, to the column that contains the second letter and using the letter you find at the intersection as the cipher letter. Do the same thing for the second letter. So in Fig. 5.1 if our plaintext is MG, then the ciphertext is NE, in that order [6].

Deciphering is just the inverse of enciphering.

Say we want to send the message *flee, all is discovered* using a Playfair cipher with the keyword FRIEDMAN. Then the Playfair square will look like Fig. 5.2.

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Fig. 5.1 Example of a Playfair cipher square

F	R	I	E	D
M	A	N	B	C
G	H	K	L	O
P	Q	S	T	U
V	W	X	Y	Z

Fig. 5.2 Playfair square using the keyword FRIEDMAN

Then the first thing we do is divide up our plaintext into digraphs, making sure to break up any repeated letters with nulls

```
FL EX EA LX LI SD IS CO VE RE DX
```

We now use the rules above to encrypt each digraph separately

```
Plain:  FL EX EA LX LI SD IS CO VE RE DX
Cipher: EG IY RB KY KE UI NX OU YF ID IZ
```

And finally we break the ciphertext up into five-letter blocks for transmission

```
EGIYR BKYKE UINXO UYFID IZ
```

Cryptanalyzing a Playfair Cipher David Kahn gives an excellent description of the difficulties of solving a Playfair cipher

> In the first place, the cipher's being digraphic obliterates the single-letter characteristics—*e*, for example, is no longer identifiable as an entity. This undercuts the usual monographic methods of frequency analysis. Secondly, encipherment by digraphs halves the number of elements available for frequency analysis. A 100-letter text will have only 50 cipher digraphs. In the third place, and most important, the number of digraphs is far greater than the number of single letters, and consequently the linguistic characteristics spread over many more elements and so have much less opportunity to individualize themselves. There are 26 letters but 676 digraphs; the two most frequent English letters, *e* and *t*, average frequencies of 12 and 9 %; the two most frequent English digraphs, *th* and *he*, reach only 3.25 and 2.5 %. In other words, not only are there more units to choose among, the units are less sharply differentiated. The difficulties are doubly doubled. [3, pp. 201–202]

This is not to say that Playfair cipher messages are unsolvable; they are eminently solvable. For long Playfair ciphertexts, or when one has a large number of cipher messages, one can resort to digraph frequency analysis. Otherwise, luck, careful observation and a deep understanding of how the cipher works are the best methods. As mentioned earlier, U.S. Army Lt. Joseph Mauborgne was the first to publish a solution to a Playfair in 1914. In 1936, Alf Mongé published a detailed and easy-to-follow solution to a very short challenge Playfair [4]. And in her novel *Have His Carcase*, mystery writer Dorothy Sayers has her sleuth Lord Peter Wimsey walk through a very detailed and understandable solution of a Playfair cipher that solves the case [5, pp. 355–371].

5.5 Ciphers in the Great War: The ADFGVX Cipher

The most famous cipher of World War I was solved by the greatest cryptanalyst of the war. In the spring of 1918, both sides on the Western Front were exhausted, having fought to a standstill for nearly four years. The Germans knew that they

had to crush the Allies soon, or they would run out of resources, both men and materiel. In preparation for their big spring offensives, the Germans changed their higher-level cipher system. This system was the one used to communicate at the division and corps level and above. The new system, called ADFGX appeared in early March, 1918 [3, p. 340]. It was different from any of the other cipher systems the Germans had used during the war.

ADFGX is what is known as a *fractionating cipher*. It is a substitution that produces digraphs as ciphertext, followed by a transposition where the digraphs are broken in two (the fractionating part) and then transposed.

It starts with a five by five Polybius square where a random mixed alphabet is inscribed in the square. The letters A, D, F, G, and X are used as both column and row headers of the square as in Table 5.1.

Encryption is now a three-step process. First, the message is read off one letter at a time and the corresponding row and column header becomes the digraph for that letter. Note that this operation will double the length of the message yielding Fig. 5.3.

Next, the digraphs are written out into a second table, row-by-row, one letter per column. The width of the table is the width of a pre-arranged keyword. If the keyword is GERMAN we get Fig. 5.4.

Finally, the fractionated table is sorted alphabetically by the keyword letters and the ciphertext is read off by columns Fig. 5.5.

```
AXDAA GDFDG GDAAX GXXGDX DDFFF DAGFG XDFFF A
```

Table 5.1 An ADFGX table with a mixed alphabet

	A	**D**	**F**	**G**	**X**
A	t	f	e	c	u
D	s	h	y	k	a
F	n	i	v	z	g
G	x	r	p	d	b
X	q	l	w	o	m

f	l	e	e	a	l	l	i	s	d	i	c	o	v	e	r	e	d
AD	XD	AF	AF	DX	XD	XD	FD	DA	GG	FD	AG	XG	FF	AF	GD	AF	GG

Fig. 5.3 First step of encryption using ADFGX

Fig. 5.4 Fractionated ciphertext

G	**E**	**R**	**M**	**A**	**N**
A	D	X	D	A	F
A	F	D	X	X	D
X	D	F	D	D	A
G	G	F	D	A	G
X	G	F	F	A	F
G	D	A	F	G	G

Fig. 5.5 Sorted ciphertext

A	**E**	**G**	**M**	**N**	**R**
A	D	A	D	F	X
X	F	A	X	D	D
D	D	X	D	A	F
A	G	G	D	G	F
A	G	X	F	F	F
G	D	G	F	G	A

The only way to solve an ADFGX cipher is to recover the sorted transposition key order. This is the problem that faced Georges Painvin on 21 March 1918 as the Germans launched their spring offensive.

Up to this point, less than three weeks after the ADFGX cipher had been introduced, there had not been enough traffic for Painvin to get a real handle on the cipher. But with the commencement of the offensive there was a jump in the number of messages transmitted and Painvin could really get to work.

Painvin noticed that there were messages in the pile of interceptions that had the same or very similar beginnings and a few with similar endings. He reasoned that this was because the plaintexts of these messages began with the same text and that the transpositions had moved the digraphs apart in a similar way. This was his key. Three weeks later, on 26 April he finally made a break in the initial group of interceptions and began to recover keys and break the cipher. His technique required a large number of messages and a subset of those with similar beginnings, so his technique would not work on all ADFGX messages and particularly he couldn't work with messages on days when there were few interceptions. Still, because the days immediately before an offensive saw an enormous increase in German traffic he was able to decrypt nearly 50 % of the messages sent.

Then just as he was hitting his stride and breaking more and more messages, the Germans changed the cipher on 1 June, adding an extra row and column to the Polybius square and an extra letter to the row and column headers. The cipher was now the ADFGVX cipher and each square now included all 26 letters of the alphabet and the ten decimal digits. Not too discouraged, Painvin worked for 26 h straight on the new messages and broke the updated cipher late in the day on 2 June [3, p. 345].

For a more detailed description of how Painvin solved the ADFGX cipher see [3, pp. 340–347]. For a description of a general solution of ADFGX, see [1, pp. 188–207].

5.6 A New Beginning

World War I marked the end of one phase in the history of cryptology. The volume of traffic that came as a result of the enormous armies that moved back and forth across Western Europe and their use of radio communication realistically marked the death knell for the lone cryptanalyst using paper and pencil to solve

cryptograms one at a time. Radio allowed for the easy interception of messages and this increase in their number caused the cryptanalytic organizations in all the involved countries to grow enormously. Radio also added another dimension to cryptanalysis—traffic analysis. Traffic analysis allowed G.2 A.6 to tell the cryptanalysts where a message had come from and to whom it was addressed. This allowed the cryptanalyst to examine messages in more context than previously, giving him additional information and probable words to use. The enormous number of messages sent and received also caused a re-thinking of the methodology and process of cryptologic systems. Cipher systems in particular needed to be fast and easy to use, all the while providing an even higher level of security. The process of sending and receiving messages was found wanting in many areas as cipher clerks and telegraph operators made mistake after mistake both in enciphering and sending messages, giving more openings for the cryptanalysts to work their magic. Finally, the various intelligence bureaus and the general staffs at last came to the realization that cryptologic information was one of the most worthwhile and valuable forms of intelligence.

Speed, accuracy, simplicity, and increased security were desired going forward. The machines were on their way.

References

1. Bauer, Craig P. 2013. *Secret history*: *The story of cryptology*. Boca Raton, FL: CRC Press.
2. Clark, Ronald. 1977. *The man who broke purple*. Boston: Little, Brown and Company.
3. Kahn, David. 1967. *The codebreakers*; *The story of secret writing*. Hardcover. New York: Macmillan.
4. Monge, Alf. 1936. Solution of a playfair cipher. *Signal Corps Bulletin* 93.
5. Sayers, Dorothy. 1932. *Have his carcase*: *A Lord Peter Wimsey Mystery*. New York: Brewer, Warren & Putnam.
6. Singh, Simon. 1999. *The code book*: *The evolution of secrecy from Mary, Queen of Scots to quantum cryptography*. New York, NY: Hardcover.
7. Yardley, Herbert O. 1931. *The American Black Chamber*. Indianapolis: Bobbs-Merrill.