Excerpts from The Secret Service of America

1. Before the first World War, America was using codes and ciphers so simple a schoolboy could work them out. The texts of Colonel House's messages to Wilson were undoubtedly quickly decoded by every other nation. The secret dispatches of the American Mission to Russia were used as elementary examples in the training of student cryptographers just after we'd entered the war. And on these messages depended the fighting of the war and the making of the peace!

p. 4

2. Even the ranking officers on the Western Front could not be persuaded that their existing method of communication was entirely insecure. A young officer with the sketchiest knowledge of cryptography set out to prove this. From an intercept of an American message he learned the disposition of troops along the St. Mihiel salient, the number and names of our divisions, and, finally, the actual hour at which the great American offensive would be launched. The enemy, through reading the messages, was prepared for the great offensive of 1918 and began to withdraw. The surprise attack had missed its purpose.

p. 19

The story of

3. The use of secret ink by German spies in this country during the last war is a fascinating one. Their chemists' technique was perfected to the point where they could conceal secret inks impregnated, without discolouring, in [redacted] handkerchiefs, collars, or silk scarfs. The spy had only to soak the garment in water to bring out the chemicals. He used this solution to write his letter, threw out the solution, dried the garment and wore it until the next time it was needed. Later they developed a reagent which could develop a letter written with clear water. American chemists had an anxious time before they discovered this simple solution: Insert a secret-ink letter in a glass case and shoot in a thin vapour of iodine. This vapour gradually settles into all the tiny crevices of the paper that have been disturbed by pen and water, and the clear outline of the writing is visible.

p. 35, 42, and 44

4. By January, 1918, the Code and Cipher Solution Section of MI-8 had mushroomed rapidly. At this time several strange messages from Germany to Mexico were interesting them especially. Through guess after guess, each one confirmed later by a mathematical formula, they found that the Germans were using an English dictionary to encode their dispatches. The messages were beamed straight at the government radio station, were addressed to the German Minister in Mexico City and authorized a huge bribe to Mexico to stay neutral. Later dispatches proved the machinations of Japan in Mexico. Then, suddenly, the station became silent, just as it promised so much. Someone in MI-8 was either a German spy or had a loose tongue, for that avenue of information was closed for the rest of the war.

P. 85-89, 108

5. In February, 1918, a man was captured crossing the Mexican border who was believed to be one of the most dangerous and unscrupulous of the German spies in America. Nothing was found on him but a scrap of paper bearing a jumble of letters. Its decipherment resulted in the death sentence [redacted] for the man carrying the document, for it read, "The bearer of this is a subject of the Empire who travels as a Russian under the name of Pablo Waberski. He is a German secret agent. Give him all the protection and assistance necessary." It was addressed to the German consular authorities in Mexico.

P. 91-112

6. The Navy Department had insisted on organizing their own Cryptographic Bureau, but in July, 1918, they suddenly discharged all their employees, donated their elaborate secret-ink equipment to our laboratory, and placed a liaison officer in MI-8 to represent them. Though it had been in existence for over a year and had a

641

large personnel, it had failed to decipher a single ciper or code message or to develop one secret-ink letter,

7. In the last war, the British considered the Cipher Bureau so important that they placed an Admiral at its head. Because of the messages that he obtained from the messages that his enormous bureau deciphered, this man, Admiral Hall, stood next to Lloyd George in power. The Foreign Office envied his position greatly, for it was almost wholly dependent on him for information revealing the secret political intrigues of enemy and neutral governments. For instance, the famous Zimmermann-Carranza note, in which Germany promised Mexico the States of New Mexico, Texas and Arizona if she would declare war against the United States, came from the British Cipher Bureau. p. 149

8. There was no wonder that England was a great Power. She read practically every code telegram that passed over her cables. p. 150

9. During the Peace Conference a telegram was deciphered which reported an Entente plot to assassinate President Wilson, either by administering a slow poison or by giving him the influenza in ice. There is no way of knowing whether this plot had any truth in fact, and if it had, whether it succeeded. But there are these undeniable facts: Ptresident Wilson's first sign of illness occurred while he was in Paris, and he was soon to die a lingering death. p. 164

10. After the war, all sections of MI-8 were demobilized except that which dealt with the solution of codes and ciphers. The funds allowed could not be expended withing the District of Columbia, so they located in a brownstone front in the East Thirties in the heart of New York City. There they stayed for ten years was housed the American Black Chamber. No one knew of its existence but a few men in the State Department. P. 166

11. During the Washington Armament Conference held in 1921, some five thousand deciphered Japanese messages containing the secret instructions of the Japanese delegates were sent to Washington. Through them we learned just how close Great Britain and Japan were, and that a complete understanding between the two countries was proposed before the conference. P. 174, 208

12. For instance, Lord Curzon proposed that before the Japanese Government made any proposal to the American Government concerning the Pacific Conference, the contents of the proposal could be confidentially communicated to the British Government. P. 209

13. On November 28, 1921, the Black Chamber deciphered the most important and far-reaching telegram that ever passed through its doors. It is from the Japanese Foreign Office to the Japanese plenipotentiary in Washington. It is the first sign of weakness on the ten-to-seven Japanese demands. The following telegram definitely determined the respective strength of the fleets of Japan and the United States:

"We are of your opinion that is is necessary to avoid any clash with Great Britain and America, particularly America, in regard to the armament limitation question. You will to the utmost maintain a middle attitude and redouble your efforts to carry out our policy. In case of inevitable necessity, you will work to establish your second proposal of 10 to 6.5. If, in spite of your utmost efforts, it becomes necessary in view of the situation. ....to fall back on your proposal No. 3, you will endeavour to limit the power of concentration and manoeuvre of the Pacific by a guarantee to reduce or at least to maintain the status quo of Pacific defenses and to make an adequate reservation which will make clear that this is our intention in agreeing to a 10 to 6 [illegible]

45.00 cryptography 1917-1929

Excerpts from Secret and Urgent

1. P. 15...It was often seen said that there is no such thing as an insoluble cipher. In a strict sense, this is not true, for in the early Middle Ages Roger Bacon wrote a whole manuscript in a cipher that has thus far defied analysis. However, in actual use, all ciphers are k down on repetition--and repetition is practically unavoidable. And wherever ciphers are most frequently used, they must be written in a hurry, usually by men without much special training, and also go without special apparatus. The effort to break them down will always be made by experts with ample training, a wealth of time at their disposal and whatever special apparatus they need.

2. P. 16...Also, the more complex and safe the cipher, the greater likelihood there is of error. If a cipher is progressive, a single error renders all the rest of the message gibberish, even to the man with the key. An officer of the British Black Chamber estimates that one-third of all the cipher messages which passed through that department during the World War were garbled.

3. P. 56...The allegorical code was very much in use at the time of the World War, and the only answer any nation found to it was by censoring telegrams. At one time the censor found in his hands a telegram from a man suspected of being a spy. "Father is dead," the message said simply. The censor considered it briefly, changed the text to "Father is deceased" and let it go through. Next morning the reply was placed on his desk: "Is father dead or deceased?"

4. P. 77-82...Much of the centuries-old mystery surrounding the condemnation and execution of Mary Queen of Scots can be cleared up by evidence furnished in ciphered letters. When Mary was in captivity and scheming for the throne of England, all her correspondence with her co-plotters was enciphered. Walsingham, Elizabeth's Secretary for Secret Service, trained a young Jesuit in forging and seal-breaking and managed to place him with the Queen of Scots as a messenger for her secret correspondence. The first message to fall into Walsingham's hands broke down easily. It explained the detail of an ingenious plan to assassinate Elizabeth, and named -- in code number -- six young men of Elizabeth's own household who were in the scheme. After Mary definitely approved of the plot, a huge manhunt was started which had its desired effect--the six young men fled for their lives. They were all caught, and, within a month, Mary Queen of Scots was on trial for her life.

5. P. 87-88...Endless research has gone into proving that Bacon wrote all we now call the product of Shakespeare's pen-- and to no avail. All the attempts claim this fact is enciphered in several of Shakespeare's plays, but they use a ridiculous number of variables to prove their point. The anti-Baconians show that even more remarkable coincidences of numbers and text can be discovered elsewhere. For example, it can be demonstrated that Shakespeare wrote the Forty-Sixth Psalm: the Psalm is numbered forty-six; the forty-sixth word from the beginning is shake, the forty-sixth word from the end is spear: Q.E.D.

6. P. 92....Acrostics are in a good literary tradition: Villon, as well as Edgar Allan Poe used them; and the Harvard baccalaureate hymn of 1926 was a famous and scandalous acrostic whose hidden properties the university authorities did not discover till it had been sung in their chapel and published in the Boston press.

7. The general criticism of all the Shakespearean-decipherments is that Bacon's description of his bi-literal system clearly demands the use of two altogether different forms of type,(a roman font to mean a and an italic, b . Each letter of the alphabet was assigned to it a series of values made up of a and b in different combinations: aaaaa or aaaab, for instance) while all the decipherments thus far offered depend upon the detection of minor variations, often imperceptible only with a magnifying glass, in two fonts of type which are essentially the same. In addition, the Elizabethan custom of using scattered type makes any consistent bi-literal decipherment practically impossible. All the techniques devolve into anagramming or insanity. This does not necessarily deny that Bacon wrote the plays; it merely means there is no unquestionable cryptographic evidence that he did.

643

Excerpts from Secret and Urgent

8. P. 110-116...In the 1870's Russia was ruled by the liberal Tsar Alexander. His reforms progressed too slowly for the radical Nihilists and they passed a solemn sentence of death on him as the one step which would throw the country into a state of terror and re ression. The police succeeded in capturing one of the most important of the revolutionaries, a man named Mikhailoff. A warder who had insinuated himself into his trust was given a bulky document to deliver to the comrades outside; it was an intricately enciphered manuscript which he turned over immediately to the authorities. Broken down, it was nothing more than a long harangue on the woes of the working class, which they allowed to be published. After the Tsar had been killed on his morning trip through a street that had been mined, it was learned that Mikhailoff had smuggled to the assassinators a full set of directions. How? Right under the noses of the police, he had concealed in the enciphered texts that were allowed to go through for publication a very clever second cipher which gave implicit instructions for the murder.

9. P. 122-3...For a brief time during the Thirty Years' War the use of unknown tongues as cipher seems to have risen to the dimensions of a regular system. This device has been tried since. During th great Sepoy Mutiny, British officers made a regular practice of writing messages to one another in straight English, but with Greek characters, and during the Boer War, where few of their opponents had any but the most elementary education, Latin was found thoroughly adequate as a cipher.

10. P. 28...Battles and wars in all times have been decided by the ability of one side to break its enemy's ciphers and codes. In the seventeenth century, the royalists under the Prince of Condé were laying seige to the Huguenot stronghold of Realmont. It looked very much as though the besieged would hold until spring, and by that time Conde's army would be decimated by disease. Just as he was considering raising the seige, a man was caught trying to sneak through the lines and carrying a long, suspiciously bad poem. A nearby mathematician was summoned who by nightfall revealedthat the message really asked the Huguenots in the next town to relieve them with munitions of war, without which they would have to surrender. Condé had a trumpet blown, and under a flag of truce returned the message and its clear to Realmont. Next morning the place surrendered.

11. P.145...Though we are usually more familiar with fiction's use of cryptography, parallels may often be found in real life. Conan Doyle's cipher of the dancing men,which he used so effectively in the Sherlock Holmes story of that name,was also used by the secret society of the Carbonari, in the days of Italy's revolt against Austrian-Spanish rule in the nineteenth century.

12. P. 146...The cipher which is written by substituting musical notes for letters is another conventional device in fiction. Very effective use of it was made in the movie Dishonored, with Marlene Dietrich as the courteous lady spy who rolled out a few magnificent chords on the piano (she had memorized the air), then turned and wrote down the positions of the enemy units on the front, having recorded the words in a musical cipher.

13. P. 146...The diagram cipher has always remained a favorite of the classes which hover along the edges of criminality. In the literature of tramp scrawlings, a circle with a diagonal line through it once meant, "This is a good place to rob," a crudely drawn cat "Woman only in this place," a crudely drawn hammer "You'll have to work for anything you get."

14. P. 151...The greatest diary in English literature was first revealed to us through the skill of the cryptographer. When Samuel Pepys almost wrote his diary during the rule of Charles II, it was done in a hand almost microscopically small and in what appeared to be some type of conventional design cipher which no one who had yet looked at could interpret. It lay in manuscript until the nineteenth century, when the head of Magdalene College at Cambridge assigned the task of deciphering it to a divinity student named John Smith. Some of the messages had first been put into foreign languages, spelled phonetically, then enciphered and finally written in shorthand. John Smith worked over that manuscript for three years, twelve or fourteen hours a day, and the result was probably well worth the labor. (Later, a complete key to the diary was found.)

.644

Excerpts from Secret and Urgent

P. 189...The failure to find a good and workable cipher promptly cost many men their heads. Many men who have been executed tardily died of bad cryptography.

P. 160-161...It was a misunderstood rather than an intercepted dispatch that ruined Napoleon's chances. In the battle of Leipzig, the French had been half-victorious the first day; they were half-defeated the morning of the second day when Napoleon, realizing he could not hold his position, planned a retreat. It was to take place that night; Marshal Augereau was ordered up from the rear with an army corps to build bridges across the river at the army's back and to cover the retirement. The order went in Napoleon's Great Cipher, and Augereau replied in the same. His men had marched long and late on the previous night, he said; he would come, but could not arrive as soon as the Emperor expected. Emergency measures would be needed to hold the lines till his arrival.

The answer reached headquarters, but hopelessly garbled. No one could read it. Neither Augereau nor an explanation of his non-appearance arrived, and the army did nothing in nearly expectation of his coming. Napoleon himself had fallen asleep and nobody dared wake him or give orders without his approval. The Allies broke the French lines, the single bridge behind the army was insufficient. What had been a check turned into a wild rout; the French organization was broken, they lost twenty thousand prisoners and never recovered.

P. 178...Cryptography was first brought out of the Dark Ages by a German officer and an American Southerner. In 1863, Kasiski, a major on the Prussian staff, published the first comprehensive book on cryptography in a century. He did what nobody had been able to do for centuries--gave a method for deciphering the Vigenère tableau. He completed the task of Edgar Allan Poe. Between them they demonstrated that there was not in existence in their time any cipher both practically useful and practically unbreakable. Between them they changed the main stream of cryptography. The early cipherers were more interested in concealing their own messages than in solving those of others; in the age just dawning the center of gravity was shifted to decipherment.

P. 188-89...It took the Franco-Prussian War to reveal publicly that the European powers had for some time been quietly concentrating on decipherment to the neglect of their own secret communications. Bazaine had been driven back into the fortress of Metz with half the French forces by von Moltke. There the Germans laid siege to him; southward, MacMahon and Napoleon III drew in reinforcements and came up to break the circle of the siege. The question was whether the relievers could concert time and place of attack with the besieged and fall in mass on some point in the thinly encircling lines. Metz was set high on the hills, and the bright summer days allowed easy heliograph communication across the summits. Unfortunately, the old diplomatic cipher with "none of the technical terms used in war" was still in use.

Such perfect patterns-words as <u>general, bataillon</u> and <u>artillerie</u> had to be spelled out in simple substitution. Not half a dozen messages had been passed before the Germans had solved the whole thing. They concentrated opposite the spot of MacMahon's drive; Bazaine's sortie was broken, MacMahon dreadfully defeated and driven to the hill of Sedan, where French Army and French Emperor were forced to surrender together.

P. 190...In peacetime, cryptography generally goes to seed. Diplomatic questions are no longer as urgent as during a war. During the more leisurely negotiations of a period of general peace it is possible to send out ambassadors who have received full instructions by hand.

P. 163...The influence of the invention of the electric telegraph on cryptography was tremendous. It was now possible to direct minutely from a home office the steps of a military, diplomatic or commercial manoeuver being carried on at a distance. At the same time, it threw these communications open to the public, for anyone could, in a few hours, acquire the knowledge necessary to read the messages transmitted through the wires. Ciphers became almost obligatory in communications of great public moment.

P. 193...In 1866 the first transatlantic cable was laid. It probably had much to do with the maturity of the full code, which now soon made its appearance. No date or place can be assigned to its debut: codes are an obvious product of the cable with its high rates and emphasis on getting a great deal of meaning

into a very few letters. The commercial code s appear to antedate the military, and almost at once assumed their ultimate form--dictionaries of words and phrases for which in transmission are substituted words or pronounceable groups of letters.

2. P. 194-200...Few people realize that in the famous Dreyfus case the innocence of the unjustly sentenced captain was eventually proved by cryptography. One of the most condemning pieces of evidence was a telegram in numerical code involving Dreyfus with the Italian military attache in Paris, Panizzardi, and sent the day after the Dreyfus story reached the press. The French Army decipherers had managed to break down the code and had read: " Captain Dreyfus has been arrested. The Ministry of War has announced proofs of secrets offered to Germany. If the captain has had no direct dealings with you it would be well to publish a My emissary has been warned.' This with other evidence (later found to was enough to send Dreyfus to prison.

It seems, however, that the cryptoanalysis took place under great and when the French Black Chamber checked their work, the second and true was radically different. It read: 'Captain Dreyfus has been arrested. Ministry of War has announced relations with Germany. If he has had no dealings with you, it would be well to publish a denial to prevent newspaper comment on us. We do not know his here.'

This put an entirely new face on the matter, but when the new evidence was produced, it was suppressed by Colonel Henry, the head of all French (As well he might; his friend Esterhazy was the real scoundrel.) When an prising captain at last reported the fraud to the Minister of War, Colonel cut his throat, Esterhazy was sentenced, and Dreyfus released and honored.

3. P. 201...The year 1890 is a key-date in the history of ciphers. The Prussian and Russo-Turkish wars had showed conclusively that it was no possible for a general to control strategy by aides carrying He must work from the army and his communications must be fast as secret as the grave. They saw, too, that the value of ciphers in communications depended less upon the theoretical qualities of the upon the skill of the operators. 1890 saw this realization every one of the major powers added a course in cryptography to its system of instruction.

4. P. 207...There is no end to the number of complicated machines used in cryptoanalysis. Let's skip them.

5. P. 220...The invention of the wireless showed more emphatic than ever on the necessity of throwing confidential correspondence into cipher, for it is the property of the wireless that it turns over to the enemy a copy of every dispatch.

6. P. 231... The international messengers of pre-World War I were concentrated in Vienna. It was there that Colonel Alfred Redl, head of the Austrian espionage and counter-espionage, was blackmailed into betraying to Russia Austria's war plans for the eastern front, delivering up every Austrian spy in Russia and turning over to the Russians the Austrian military dictionary code. The treason was not discovered till late in 1912, and ultimately had much to do with the frightful Austrian defeats in Galicia during the early part of the war. The Austrian military wireless held no secrets till its whole system was changed in November, 1914.

7. P. 233...It was a Viennese cryptographer who noted that in dispatches sent in clear the diplomats of every gr at power used a certain opening formula--"I have the honor to inform your Excellency". Using it as a probable opening phrase in coded telegrams, he attacked the communications of all the ambassadors with their home governments. All the great powers thought their diplomatic codes so safe they did not bother to change them; their smugness resulted in Vienna possessing code dictionaries almost as good as those the ambassadors themselves used.

6 15

Excerpts from [redacted]

28. P. 234.5...In the first days of the first World War, the whole of the German march through North France became a chronicle of missed opportunities and faulty cooperation, and their bad communications were at the bottom of it. The air was filled with radio traffic, French, British, Belgian, German, often with several instruments working the same wave-length, jamming one another. Whole sections of messages became lost or unintelligible, and the loss of even one lettering in a message composed in the German two-step cipher which involved double substitution as one of its steps, rendered the whole message gibberish. Everything had to be repeated up to five, ten or a dozen times, and even then some of the most important communications failed to get through.

29. P. 236-7...Before the start of the war, the Russians knew very well that the Germans were in possession of their ciphers, but they blandly continued to use them until the very day of the declaration. On that day the one copy of a new cipher came out of hiding, and for some inexplicable reason, was given to but one of the two generals commanding the separate armies invading East Prussia. So signals in the new cipher began to be picked up by German listeners; then messages in the old peacetime cipher. One side had destroyed their copies of the old cipher; the other side did not possess the new one. Soon there were requests on the air from either Russian commander to send the messages in the clear.

Very soon the Germans were apprised that one general was halting his advance for three days, to allow his supply train to catch up. Immediately the other army was encircled, and the three days following became a massacre. This was the Battle of Tannenburg and started Russia on her long gradient into ruin and revolution.

30. P. 238-39...In the battle of naval codes the tables were turned. At one time, early in the war, the German Magdeburg was raiding along the Russian coast. She ran aground during a fog, and when the mists cleared, the Russian fleet was seen bearing down. Just as a German officer reached the deck bearing the secret naval code books, bound in lead, in preparation for taking them as far from the ship as possible and dropping them in the deep water, a huge swell washed him overboard. When the Russians arrived, they ordered the bodies around the ship taken up for burial. The act of humanity was well-rewarded; the code-books, still in the arms of the officer, were one of the first things the dredge brought up.

For the two years following, from the capture of the Magdeburg to the battle of Jutland, the Germans' radio messages at sea were seldom a mystery long. Though they changed keys fast and furiously, it availed them little, for "Room 40" was in possession of their system--which they never changed.

31. P. 242... It was a German wireless code which helped to bring American indignation to the boiling point at the time that a declaration of war was asked. British Intelligence had persuaded a young Austrian with Allied sympathies who was an operator at the Brussels station which disseminated German diplomatic messages all over the world to steal the German code a few words a day and pass it on to an English spy. The Allies' valuable possession was not made public until the time of the Zimmerman message, when the German ambassador was instructed to work up an alliance with Japan to attack the United States with the aid of Mexico, and Mexico was offered three American states as her prize.

32. P. 245...When our government entered the war, we thought we had an answer to the problem of intercepted telephone messages. A number of Choctaw Indians were sent into the trenches to phone messages to one another in their own tongue. The idea was a success in concealing the content of the messages from the Germans, for they had no Choctaw interpreters; but it was too much of a success: The Indians were unable to understand each other over the telephone, and their language held no equivalent for such un-Indian devices as "barrage" "machine gun" and "zero hour".

33. P. 246...Although the Germans changed their naval code after Jutland, they still could not keep their secrets long. Every time a submarine was sunk in waters at all possible for diving operations, men were sent down. Sure enough, the Systematic Teutons kept their code-books in the same place aboard every submarine, and though the work of extracting them was hard and dangerous, British divers got enough of these code-books to keep them well apprised of the latest developments.

647