History of Computing

John F. Dooley

The Gambler and the Scholars

Herbert Yardley, William & Elizebeth Friedman, and the Birth of Modern American Cryptology

Springer

History of Computing

The *History of Computing* series publishes high-quality books which address the history of computing, with an emphasis on the 'externalist' view of this history, more accessible to a wider audience. The series examines content and history from four main quadrants: the history of relevant technologies, the history of the core science, the history of relevant business and economic developments, and the history of computing as it pertains to social history and societal developments.

Titles can span a variety of product types, including but not exclusively, themed volumes, biographies, 'profile' books (with brief biographies of a number of key people), expansions of workshop proceedings, general readers, scholarly expositions, titles used as ancillary textbooks, revivals and new editions of previous worthy titles.

These books will appeal, varyingly, to academics and students in computer science, history, mathematics, business and technology studies. Some titles will also directly appeal to professionals and practitioners of different backgrounds.

John F. Dooley

The Gambler and the Scholars

Herbert Yardley, William & Elizebeth Friedman, and the Birth of Modern American Cryptology

Springer

John F. Dooley
William and Marilyn Ingersoll Professor Emeritus
of Computer Science
Knox College
Galesburg, IL, USA

ISSN 2190-6831 ISSN 2190-684X (electronic)
History of Computing
ISBN 978-3-031-28317-8 ISBN 978-3-031-28318-5 (eBook)
https://doi.org/10.1007/978-3-031-28318-5

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

For Diane, Patrick, and for David Kahn

Preface

These days pretty much everyone has heard of the various cryptologic agencies of the US Government. The National Security Agency (NSA) comes to mind first, but there are also cryptologic groups in the FBI, CIA, State Department, Secret Service, and other departments of the government. These organizations are arguably the most sophisticated—and secretive—on the planet. It was not always like this. While the major European and Asian powers have had permanent, professional code and cipher bureaus for several hundred years, the United States did not have a permanent code and cipher organization until after World War I.

This book is the story of how that permanent organization came to be. More specifically, it is the story of the two men and one woman who were there at the beginning and were instrumental in the creation of modern American cryptology and our modern code and cipher organizations.

For the first one hundred fifty years of its existence, the United States depended on ad hoc intelligence organizations that would come into being in the Army and Navy during wartime and just as quickly disappear as soon as peace was finalized. As late as March 1917, just as America was getting ready to enter World War I, the entire military intelligence organization of the US Army consisted of a single officer stationed in Washington, DC. That officer, Major Ralph van Deman, however, was the right person in the right place at the right time. Van Deman was determined to create a professional military intelligence section for the United States and hopefully have it continue in existence after the war. Van Deman did two things in the spring of 1917 that made his dream come true. First, he worked out an arrangement with a private research laboratory in Illinois to decrypt secret messages for the Army while the new Army intelligence operation was being set up. Second, he went looking for ambitious government employees who were interested in intelligence. These two acts brought to the Army's attention three individuals, Herbert Yardley, William Friedman, and Elizebeth Smith Friedman.

We will explore their origins and examine how they came to learn the arcane science of cryptology. We will look at how they came to cryptology because of happenstance and then the entry of the United States into World War I and the efforts they made to make sure the United States had the best code and cipher experts in the

world. In 1917, Herbert Osborn Yardley, a young telegrapher from Indiana, was a code clerk in the U.S. State Department who had become interested in codes and ciphers. Interested enough that he had broken the State Department's own systems. After the Americans entered the Great War, Yardley was referred to van Deman and talked himself into a job heading up a fledgling cryptanalytic bureau in the US Army. At the same time, William Fredrick Friedman, a Russian immigrant of Jewish descent, and his wife, Elizebeth Smith Friedman, a mid-Western Quaker, were working on the Illinois prairie for an eccentric millionaire in a private research laboratory and trying to decode cryptograms that may have been found in the plays of William Shakespeare. Just as Yardley was convincing the Army to set up a cryptanalytic organization, the Friedmans were volunteered by their boss and approved by van Deman to set up a group to decrypt messages sent to them by the Army, Justice, and Treasury departments. For all three of these people, this was the beginning of life-long careers in code and cipher creation and breaking that would transform the American intelligence community.

All three of our subjects have had biographies written about them. William was first, with an unfortunately flawed biography commissioned by Elizebeth Friedman and written by Ronald Clark within a decade of his death in 1969. Yardley's excellent biography was written by the cryptologic historian David Kahn in 2004, 46 years after Yardley's death in 1958. Elizebeth was last, with her first—and excellent—biography appearing in 2017, 37 years after her own death. What none of these biographies have done, however, is to deeply examine the relationships between these three remarkable people, their competition, friendship, and later animosity, and how their paths continued to cross over the course of 40 years. That is what the current book hopes to do. The book draws on resources from the Library of Congress, the National Archives, the National Security Agency's Archives, the collections of the National Cryptologic Museum Library, where David Kahn's and the Yardley's papers are housed, the Research Library at the George Marshall Foundation, where William and Elizebeth Friedman's papers are held, and the papers of a number of other people who were instrumental in the creation of the American intelligence community and which are held in a number of other collections. As much as possible, I have tried to take materials, stories, and quotes directly from the words and writings of Yardley and the two Friedmans.

Galesburg, IL, USA John F. Dooley
26 January 2023

Acknowledgments

This book is the result of over a decade of work, so there are many people to thank. I would like to thank the library staff at Knox College for their patient and professional help in finding copies of many of the articles and books referenced here. The Faculty Development office at Knox College provided me with travel and research funds for several years so I could work on various projects, including this one. My colleagues in the Computer Science department at Knox were always supportive and encouraging of my research. I would also like to thank the staff of the National Archives and Records Administration (NARA) in College Park, MD, Librarians René Stein and Rob Simpson in the Research Library at the National Cryptologic Museum in Ft. Meade, MD, and Paul Barron, Jeffrey Kozak, and Melissa Davis of the George C. Marshall Foundation Research Library in Lexington, VA for their excellent help. Thanks also to Wayne Wheeler and his excellent team at Springer Nature. They are always a pleasure to work with. As always, the World Wide Web allows a writer in the middle of the American prairie to access libraries and archives around the country and the world, for which I am very grateful. Thanks to an anonymous reviewer of the first draft of the manuscript who did herculean work and made a large number of very helpful suggestions that have improved the text greatly. Thanks also to our furry feline roommates Arlo and Janis for walking on the keyboard at all the right moments. And, of course, special thanks to my wife, Diane, who inspires me, encourages, me, and—above the call of duty—reads and edits everything I write (except for the equations and cryptograms, which she skips right over).

Contents

About the Author

John F. Dooley is the William and Marilyn Ingersoll Professor Emeritus of Computer Science at Knox College in Galesburg, Illinois. After more than 16 years in industry and 22 years teaching undergraduate computer science, he retired in 2017 but continues to do research and writing, particularly in the history of cryptology. He has written more than two-dozen refereed articles and numerous book reviews published in journals and in computer science and cryptologic history conference proceedings. He has published six previous books, *Software Development and Professional Practice* (Apress 2011), *A Brief History of Cryptology and Cryptographic Algorithms* (Springer 2013), *Codes, Ciphers, and Spies* (Springer 2016), *Software Development and Design* (Apress 2017), *Codes, Villains, and Mystery* (CreateSpace 2017), and *History of Cryptography and Cryptanalysis* (Springer 2018). Since 2004, his main research interest has been in the history of American cryptology, particularly in the period from the beginning of the twentieth century through World War II. His web page is at https://www.johnfdooley.com.

Chapter 1
Introduction

In all of the wars and insurrections in which the United States was involved from 1776 through 1916, the Army had never had a permanent code and cipher organization. Whenever the United States would enter into a war—the Revolution, 1812, the Civil War, the Spanish-American War—the Army, usually at the encouragement of a single officer, would create an intelligence service that would mostly be involved in what is known as positive intelligence, that is, gathering intelligence about the enemy usually through the use of human resources. This organization would also have a technical body—the cryptographers who would create and use codes and ciphers to hide the contents of Army communications from enemy spies and whose members would attempt to decrypt intercepted enemy communications. There would also be a negative or counterintelligence branch whose job was to prevent enemies from using espionage or sabotage against American resources or intelligence services; they would try to catch enemy spies. Intelligence operations were generally seen as necessary but somehow not gentlemanly or fair. It was the type of service for which very few officers would volunteer. As soon as the current conflict was concluded, the intelligence service would be disbanded, and all its knowledge and experience would be lost. When this knowledge was needed again for the next war, it would need to be created from scratch. This cycle of creation and dissolution of intelligence services continued primarily because the American military "did not feel threatened by enemies on its borders and thus saw no need for an early warning mechanism."[1]

The State Department recognized the need for diplomatic codes and ciphers to protect diplomatic correspondence, so they would periodically create new code systems and replace existing ones at embassies and consulates. However, they never felt the need for having an organization designed to break other nations' codes. It

[1] James L. Gilbert, *World War I and the Origins of U.S. Military Intelligence* (Lanham, MD: Rowman & Littlefield Publishing Group, Ltd., 2015), https://rowman.com/ISBN/9780810884601/World-War-I-and-the-Origins-of-U.S.-Military-Intelligence, 1.

J. F. Dooley, *The Gambler and the Scholars*, History of Computing,
https://doi.org/10.1007/978-3-031-28318-5_1

was only during wartime that the United States government saw the need to attempt to break enemy codes and ciphers. This was in stark contrast to most of the European powers that had had secret departments known as Black Chambers that were used to intercept and break diplomatic correspondence since the late 1500s. All European armed forces also had their own cryptologic staff that continued in existence even between conflicts.

Once again, at the entry of the United States into World War I in April 1917, a formal military intelligence organization was created. And once again, it was likely to be disbanded at the end of that war. However, that is not what happened. Finally, in 1919, the War, Navy, and State Departments were convinced of the utility of a continuing organization dedicated to creating codes and ciphers for the government and for breaking the codes and ciphers of other countries—friend and foe alike. This change in attitude was largely because, first, with the easy victory over Spain in the Spanish-American War, and second, in coming to the aid of the faltering Allied powers during World War I, the Americans had finally realized that their country was a world power on par with the Europeans and as such needed to not only protect itself but also project power around the globe. America couldn't do either of those things without being able to gather and assess intelligence about friends and potential foes in a timely fashion and communicate securely with its own far-flung forces. Codes and ciphers were key elements of that intelligence organization.

It turned out that in 1919 there were two men in the country who were uniquely positioned to take on the challenge of creating the cryptographic and cryptanalytic organizations that would provide the type of intelligence America would need in peacetime and would prepare the armed forces for assuming that task in wartime. Born 2 years apart at the end of the nineteenth century, they had both served in the Army during the war, performing exactly the tasks that would be needed in the new permanent cryptologic organizations. Both were self-taught in cryptology, having read and digested nearly all the available cryptologic texts available in English in the United States just before America's entry into the war. Both were ambitious, driven by curiosity, service to country, and a deep, abiding need to succeed.

At the time that the United States entered World War I on 6 April 1917, there were just about a dozen people in the US Army and Navy who knew anything at all about cryptography and cryptanalysis. Half of them never got to practice their skills with codes and ciphers because the Army and Navy needed them elsewhere. The other half were generally assigned to the newly forming signals intelligence units in the American Expeditionary Force (AEF) and the Office of Naval Intelligence. Resources were thin, and the Army was scrambling to put together its General Staff organizations for the entire Army and the AEF. Anybody with any skills in codes and ciphers was being recruited as quickly as possible.

Herbert Osborn Yardley was a code clerk in the State Department where he had worked since 1912. Yardley, bored on overnight shifts in the State Department code room, had set himself the task of seeing if he could break the State Departments' own codes. It turned out he could. This appalled him, and he wrote a report on his midnight adventures and gave it to his boss, who did not quite believe him but who made a change in a State Department code anyway. Yardley broke that one as well,

just in time to be recruited by the Army, commissioned an officer, and told to create a cryptanalytic section within Military Intelligence. His section, originally called the Cable and Telegraph Section and later the Code and Cipher Section, was the eighth in Military Intelligence, MI-8. Yardley immediately began recruiting cryptanalysts. But this was not an easy task because the skill set was rare, and he was competing with every other section in the Army for personnel.

William Frederick Friedman was a Russian immigrant who had come to the United States at the age of two. A graduate of Cornell University in genetics, at the American entry into the war he was working for an eccentric millionaire at a private research laboratory in Illinois, outside Chicago. Friedman was also an amateur photographer, and his boss, George Fabyan, roped him into taking pictures of pages from a First Folio of Shakespeare for another project at the laboratory, proving that Sir Francis Bacon had written all of the Bard's plays and had hidden coded messages in the plays that proved his authorship. The coded messages were allegedly written in a cipher of Bacon's own devising that used differences in the shapes of typefaces to disguise different letters of the alphabet. Enlarging the pages from the First Folio was thus essential to finding the typeface differences, hence the need for Friedman's photographic skills. Friedman became fascinated with the cipher and proceeded to teach himself cryptology. He was eventually dragooned into the Bacon-Shakespeare project, a prospect he anticipated eagerly mostly because in addition to the cipher, Friedman was interested in one of the project assistants, Elizebeth Smith.

While the Army was busy forming Yardley's MI-8 section, it still needed to create codes and break German Army and diplomatic cipher messages. With Yardley having no one in his section early on, the Army turned to Fabyan and his Baconian researchers to help decrypt intercepted messages. So, in the summer of 1917, William Friedman, the now Elizebeth Smith Friedman, and several others at Fabyan's Riverbank Laboratories began a side project working to decipher messages delivered from various US government departments.

Over the course of the 20 months that the United States would fight in World War I, these two men, Friedman and Yardley, would become the nucleus of that new permanent US government cryptologic organization. Yardley grew his MI-8 section from two people, himself and a clerk, into an organization with half a dozen subsections and more than 165 personnel by the end of the war. Friedman, after spending 9 months training cryptanalysts for the Army and breaking codes and ciphers on the Illinois prairie, would join the Army himself, be assigned to Military Intelligence, and end up as the head of the Code Solution Section of the AEF in France. The two men would meet for the first time in France in December 1918. It was an interesting and cautious meeting. They knew of each other by reputation. Friedman was rapidly gaining status within the Army as a brilliant cryptanalyst; he soaked up new cryptologic ideas like a sponge and generated new ideas almost as quickly. Yardley had shown he had the organizational skills to quickly grow a large, efficient bureau; he was an excellent manager and a terrific salesman, and he had already convinced his boss of the need for a permanent cryptanalytic bureau after the war, with him at the head.

This was their beginning.

Chapter 2
Beginnings: Herbert Yardley

Herbert Osborn Yardley was born on 13 April 1889 in Worthington, Indiana, which at that time had a population of 1,448. Herbert was the second of four children of Robert Kirkbride and Mary Emma Osborn Yardley. His father was a railroad station manager and telegrapher, and his mother was a housewife. Herbert's mother died of a sudden heart attack in February 1903 when he was 13, and his father's parenting skills were tested in the years after that. In high school, Yardley was not tall, just five-feet-five-inches, but he was good looking, intelligent, personable, and a terrific storyteller. He edited the high school paper, was elected class president, and captained the football team. He was also a voracious reader and an excellent poker player, having picked up the game early and starting at sixteen was a regular at games in the back room of one of Worthington's seven saloons. Herbert graduated from high school in Michigan because he'd been expelled from the Worthington high school for a senior prank in 1907.[1] He attended the University of Chicago for a year studying English but then quit. He spent two summers in 1906 and 1907 traveling the rails around the American West with a high school friend working odd jobs and playing poker before ending up back in Worthington, working in 1908 and 1909 as a railroad telegrapher like his father. However, Worthington, indeed no small town in the American Midwest, was big enough or exciting enough for Herbert, and his ambition drove him to the big city. He ended up in Washington, DC, in the second half of 1912 at the age of 23 after having taken the Civil Service exam for telegrapher and receiving the highest score. On December 23rd of that year after swearing an oath to "support and defend the Constitution of the United States against all enemies, foreign and domestic," Yardley started work as a $900 per year code clerk at the State Department in an office in the State, War, and Navy Department Building (now the Eisenhower Executive Office Building (EEOB)) immediately to the west of the White House on Pennsylvania Avenue (Fig. 2.1).

[1] David Kahn, *The Codebreakers: The Story of Secret Writing* (New York: Macmillan, 1967), 5.

J. F. Dooley, *The Gambler and the Scholars*, History of Computing,
https://doi.org/10.1007/978-3-031-28318-5_2

Fig. 2.1 Herbert Yardley. (US Army photo)

Young, living in a big city for the first time, and employed at the center of Woodrow Wilson's new government, Yardley had a great time. The State Department and its code room fascinated him.

> This spacious room with its high ceiling overlooked the southern White House grounds. By lifting my eyes from my work I could see a tennis game in progress where a few years earlier President [Theodore] Roosevelt and his tennis Cabinet had played each day.
>
> Along one side of the room ran a long oak telegraph table with its stuttering resonators and sounders; cabinets containing copies of current telegrams almost blocked the entrance. In the center sprawled two enormous flat-topped desks shoved together, about which a few code clerks thumbed code books and scribbled rapidly, pausing now and then to light cigarettes. The pounding of typewriters specially constructed to make fifteen copies of a telegram mingled with the muted click of the telegraph instruments. The walls were covered with old-fashioned closed cupboards filled with bound copies of telegrams from and to consular and diplomatic posts throughout the world. In the corner stood a huge safe, its thick doors slightly ajar.
>
> There was an air of good-fellowship in the room and I was soon at home.[2]

Yardley's time at the State Department was interesting but eventually boring. The code clerks handled all the telegraphic and cable communications for the State Department, and the office was full of diplomats of all levels coming and going even

[2] Herbert O. Yardley, *The American Black Chamber* (Indianapolis: Bobbs-Merrill, 1931), 17–18.

into the late evening. Yardley was not that impressed with the Ivy League diplomats but was certainly interested in their power, influence, aplomb, and finesse.[3] His career progressed at a nice clip, and he was given a raise to $1000 a year in April 1914, enough money for a small family to live on.

When Herbert left Worthington, he also left behind the girl next door, Hazel Milam. Hazel's family was well off for Worthington, and her father was a big player in local Republican politics. Hazel, five weeks older than Herbert, was in the same classes as he all through elementary and high school. They had dated on and off and finally became engaged on 12 May 1914. Hazel immediately got on a train and followed Herbert to Washington. Herbert Yardley and Hazel Milam were married in Washington, DC, on the day she arrived, 20 May 1914, both of them just twenty-five. They moved into the small apartment that Yardley was renting in northwest Washington. Over the next couple of years, they visited Worthington a few times, and their younger brothers, Pat Milam and Dick Yardley, came out to Washington in 1915. Hazel escaped the Washington heat and humidity and spent the summer of 1916 at her parent's home in Worthington. In 1917 Hazel got a job as a typist with the Quartermaster's Corps at $1000 per year. Nearly doubling their income allowed them to move into a row house at 542 Shepherd Street NW.

Yardley was intensely interested in the code and cipher messages that passed through the State Department Code Room. They were a challenge to his inquisitive mind. Ambitious as he was, Yardley figured that learning more about those codes and ciphers would help his career. "As I asked myself this question I knew that I had the answer to my eager young mind which was searching for a purpose in life," he wrote. "I would devote my life to cryptography. Perhaps I too, like the foreign cryptographer, could open the secrets of the capitals of the world. I now began a methodical plan to prepare myself."[4]

Starting in early 1915 he proceeded to learn as much as he could about the mysterious field of cryptology. He explored libraries, including the Library of Congress, for books on cryptography, only to be very disappointed. It turned out that in 1915, there were precious few books in English on cryptography and even fewer in the libraries around Washington. He read fiction, finding the classic story of codebreaking in Edgar Allan Poe's *The Gold Bug*, and relishing it. But he was ultimately disappointed in Poe and his declarations of expertise in cryptanalysis. "I searched Edgar Allan Poe's letters for a glimpse of the scientific treatment of cryptography. These were full of vague boasts of his skill - nothing more... I know that Poe merely floundered around in the dark and did not understand the great underlying principles."[5] One slim, 105-page book he found at the Library of Congress and

[3] Yardley, *ABC*, 18.

[4] Yardley, *ABC*, 20.

[5] Yardley, *ABC*, 20–21.

devoured was the then new US Army *Manual for the Solution of Military Ciphers* by Captain Parker Hitt, which was published early in 1916 (Fig. 2.2).[6]

Hitt's book was an excellent place to start. It reads like an introductory course in cryptography and cryptanalysis. It covers language characteristics, transposition ciphers, substitution ciphers—both monoalphabetic and polyalphabetic, and polygraphic ciphers such as Playfair, which was the standard English Army cipher at the time. It also discusses methods of analyzing encrypted messages to determine their type and examines errors that encipherers make. Yardley ate it up. The book provided his real foundation of cryptologic knowledge and his first introduction into breaking enciphered messages. As we will see, Hitt's book was also the introductory text that William and Elizebeth Friedman used to learn elementary cryptanalysis and was their initial textbook when they taught cryptanalysis to Army officers at the Riverbank Laboratories in 1917.

Unfortunately, Hitt's book contains nothing about codes, only ciphers. However, one thing Yardley knew was that many messages in code were also enciphered

Fig. 2.2 Parker Hitt during World War I. (US National Archives)

[6] Parker Hitt, *Manual for the Solution of Military Ciphers*, SRH-004 (Fort Leavenworth, KS: Press of the Army Service Schools, 1916).

before they were dispatched. This is called superencipherment. So, in order to break an encoded message, the first thing to do was to remove this superencipherment to reveal the underlying code words. For homework, Yardley would make copies of select State Department coded messages and try to break them. He also convinced a friend or two at the telegraph companies in Washington to slip him the occasional coded telegrams of foreign embassies.[7]

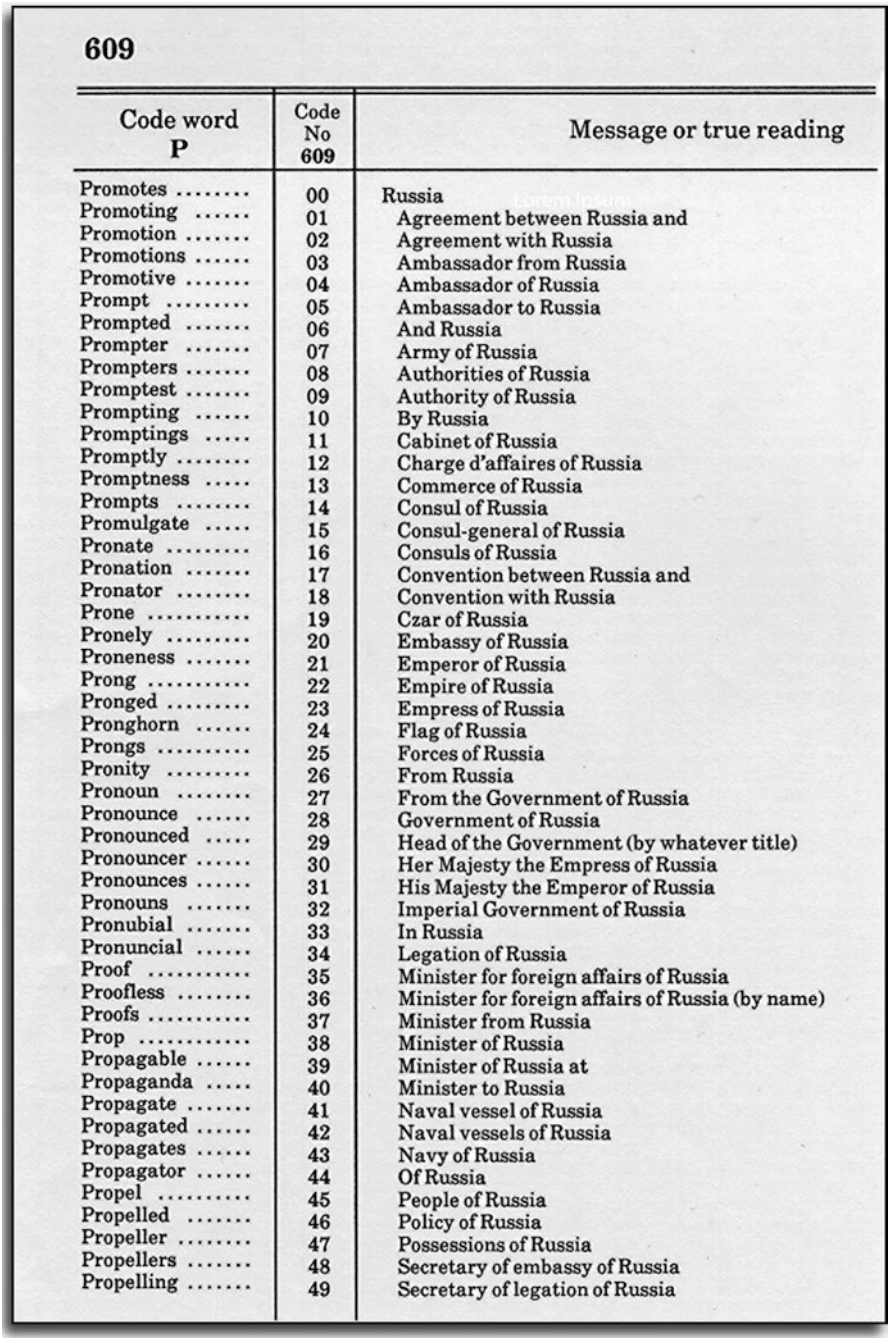
Yardley was shocked by what he found. The American State Department codes were distressingly easy to break. In 1915, the State Department was using three different codes to transmit messages between Washington and embassies and consulates around the world. The Red Code, released in 1876 and named for the color of its cover, was a 1200-page book that listed nearly ten thousand plaintext equivalents, codewords, and associated numeric codewords. The codewords were real English words designed to make it easier for telegraphers to send messages and recover from mistakes. The Blue Code, released in February 1899, added 300 pages to the Red Code, for a total of 1500. Finally, the Green Code was a 1418-page book that was released in 1910 and was the current code used for messages between Washington and most embassies abroad when Herbert Yardley started work in the State Department code room in 1912.[8] The biggest change in the Green Code was the replacement of plain English codewords with five-letter random codewords. All three of these codes also contained a separate sixteen-page addendum with the wishful title *Holocryptic Code, An Appendix to the Cipher of the Department of State*. In the spirit of the inconsistency of cryptographic nomenclature, the *Holocryptic Code* describes a cipher and the *State Department Cipher* was a code. The Holocryptic Code contained fifty (later seventy-five) rules on how to increase the security of the three Department codes, including rules on how to add a superencipherment to code messages.

All three codes were *one-part codes*, which consisted of a single table with the plaintext words and their alphabetic and numeric codeword equivalents listed in ascending order. This type of code was easy to use for encryption, slightly more difficult for decryption (because for the code numbers, one had to find the right number in the right-hand column) and, unfortunately, fairly easy for an experienced cryptanalyst to crack. One-part codes are easier to solve because the cryptanalyst needs to uncover just a few words and their equivalent codewords before they can start to guess the meanings of plaintext around nearby alphabetic or numeric codewords. When Yardley was working in the State Department Code Room, many European powers were able to read all three of the American codes (Fig. 2.3).

Yardley's most interesting piece of "homework" was a 500-word enciphered message sent in the spring of 1915 after a peace-making trip that President Wilson's confidante Colonel Edward House took to Europe and written in a cipher system devised by House and used between the two men. This message presented Yardley

[7] Yardley, *ABC*, 21.

[8] Ralph Edward Weber, *United States Diplomatic Codes and Ciphers, 1775–1938* (Chicago: Precedent Pub., 1979), 246.



609

Code word P	Code No 609	Message or true reading
Promotes	00	Russia
Promoting	01	Agreement between Russia and
Promotion	02	Agreement with Russia
Promotions	03	Ambassador from Russia
Promotive	04	Ambassador of Russia
Prompt	05	Ambassador to Russia
Prompted	06	And Russia
Prompter	07	Army of Russia
Prompters	08	Authorities of Russia
Promptest	09	Authority of Russia
Prompting	10	By Russia
Promptings	11	Cabinet of Russia
Promptly	12	Charge d'affaires of Russia
Promptness	13	Commerce of Russia
Prompts	14	Consul of Russia
Promulgate	15	Consul-general of Russia
Pronate	16	Consuls of Russia
Pronation	17	Convention between Russia and
Pronator	18	Convention with Russia
Prone	19	Czar of Russia
Pronely	20	Embassy of Russia
Proneness	21	Emperor of Russia
Prong	22	Empire of Russia
Pronged	23	Empress of Russia
Pronghorn	24	Flag of Russia
Prongs	25	Forces of Russia
Pronity	26	From Russia
Pronoun	27	From the Government of Russia
Pronounce	28	Government of Russia
Pronounced	29	Head of the Government (by whatever title)
Pronouncer	30	Her Majesty the Empress of Russia
Pronounces	31	His Majesty the Emperor of Russia
Pronouns	32	Imperial Government of Russia
Pronubial	33	In Russia
Pronuncial	34	Legation of Russia
Proof	35	Minister for foreign affairs of Russia
Proofless	36	Minister for foreign affairs of Russia (by name)
Proofs	37	Minister from Russia
Prop	38	Minister of Russia
Propagable	39	Minister of Russia at
Propaganda	40	Minister to Russia
Propagate	41	Naval vessel of Russia
Propagated	42	Naval vessels of Russia
Propagates	43	Navy of Russia
Propagator	44	Of Russia
Propel	45	People of Russia
Propelled	46	Policy of Russia
Propeller	47	Possessions of Russia
Propellers	48	Secretary of embassy of Russia
Propelling	49	Secretary of legation of Russia

Fig. 2.3 A page from the 1899 State Department Blue Code (note that code numbers all start with 609xx).[a] (National Security Agency)

[a] John H. Haswell, "State Department Cipher" (U. S. Government Printing Office, 1899); Ralph Edward Weber, *Masked Dispatches: Cryptograms and Cryptology in American History, 1775–1900*, vol. 2nd (Fort George G. Meade, MD: Center for Cryptologic History, National Security Agency, 1993), 205.

with what he thought was most surely a very challenging cryptanalytic task. It took him just 2 hours to break the cipher and read the message.[9] The message itself, sent after House's trip to Berlin and while he was on his way home and in Berne, Switzerland, is really only 301 code words, although Yardley may have been referring to plaintext words in the decrypted message. House and Wilson were using the State Department Blue Code, along with a superencipherment designed by House.[10]

No wonder Yardley was astounded at the contents of the message and aghast that he could decode it so easily. His description in his later book does not give any hints as to how he did his decryption, but it is full of commentary on the weakness of American codes and the small-mindedness of its leaders; this would be a theme in Yardley's later writings as well. However, while a very good example of cryptanalysis on Yardley's part, this is not as significant an achievement as it appears at first. Yardley was working in the State Department code room and thus had access to both the Blue Code book and the Holocryptic Code book addendum. House's variation on the Blue Code used the Blue Code book but created a novel way of creating numeric codewords using that book. In House's system, the correspondents renumbered the pages starting at the back and finishing at the first page of the code. Then, when looking up a plaintext word or phrase, the person creating the coded message would count down the words on the page to the word or phrase they wanted and then append those two digits to the end of the reworked page number. While tricky, if one has possession of the Blue Code codebook and determines the renumbering of the pages and the reworking of the numeric codewords as a book cipher, then the decryption is simple. This decryption is a commendable feat for a beginning codebreaker, but nothing spectacular. Nevertheless, it showed Yardley that he had some talent at codebreaking and that creating good, secure ciphers and codes was much harder than it appeared.

This was still a very disturbing development for State Department cryptology. Yardley knew that House was in Europe and on his way home from his peace mission, so House's telegram would have gone through both French and English telegraphic cables on its way to the trans-Atlantic cable. He also knew that both countries were in the habit of examining all traffic that passed over their cables. Surely if an amateur like Yardley could break messages in these weak codes and ciphers, England and the other European powers, with their professional codebreaking organizations, were having a field day. In fact, while the British MI1(b) Army cryptographic organization that had intercepted House's message had not yet fully broken the Blue Code, it would do so by the fall of 1915, followed quickly by its break of the Green Code before the end of the year.[11] This would make the

[9] Yardley, *ABC*, 22.

[10] Ralph Edward Weber, "State Department Cryptographic Security, Herbert O. Yardley, and Woodrow Wilson's Secret Code," in *In the Name of Intelligence: Essays in Honor of Walter Pforzheimer*, (Washington, DC: NIBC Press, 1994), 594–595. and Daniel Larsen, "Creating An American Culture Of Secrecy: Cryptography In Wilson-Era Diplomacy," *Diplomatic History* 44, no. 1 (January 1, 2020): 102–32, https://doi.org/10.1093/dh/dhz046

[11] Larsen, *American Culture*, 123.

messages—again mostly in the Blue Code—between House and Wilson during House's second peace-making mission in early 1916 transparent to the British.

Yardley was also distressed that nowhere in the American government was there the equivalent to these European Black Chambers that routinely read the diplomatic messages of other countries and had for centuries. This was not just in Yardley's imagination. John H. Haswell had written to the Secretary of State in 1898 as he was creating the Blue Code that the European governments all had Black Chambers and could all likely read American State Department coded messages.[12]

Yardley decided that he needed to do something about the weakness of the American codes. But, what could he do? He was just a lowly code clerk, and it was his boss who was responsible for many of the State Department codes. Besides, he did not think that President Wilson would be pleased to know that a State Department clerk was reading the secret messages between him and his most trusted advisor.[13] What he did in the end was to spend nearly 2 years learning as much as he could about codes, ciphers, and cryptanalysis and then find as many weaknesses as he could in the State Department codes and ciphers. This exercise made Herbert Yardley the first civilian peacetime professional codebreaker in American history. Late nights when there was little to no traffic, Yardley would look through the days' messages and figure out how an enemy cryptanalyst would attack them. Over the course of the years, he worked through the State Department codes and the Holocryptic code and wrote up everything that he found in a 100-page report. Finally, in early 1917, as America was becoming increasingly nervous about the war in Europe, he presented the report to his boss, David A. Salmon, who had just been named chief of the Office of Indexes and Archives. Salmon was shocked and impressed by Yardley's report, calling it a "fine piece of work." Just about a month later, Salman presented Yardley with a series of messages using a new set of rules for the superencipherment of State Department coded messages and asked him to break it. Several weeks later and likely just after the United States had declared war on Germany, Yardley presented his solution to Salmon, who confirmed it. Yardley then asked Salmon for a recommendation letter so that he could apply for a commission in the Army and go to work for them breaking codes. Salmon was reluctant to let Yardley go but was finally convinced to write the letter. Yardley then went about finding the right person to talk to at the War Department and was ultimately pointed to one Major Ralph Van Deman who was head of the newly created Military Intelligence Section of the Army General Staff.[14]

At its entry into the war in April 1917, the United States had no military intelligence organization.[15] This state of affairs was finally rectified on 3 May 1917—nearly a month after war had been declared—when the War College Division created

---

[12] Weber, *State Dept Cryptographic Security*, 564.

[13] Yardley, *ABC*, 21–22.

[14] Yardley, *ABC*, 31–36.

[15] James L. Gilbert, *World War I and the Origins of U.S. Military Intelligence* (Lanham, MD: Rowman & Littlefield Publishing Group, Ltd., 2015), https://rowman.com/ISBN/9780810884601/World-War-I-and-the-Origins-of-U.S.-Military-Intelligence, 1–5.

the Military Intelligence Section (MIS), later the Military Intelligence Division (MID), under Major Ralph Van Deman.[16] Van Deman, a Harvard graduate who also had both law and medical degrees, had been in the Army since 1891. He was in the first class of the Army War College in 1904 and had organized and run the Military Intelligence Division in the Philippines during the Philippine-American War (1899–1902). He was the ideal person to run the new MID and would become known as the "Father of American Military Intelligence" (Fig. 2.4).[17]

Van Deman lost no time in organizing the MID. Beginning with just a couple of enlisted soldiers and some civilians, Van Deman had, by the end of 1917, an organization of several hundred soldiers and civilians and a budget of over $1 million, modeled on the British military intelligence organization. One of the subsections that Van Deman created was Subsection 8, the Code and Cipher Section, MI-8.

In early June, when Yardley dropped into his office, Van Deman was intrigued with Yardley's idea for a War Department Cipher Bureau. However, Yardley was not Van Deman's first choice for MI-8. He really wanted a Regular Army officer who

Fig. 2.4 Ralph Van Deman during World War I. (US Army photo)

[16] Gilbert, *Origins*, 28–29.

[17] Gilbert, *Origins*, 11–13.

had been trained in cryptology. However, at the beginning of the American entry into the war, there were exactly three Regular Army officers trained in codes and ciphers—Captains Parker Hitt, Frank Moorman, and Joseph Mauborgne, and, in a brilliant bit of Army wisdom, none of them were ultimately assigned to strictly cryptographic duties.[18] Hitt would become the Chief Signal Officer of the American 1st Army in France, Moorman would be the chief of the American Expeditionary Force's (AEF) Radio Intelligence Section G-2 A-6, and Mauborgne would head up the Signal Corps research division. So, after convincing the State Department to let Yardley go, Van Deman had him commissioned a first lieutenant in the Signal Corps of the National Army on 29 June 1917, and he was assigned to active duty in Military Intelligence on July 5th. On July 11th, Van Deman put Yardley, then twenty-eight years old, in charge of the Code and Cipher Section of Military Intelligence, section MI-8. According to David Kahn, when Yardley took command of MI-8, "He had broken some codes and believed he could crack others. He was ambitious. And now he had, via cryptology, a chance to be not an underling, but a boss. Sure that he could handle the opportunity, he seized it."[19]

Thus, unbeknownst to either Yardley or Friedman began the competition that would follow them through the next 25 years.

[18] Gilbert, *Origins*, 44.

[19] David Kahn, *The Reader of Gentlemen's Mail: Herbert O. Yardley and the Birth of American Codebreaking* (New Haven: Yale University Press, 2004), 21.

Chapter 3
Beginnings: William Friedman and Elizebeth Smith

Wolfe Frederick Friedman was born on September 24, 1891, in Kishinev, Russia (now Chisinau, the capital of Moldova), a city near the Romanian border. His father was an interpreter and translator for the Russian Postal Service, and his mother was the daughter of a well-to-do merchant in Kishinev. The late 1800s were not a good time to be Jewish inside the Russian Empire. The pogroms in the southwestern part of the Empire from 1881 to 1884 resulted in a series of laws restricting Jewish settlements and occupations. Sensing the approach of more restrictions and the increasing tensions that heralded more pogroms, the Friedmans emigrated to the United States in 1892 and 1893; Wolfe's father Frederick left in 1892, headed west, found a job, and established himself. The rest of the family followed the next year, all of them settling in Pittsburgh, Pennsylvania. Not finding a job as an interpreter, Frederick ended up as a door-to-door salesman, selling sewing machines for Singer, and the family settled into their new life in America. Wolfe's name was changed to William shortly after the family landed in Pittsburgh when his parents became citizens. William grew up as a typical first-generation immigrant boy in early twentieth-century urban America. Graduating from high school in 1910, William at first embraced a back to the land movement that was having its day and attracting many young Jewish immigrants to the rural, farming life, enrolling at Michigan Agricultural College in Lansing. It turned out that farming was not exactly to William's city-raised liking, and so after 1 year he transferred to Cornell University in upstate New York and switched his major from agriculture to genetics. He graduated in February 1914 and then stayed on at Cornell to start graduate school. However, a little over a year later, William's graduate study plans would be upended by an opportunity that he could just not pass up (Fig. 3.1).

George Fabyan was a decidedly successful American businessman. Born in 1867 into a wealthy industrial family, he was the elder son of George Francis and Isabella Fabyan. The elder Fabyan had founded and built a successful dry goods and textile company in Boston. George decided early on that he did not want to follow in his father's footsteps and work in the family business; he would leave that to his younger

J. F. Dooley, *The Gambler and the Scholars*, History of Computing,
https://doi.org/10.1007/978-3-031-28318-5_3

Fig. 3.1 William Friedman c1924. (Library of Congress)

brother Francis. Instead, he threw it all over, quit school at 16, and spent several years roaming the western United States, working here and there as, among other occupations, a salesman, a tie and timber agent, and a cotton broker, acquiring a nonstandard education in the process.[1] While working for a timber company in northern Wisconsin, George met and married Nelle Wright, the daughter of a local merchant. Nelle was anxious to be out of the northern forests and live in a big city, so the young couple headed to Chicago. Landing there in 1892, Fabyan went to work in his father's Chicago office as a warehouse assistant under an assumed name. Working his way up, he did so well that his manager insisted on introducing him to the senior George Fabyan during one of his visits to the Chicago operation. Reconciled to his family, George became the Chicago managing partner of Bliss Fabyan & Company and grew the business substantially during the Gilded Age in the 1890s and early 1900s. In 1905, George Fabyan bought the first of what was ultimately several hundred acres about 40 miles west of Chicago along the Fox River in the little town of Geneva and proceeded to convert the existing farmhouse into a modern mansion—designed by Frank Lloyd Wright and called the "Villa." He

[1] Richard Munson, *George Fabyan* (North Charleston, SC: CreateSpace Independent Publishing Platform, 2013), 17.

then set about creating one of the first private research laboratories in the United States, Riverbank Laboratories. Fabyan would hire scientists and engineers and allow them a free hand to do research as long as it was in an area in which Fabyan himself was interested. The laboratories specialized in acoustics (a spin-off acoustics company still exists today), genetics, and in an obscure area that Fabyan found fascinating—proving that Sir Francis Bacon wrote all of William Shakespeare's plays and left coded messages in the plays verifying that authorship. On the estate, Fabyan built a lavish Japanese garden, a spacious lodge, laboratory buildings, a Roman-style swimming pool, a lighthouse, and housing for many of the more than 150 workers. He even imported a complete windmill that he had erected on the banks of the Fox River (Fig. 3.2).[2]

Fabyan acted like a feudal lord. Tall and heavyset with a goatee and always in a riding outfit and boots, even though he did not ride, he would stride around his estate every day, micromanaging his workers and sharing his opinions on everything. As a manager, he was rude, loud, and imperious. He paid his workers as little as possible, lied to them in order to get his way, and inserted himself into their private lives to the point of intercepting and reading their mail. He was everyone's least favorite boss, a bully. However, for the scientists and engineers on his staff, he gave them the opportunity to work on interesting problems (Fig. 3.3).

Fig. 3.2 The grounds of Riverbank looking across the gardens and toward the windmill (author's collection)

[2] Munson, *Fabyan*, 47–56.

Fig. 3.3 George Fabyan in his "Hell Chair" where he would interrogate his employees. (Courtesy of Preservation Partners of the Fox Valley)

For the 23-year-old William Friedman, it was the genetics laboratory that attracted him to Riverbank in the spring of 1915 when George Fabyan asked the faculty at Cornell for any bright young men who wanted to do research in crop hybridization. Friedman's faculty adviser recommended him to Fabyan, and after some negotiations, William left Cornell and arrived at Riverbank in the summer of 1915 as the head of the new Department of Genetics. He lived on the second floor of the windmill across the Fox River from Fabyan's villa and the Lodge where Mrs. Elizabeth Wells Gallup was in charge of the Bacon/Shakespeare cipher project.

Mrs. Gallup's obsession was to prove that Francis Bacon had embedded coded messages into the works of Shakespeare using a cipher of his own invention called the biliteral cipher. The biliteral cipher used two different fonts to create two different types of letters in the plays. The two letter types, called A and B, were used in groups of five to encipher individual letters of the alphabet. In Bacon's cipher system, the letter "a" is represented by AAAAA, "b" is AAAAB, "c" is AAABA, etc., on down to "y" encoded as BABBA and "z" as BABBB. The complete alphabet

from Bacon's time (where I = J because there was no J in the English alphabet in the late sixteenth century, and U = V because there was no V) is[3]:

a	AAAAA	b	AAAAB	c	AAABA
d	AAABB	e	AABAA	f	AABAB
g	AABBA	h	AABBB	i = j	ABAAA
k	ABAAB	l	ABABA	m	ABABB
n	ABBAA	o	ABBAB	p	ABBBA
q	ABBBB	r	BAAAA	s	BAAAB
t	BAABA	u = v	BAABB	w	BABAA
x	BABAB	y	BABBA	z	BABBB

For example, if the A type font is a regular Times font and the B is the italic version of the Times font, then the sentence "I am Fr Bacon" might be enciphered using the sentence "N*o*w is the win*te*r *o*f o*u*r *di*scontent *m*ade glorious su*m*me*r b*y *th*i*s* sun of York" with a few extra letters at the end.

Mrs. Gallup's objective was to identify the two different font types and then to extract the cipher letters and read pages from Shakespeare's First Folio to uncover the secret coded messages. In order to do this, and because the differences in the type fonts were minuscule, she needed blown up pictures of the individual pages of the First Folio. So, she required a good photographer to take pictures of each of the pages and blow them up to a useful size so she and her assistants, using magnifying glasses, could identify the two font types.

It turned out that William Friedman was a very good amateur photographer, and as a result, for increasingly long periods of time during 1916, he was dragged away from his plants and genetics work to take pictures of Shakespearean plays for Mrs. Gallup. Not that he minded being diverted from his primary work that much, because starting in the summer of 1916 he was increasingly distracted by one of Mrs. Gallup's assistants, a young lady from Indiana named Elizebeth Smith.

Elizebeth Smith—the spelling is deliberate; her mother did not want her being called Eliza—was the tenth and last child of John Marion Smith, a Quaker farmer and local Republican office-holder in Huntington, Indiana, and his wife Sopha Strock Smith. By the time Elizebeth was born on August 26, 1892, most of her siblings were already grown and out of the house. Growing up, Elizebeth was closest to her next older sister, Edna, who was just two years her senior. Elizebeth was a precocious, fidgety, and talkative child who had, over the years, a strained relationship with her father. John Smith did not want his youngest child to go to college; he thought that it was a waste of money for a woman to get a higher education. When Elizebeth insisted and went behind his back to apply to several small colleges, he was furious. Instead of giving her the money for her college tuition, he loaned some of it to her at an interest rate of 4 percent—and she paid it back. She attended the College of Wooster in Wooster, Ohio, between 1911 and 1913. When her mother

[3] Sir Francis Bacon, *The Advancement of Learning*, ed. Joseph Devey (New York, NY: P. F. Collier & Son Company, 1901), http://oll.libertyfund.org/titles/bacon-the-advancement-of-learning, 124.