No 5 - FINAL

Wm F. Friedman

Lecture No. 5 1st Draft

For a half century following the close of the Civil War, cryptology in the United States enjoyed a period of hibernation from which it awoke at long last, ~~in~~ about 1914, not refreshed, as did Rip Van Winkle, but weaker. This is perhaps understandable if we take into account the fact that the United States was able to enjoy a long era of peace, broken only briefly by ~~one~~ the short war with Spain, in 1898. ~~the Spanish-American, of 1898.~~ For over three decades there ~~was no~~ appeared to be little or no interest in or need for, cryptologic operations, except such as were required for ~~the~~ secret communications of the Department of State. The military and naval services apparently felt that in time of peace there ~~is~~ was no need for either cryptography or cryptanalysis, and since it looked as though the US was going to enjoy peace for ~~a long,~~ an indefinitely long time, those services did not think it necessary or desirable to engage in cryptologic studies. Of course, the War Department and the Army still had their route ciphers and cipher disks; the Navy Department and the Navy had their disks for producing monoalphabatic ciphers; and the Department of State had a code more or less specifically designed for its communications. Everything on the international scene, so far as concerned the US, was quiet. Let Europe fight - it was not of our way of life or our affiar.

The long hibernating period was briefly broken by one episode that may interest you. I had not planned to bring it to your attention in this brief history but certain events in the very recent past lead me to tell you about it. I refer here to the very small popular-vote majority by which Democratic candidate Kennedy won the Presidency over Republican candidate Nixon, and the consequent talk about the possibility of an upset when the electoral college would convene to do its work. The very same sort of situation occurred in the presidential election of 1876, in which Democratic candidate Samuel J. Tilden was pitted against Republican candidate Rutherford B. Hayes. On the basis of early returns Tilden seemed to be easily the winner. Going to bed on election night, 8 November 1876, Hayes conceded to Tilden and the newspapers next morning in fact reported a Tilden victory. But a couple of days after the election it began to appear that perhaps Tilden's victory was not sure, and his supporters began maneuvers to try to make it certain by taking advantage of our peculiar system of electing a president, peculiar because it is the electoral, not the popular, vote which determines who is to be president. Two days after the people had voted it became clear that Tilden would have 184 electoral votes, just one vote short of insuring victory, whereas Hayes would have only 163, thus needing 22 more. The Tilden supporters began a frantic campaign to get that one additional vote and they didn't hesitate to try bribery, a rather serious piece of business obviously requiring a good deal of secrecy. Of course, many telegrams had to be exchanged between the Tilden headquarters in New York City and confidential agents sent to certain states where electoral votes could perhaps be purchased; telegrams also had to be exchanged among secret agents in the field. About 400 telegrams were exchanged and about 200 of these were in cryptographic form. Because of communication difficulties two almost-consummated deals fell through; a third deal failed because the electors were honest Republicans not susceptible to bribery. The existence of these telegrams remained unknown for months. But the outcome of the election remained in doubt because four states, Florida, South Carolina, Louisiana and Oregon each sent two groups of electors, an event not foreseen and provided against in the Constitution. A crises arose and the country seemed on the verge of another civil war. By an act of 29 January 1877, Congress created a special electoral commission to settle the disputed electoral votes in the four states. The commission voted in favor of the Hayes electors in each case and Hayes entered the White House. But it was only some months afterward that the telegrams to which I have referred were brought to light and a situation arose which Congress felt it had to look into. Somehow or other, copies of the telegrams came into the possession of a Republican newspaper, The New York Tribune, in the summer of 1878, and two members of its staff succeeded in solving those in cryptographic form.

Those of you who are interested in the political aspects of this intriguing story will find excellent reading material in various books dealing with it. Those of you who are interested only in its cryptologic aspects will find excellent material in the following three documents:

(1) "The Cipher Dispatches", The New York Tribune, Extra No. 44, New York, (14 January) 1879.

(2) Hassard, John R. G., "Cryptography in Politics", The North American Review, Vol CXXVIII, No. 268, March 1879, pp 315-325.

(3) U.S. House Miscellaneous Documents, Vol 5, 45th Congress, 3rd Session, 1878-79.

The Congressional House Committee designated to conduct the investigation was named "The select Committee on alleged frauds in the Presidential Election of 1876." In the course of the investigation, the Committee called a Professor Edward S. Holden, of the United States Naval Observatory in Washington. I think he was a captain in the Navy and specialized in mathematics. The Tribune had brought him into the picture and Proffessor Holden solved the ciphers but only after Mr. John R. G. Hassard, the chief of The Tribune staff, and his colleague, Colonel William M. Grosvenor, also of that staff, had reached a solution.

Professor Holden's testimony is of considerable interest. He presented his solution of the nearly 200 cryptograms entered in evidence. His testimony is summarized in a letter dated 21 February 1879 and it sets forth all the cryptosystems used by both parties, together with their keys and full details of their application. In that letter, Professor Holden makes the follow statement: "By September 7, 1878, I was in possession of a rule by which any key to the most difficult and ingenious of these (the transposition cipher of the Democrats)could infallibly be found." Holden worked out the transposition keys but in this he was of course anticipated by the Tribune cryptanalysts. There were in all 10 different keys, two for messages of 10 words, two for messages of 15 words, etc, up to and including two for messages of 30 words. Here is the complete table of keys:

Leave one quarter page space

You may be wondering why there are two transposition keys for each length of message from 10 to 30 in multiples of 5. The two keys constituting a pair are related to each other, that is, they bear a relationship which one of the Tribune cryptanalysts, Hassard, termed "correlative", but which we now would call an "encipher-decipher" or "verse-inverse" relationship. Either sequence may be used to encipher, the other to decipher a message. For example, key III consists of the following: 8-4-1-7-13...etc, and the correlative, key IV, is 3-7-12-2-6...etc. A cipher message of 15 words can be deciphered either by (1) numbering its words consecutively and then assembling the words in the order 8-4-1-7-13, or by (2) writing the sequence 3-7-12-2-6... above the words of the cipher message and then assembling the thus-numbered words according to the sequence 1-2-3-4-5... Thus, there were, in reality, not ten different transposition keys but only five. In the case of each pair of keys one of them must have been the basic sequence, the other the inverse of it.

I suspect that the basic or "verse" sequences of numbers were not drawn up at random but were derived from words or phrases; and I suspect that the odd-numbered ones are the "verse". I have not had time to try to reconstruct them. Perhaps some of you may like to make the attempt. You will notice that in the odd-numbered keys, the positions of sequent digits reflect an underlying key word or phrase.

In addition to transposition, this system involved the use of code words to represent certain words and the names of certain persons and places, and numerals. There were also a few nulls. Here is the entire vocabulary:

Leave ¼ page space

Professor Holden adds some comments about this system which are worth presenting:

> The essence of this ingenious and novel system consists in taking apart a sentence written in plain English (dismembering it, as it were) and again writing all the words in a new order, in which they make no sense. The problem of deciphering it consists in determining the order according to which the words of the cipher should be written in order to produce the original message.
>
> There is one way, and only one way, in which the general problem can be solved, and that is to take two messages, A and B, of the same number of words, and to number the words in each; then to arrange message A with its words in an order which will make sense, and to arrange the words of message B in the same order. There will be one order - and only one - in which the two messages will simultaneously make sense. This is the key.

It appears that Professor Holden did not note the verse-inverse relation in each pair of sequences, or, if he did, he failed to mention it, as Hassard did in his article.

There were enough messages to permit of establishing the meanings of the code words used, so that the plain text of practically all the messages in this, the most complicated of the cryptosystems involved in this bizarre political episode, became quite clear.

Another system used by the conspirators employed a 2-letter for one letter substitution and was based upon a 10 X 10 checkerboard. Apparently neither Professor Holden nor the Tribune cryptanalysts recognized the latter principle, nor did they find that the coordinates of the checkerboard employed a key phrase, nor did they realize that the same checkerboard, with numerical coordinates, was used for the two-digit for one letter substitution. Here are two of the messages exchanged by the conspirators, one in the letter cipher, the other in the figure cipher:

Leave $\frac{1}{4}$ page space

They are long enough for solution, if you wish to try to solve them and find the key phrase, which should amuse you by its appropriateness.

There were several other systems involved, but I am going to have to pass them by because they hardly deserve attention in this brief history. I do, however, want to call your attention to the very close resemblance between the word-transposition ciphers characterized by Professor Holden as "the most difficult and ingenious" of the ciphers he solved, and the USMTC route ciphers described in the preceeding lecture. Yet, not only he but also the Tribune amateur cryptanalysts solved those ciphers without too much difficulty, even though they were technically more complex. I think their work confirms my own appraisal of the weakness and futility of the route ciphers used by the USMTC in the Civil War.

Let us now go on with cryptologic history after this digression.into the realm of what may be called political cryptology. I do not know what the Department of State used for cryptographic communications in the years following the Civil War. Probably it was a small code, even an adaptation of some commercial code. But in an article entitled "secret Writing", which appeared in Century Magazine, Vol LXXXV, November 1912, No. 1, a man named John H. Haswell, apparently a code clerk in the Department, referred to a new code of the department in the following terms:

> The cipher of the Department of State is the most modern of all in the service of the Government. It embraces the valuable features of its predecessors and the merits of the latest inventions. Being used for every species of diplomatic correspondence, it is necessarily copious and unrestricted in its capabilities, but at the same time it is economic in its terms of expression. It is simple and speedy in its operation, but so ingenious as to secure absolute secrecy. The construction of this cipher, like many ingenious devices whose operations appear simple to the eye but are difficult to explain in writing, would actually require the key to be furnished for the purpose of an intelligible description of it.

Only four years later a certain telegraph operator and code clerk of the State Department proved how vulnerable the Department's system of enciphered code really was. His name was Herbert O. Yardley and many of you may know a bit about him because he was the author of a famous or infamous book (depending upon whose side you're on) entitled The American Black Chamber, which was published by the Bobbs-Merrill Co. in 1931. So far as I know it is the only book which cannot legally be reprinted in the United States because a special law passed in 1934 makes it a criminal offense to do so. That is quite a story in itself but I cannot tell it now. So if you happen to own a copy of the first and only American edition, don't let it get away from you, because you can only obtain another copy of it by a more or less "under the table" deal or may only be able to purchase an English edition by a similar sort of deal. But to return to that State Department cryptosystem considered by Haswell "to secure absolute secrecy", here is the cover page of Yardley's 21-page typewritten analysis.

Leave $\frac{1}{4}$ page space

Yardley was quite wrong in thinking that his was the first successful attempt to solve a problem in enciphered code, for in Europe successful attempts on more complicated cases were often the rule and I imagine that British cryptanalysts could have and perhaps did read State Department messages as a more or less routine matter. For in Europe, cryptanalytic studies were going on apace during the years of American neglect of such studies.

In our Navy the monoalphabetic ciphers continued in use until the middle of the eighties, when several naval officers were designated to prepare a more suitable system based upon a code particularly for naval communications. The system they worked out involved a very large codebook, 18" long, 12" wide and 2" thick, which had the official title The U.S. Navy Secret Code, and an accompanying but separate cipher book almost as large and designated as The Book of Key Words. In addition to these two books was a third book called "General Geographical Tables. The system was placed into effect on 1 December 1887. About ten years later a new edition of the third book was placed into effect. Later I will show you a most historic message sent in that clumsy system of secret communication.

In our Army in the middle eighties, too, a code was also prepared, and its composition and format hardly shed laurels upon those responsible for its production because it was merely a counterfeit of ~~the~~ a commercially available small code first published in 1870 for use by the general public under the title Telegraphic code to ensure secresy in the transmission of telegrams, by Robert Slater, Secretary of the French Atlantic Telegraph Co. As to the nature of the code, I will quote from Slater's own "Short explanation of the mode of using this work."

> It is a numbered Telegraphic Dictionary of the English language, of which each word bears a distinctive No. (from 00001 to 25000, with exactly 100 words' per page), and the method of using it is by an interchanging between correspondents that a further No. is to be added to or deducted from the number in the code, of the word telegraphed or written, to indicate the real-word intended, thus a "Symbolic" or "Dummy Word" is telegraphed, the meaning of which can only be read by those who have the key to the secret of how many should be added to or deducted from the number in the Code, of the "Dummy Word" to find the word meant.

Here we have a sentence of 116 words with a meaning which is quite murky but I think you will gather its import. The system as thus far described is what we now call an additive or subtractor method. But in the detailed instructions Slater goes one step further and suggests that instead of telegraphing the code numbers resulting from addition or subtraction, the words standing alongside the sum (or difference) of the mathematical operation be sent.

Slater's code must have met with popular acclaim because by 1906 it was in its fifth edition. You may like to see the title page of the second edition (1879), a copy of which is in my collection. I wish I had a copy of the very first edition but not even the Library of Congress has one, that's how scarce it is. To get on with the story, in 1885 the War Department published a code for its use and the use of the Army. Here is a picture of its title page. The only difference between it and the title page of the 2nd edition of Slater's Code is in the spelling of the word secrecy, as you can easily see in the picture I show you next. It would appear that Col. Gregory was just a bit deficient in imagination because not only did he simply borrow the basic idea of Slater's code but also when it came to preparing the rules for and examples of enciphering the code groups the colonel used the identical rules and wording and even the same type of transformations that are found in Slater's original. Let me show example of Slater's code side by side with the same example from Gregory's:

Leave 1/2 page space

All the other methods and examples in the two codes are practically identical. Colonel Gregory gives credit to a civilian aide, in the following terms: "The labor of compiling the new vocabulary has been performed by Mr. W. G. Spottswood. And Mr. Spottswood's work consisted in casting out such words as ABALIENATE and ABANDONEE from Slater's list and replacing them with such words as ABATEMENT and ABATIS. This sort of work must indeed have been arduous. I'm sorry to appear to be so critical of my predecessors in the construction of codes and code systems for War Department and Army usage, but I feel sure you will agree that more imagination and ingenuity could have been employed than were used by Messrs. Gregory and Spottswood.

Col. Gregory prepared a confidential letter to Lieut. General Sheridan, "Commanding Army of the U.S.", to explain the beauties of the new code. Again because I'm afraid you won't place too much credence in what I'm telling you, the confidential letter from Col. Gregory to Lieut. General Sheridan is printed in toto in Appendix I, tb.which I have added Col. Gregory's "Introduction" to the instructions for using the code.

Believe it or not, this was the code that the War Department and the Army used during the Spanish-American War. It was apparently used with simple additive, because in a copy in my collection the additive is written on the inside of the front cover. It was 777. In pages 41-42 of The American Black Chamber the author throws an interesting sidelight on this code system:

> The compilation of codes and ciphers was, by General Orders [he meant Army Regulations], a Signal Corps function, but the was [1917] revealed the unpreparedness of this department in the United States. How much so is indicated by a talk I had with a higher officer

> of the Signal Corps who had just been appointed a military attache to an Allied country. It was not intended that attaches should actually encode and decode their own telegrams, but as a part of an intelligence course they were required to have a superficial knowledge of both processes in order that they might appreciate the importance of certain precautions enforced in safeguarding our communications.
>
> When the new attache, a veteran of the old Army, appeared, I handed him a brochure and rapidly went over some of our methods of secret communications. To appreciate his attitude, the reader should understand that the so-called additive or subtractive method for garbling a code telegram (used during the Spanish-American War) is about as effective for maintaining secrecy as the simple substitution cipher which as childred we read in Poe's The Gold Bug.
>
> He listened impatiently, then growled: "That's a lot of nonsense. Whoever heard of going to all that trouble? During the Spanish-American War we didn't do all those things. We just added the figure 1898 to all our figure code words, and the Spaniards never did find out about it.

Although The American Black Chamber abounds with exaggerations and distortions, what the author tells about the inadequacies of United States codes and ciphers in the years just before our entry into World War I are true enough and Fardley's impatience and satires in this regard are unfortunately fully warranted.

We have noted how inadequately the Army and the War Department were equipped for cryptocommunications in the decades 1890-1910. Let us see how well equipped the Navy and the Navy Department were. For this purpose I have an excellent example and one of great historical significance and interest. You will recall my mention of the appointment of a board of Navy officers to prepare a suitable cryptosystem for the Navy and I told you about the large basic codebook and its accompanying almost as large book for enciphering the code groups. For the story we go back to the time of President McKinley, whose election brought Theodore Roosevelt, a former member of the Civil Service Commission, back to Washington as Assistant Secretary of the Navy. Teddy was an ardent advocate of military and naval preparedness and frankly favored a strong foreign policy, looking forward, in fact, to the ultimate withdrawal of the European powers from the Western Hemisphere. With vigor, he set to work to make the Navy ready. When the Battleship Maine was blown up in Havana harbor on 15 February 1898, Roosevelt sharpened his efforts. During a temporary absence of his chief, John D. Long, he took it upon himself to instigate the preparations which he had in vain asked the Secretary to make. He ordered great quantities of coal and ammunition, directed the assembling of the Fleet and stirred the arsenals and navy yards into activity. On a Saturday afternoon, ten days after the Maine was blown up, and still in the absence of Secretary Long, Teddy sat down and wrote out a cablegram to go to Commodore George Dewey. Here it is, with his bold signature at the bottom:

Cablegram Leave ¼ page space.

That was the now historic message which alerted Dewey and which resulted in our taking the Philippines from the Spanish,in the war which was declared ten days later on Spain.

I don't know when that classification "Secret and Confidential" was crossed out but it must have been years later, for those three words appear in the plain text of the deciphered and decoded cablegram. Here is a picture of the code cablegram as it was received in Hong Kong:

Leave ½ page space

And now I show you the deciphered and decoded text, which I produced myself by courtesy of the Chief of the Navy Security Group, who permitted me to consult and use the necessary books from Navy Security archives. To translate a message three steps are necessary. First, the cable words (the peculiar, outlandish words in line 2 - WASSERREIF, PAUSATURA, BADANADOS, CENTENNIAL, etcl) are sought in the cipher book, and their accompanying cable-word numbers set down. WASSERREIF yields 99055; PAUSTURA yields 62399, BADANADOS, 11005; CENTENNIAL, 16820. The next step is to append the first digit of the second cable-word number to the last digit of the first cable-word number to make the latter a six-digit number. Thus 99055 becomes 990556. The six-digit code group number is then sought in the basic code book and its meaning is found to be "Secret and Confidential." The transfer of demonstration of a straightford, mathematical method of solving the Vigenere cipher was published in Berlin during the mid-period of the Civil War in America. If the book created an impression in Europe it was altogether unspectacular; in America it remained unheard of until after the advent of the 20th Century. Although Kasiski's method is explained quite accurately in the first American text on cryptology, Capt. Parker Hitt's Manual for the solution of military ciphers. (Fort Leavenworth, Kansas: Army Service Schools Press, 1916), the name Kasiski doesn't even appear in it. Other books on cryptologic subjects appeared in Europe during this period among which the more important were the following:

Leave $\frac{1}{4}$ page space

Of the foregoing two deserve special mention. The first, by commandant Bazerier, is a book notable not for its general contents, which are presented in a rather disorganized, illogical sequence, but for its presentation of a cipher device invented by the author, the so-called cylindrical cipher device, a picture of which I now show you. But our own Thomas Jefferson anticipated Bazeries by a century, and here are two slides describing Jefferson's "Wheel Cypher", copied from the original manuscript among the Jefferson Papers in the

Library of Congress. The second book in the foregoing list which is deserving of altration is the one by de Viaris, in which he presents methods for solving cryptograms prepared by the Bazeries cipher cylinder or Jefferson's Wheel Cypher.

It was in the period during which books of the foregoing nature were written and published that the chanceries of European Governments operated so-called Black Chambers, organized for solving the secret communications of one another. Intercept was unnecessary because the governments owned and operated the telegraph systems and traffic could be obtained simply by making copies of messages arriving or departing from telegraph offices on in transit through them. This was true in the case of every country in Europe with one very important exception: Great Britain. The story is highly interesting but I must condense it to a few sentences.

In England from about the year 1540 on-word a black chamber was in constant operation. It was one of two collaborating organizations called The Secret Post Office and The Office of Decipherer.

In the former, letters were opened, copies of them were made, the letters replaced, the envelopes resealed, and if there were wax seals, duplicates were made. Copies of letters in cipher were sent to the Offices of Decipherer for solution and the results sent to the Foreign Office. A famous mathematician, John Wallis, took part in the activities of the Office of Decipherer. But in 1844 a scandal involving these two secret offices caused Parliament to close them down completely so that from 1844 until 1914 there was no black chamber at all in Britain. As a consequence, when World War I broke out on the first of August 1914 England's black chamber had to start from scratch, but British brains and ingenuity within a few months built a cryptologic organization known as "Room 40 O.B.", which contributed very greatly to the Allied victory in 1918.

Perhaps the greatest achievement of Room 40 O.B. was an operation which just in the nick of time brought this country into World War I as an active belligerant on the Allied side. The operation involved the interception and solution of what is known as the Zimmermann Telegram, deservedly called the most important single cryptogram in all history. On 8 September 1958 I gave an account of this cryptogram, its interception, its solution, and how the solution was handed over to the United States, bringing America into the war on the British side, without disclosing to the Germans just how the plain text was obtained, least of all that it had been obtained by interception and solution by cryptanalysis. My talk, given under the auspices of the NSA Crypto-Mathematics Institute, was recorded and is on file. It took two and a half hours and I didn't quite succeed in telling the whole story, which you will find in great detail (except for some important technical data not yet available to the public) in a book entitled The Zimmermann Telegram, by Barbara Tuchman, (Date). Also, you should consult a book entitled Eyes of the Navy, by Admiral Sir William James, (Date). Both books deal at length with the Zimmermann Telegram and tell how astutely Sir William Reginald Hall, Director of British Naval Intelligence in World War I, managed the affair so as to get the maximum possible advantage from the feat accomplished by the British Black Chamber. To summarize, as I must, this fascinating true tale of a cryptanalytic conquest, let me first show you the telegram as it passed from Washington to Mexico City.

leave ½ page space