# HERBERT O. YARDLEY, HEAD OF MI-8 (THE CODES AND CIPHERS BUREAU) AND THE BACON BI-LITERAL, SIMPLE AND KAY CIPHER SYSTEMS REVEALING BACON IS SHAKESPEARE

By A Phoenix

May 2024

# HERBERT O. YARDLEY, HEAD OF MI-8 (THE CODES AND CIPHERS BUREAU) AND THE BACON BI-LITERAL, SIMPLE AND KAY CIPHER SYSTEMS REVEALING BACON IS SHAKESPEARE

During the time Riverbank Cipher Department headed by William and Elizebeth Friedman was carrying out code and cipher work for the US government and various other federal agencies plans had secretly been underfoot in Washington to establish a Cipher Bureau of its own. On 10th June 1917 the first government Cipher Bureau under Military Intelligence 8 (MI-8) was established in Washington by the War Department with Major Ralph H. Van Deman, Director of Military Intelligence, appointing Herbert O. Yardley, as its first head.

In the Summer of 1918 Yardley armed with his letter of introduction from the French High Commission in Washington arranged to meet General Cartier to explain his mission to study the different codes and ciphers encountered and used by the French Signal Corps. After listening to his request Cartier contacted Captain Georges Painvin 'the great cipher genius of France.'[1] The brilliant French cryptanalyst had a legendary reputation as 'the most skilful cryptographer in all the Allied Governments' and Yardley recalled a lecture given by Colonel Frank Moorman, a Staff Officer at American General Headquarters, who unreservedly stated 'Captain Georges Painvin, the chief code expert of the French, an analytical genius of the highest order, was a regular wizard in solving codes.'[2] For much of the war Painvin had served in the office of General Cartier. His single greatest achievement came when he broke the ADFGVX cipher, the notoriously difficult field cipher used by the Germans at the latter end of the war. During the last weeks of the war Friedman was assigned to Painvin's cryptanalytic group to assist the Frenchman on the intercepts of ADFGVX system.[3]

Painvin came to the attention of General Cartier by sending him a memorandum outlining a simplified method of breaking the ABC system used by the Germans in the early stages of the war. In the words of Kahn it marked the beginning of his rise to prominence. The Frenchman Painvin 'was destined to become the Perseus of cryptologists in the epic struggle of World War I, slaying one German cryptographic Gorgon after another.'[4] An excited and slightly awed Yardley was introduced to Painvin by his superior General Cartier. Their shared expertise in cryptology formed the basis of a warm and lasting friendship 'I became an intimate member of his household and spent many quiet evenings there, listening to his brilliant discussion of cryptography', Yardley later recalled with some affection.[5] The great Painvin was also to add to his education, one which Yardley would use to great effect in the years to come:

> Painvin gave me a desk in his office and opened his files to me, and I made the most of the opportunity to study under this master, whose instruction and inspiration were to stand me in good stead, when later, from 1919 to 1929, I directed the energies of a group of cryptographers, deciphering the secret codes and cipher messages of foreign governments.[6]

The French cipher experts Cartier and Painvin must have often discussed the Bacon Bi-literal Cipher with Yardley, the head of the *Cipher Bureau* (MI-8) and no doubt Yardley discussed the Bi-literal Cipher with Friedman with whom Yardley had a very long private and professional relationship. When MI-8 was finally disbanded in October 1929 Yardley wrote *The American Black Chamber* revealing secrets about his time working as a codebreaker for US Intelligence which was published in 1931 and the same year he also wrote a little known and long forgotten article for *The Saturday Evening Post* entitled 'Cryptograms and Their Solution' not mentioned by the Friedmans in *The Shakespearean Ciphers Examined*:

> More has, perhaps been written about the biliteral Baconian cipher, attributed to Lord Bacon, than any other single form of secret communication. In this cipher the entire alphabet may be expressed by the two letters a and b in combinations of five.

A aaaaa B aaaab C aaaba D aabaa E abaaa

F baaaa G baaab H baaba I babaa J bbaaa

K bbaab L bbaba M bbbaa N bbbab O bbbbb

P babba Q babbb R abbbb S aabbb T aaabb

U bbabb V abaab X aabab Y babab Z ababa

One of the theories of the Baconians is that the wise men of the past did not dare write their scientific discoveries for fear of being put to death. Thus they left to posterity their knowledge by means of the biliteral cipher. This was done by using two different kinds of type in printing their literary efforts. This theory flourishes because of the fact that books of this period were actually printed with different-shaped type. Those with thin edges are called *a*'s by the Baconians and those with thicker lines are *b*'s. Thus, if there are four letters with thin edges-*a*'s-and one with heavier lines-*b*-we have *aaaab*, which equals the letter *b* in the biliteral cipher. Continuing in this fashion, many students have given the world some curious readings. Excavations have actually taken place in England for hidden treasure as a result of these decipherments. One reading from the original of one of Shakespeare's plays, if we are to believe the decipherer, is a message from Francis Bacon, who states he is the rightful author and the illegitimate son of Queen Elizabeth. I should add what, no doubt, the reader already knows: The type are different because they were made from imperfect moulds during the early forms of printing, and the so-called *a* letters and the *b* letters are so nearly alike that the decipherer may use his own imagination in his selection. Hence these curious decipherments.[7]

It starts by stating that perhaps more has been written about the Bacon Bi-literal Cipher than any other single form of secret communication. The opening statement is followed by a description of the Bacon Bi-literal Cipher 'the entire alphabet may be expressed by the two letters *a* and *b* in combinations of five'. What it does not say is whether or not this is the same combination of *a* and *b* letters for each letter of the alphabet as originally given by Bacon in *De Augmentis*. It is not. The example given here radically differs from the form in which it was first presented by Bacon. The first three letters of the alphabet in the article A, B, and C, are given the same *a* and *b* combination as given by Bacon. But from D onwards the assignment of *a*'s and *b*'s differs from the combinations given by Bacon. The letter combination in the article for the letter D is the letter for E in the original bi-literal cipher, as is the case for E, F, G, H, I, which in the original bi-literal cipher represented I, R, S, T, W, respectively. Moreover, the letter combinations alongside the letters J, K, L, M, N, O and U in the article find no equivalent in the original given by Bacon. In addition, the illustration in the article does not follow the 24 letter Elizabethan alphabet where I and J and U and V were interchangeable and nor does it follow the modern 26 letter alphabet. The illustration provides only twenty-five letters, completely omitting the letter W. These deviations, are of course, not mistakes but deliberate, done with a definite purpose. This Rosicrucian device of making what seems to be an 'error' is designed to attract the attention of the initiated. Outside the bi-literal illustration in the column directly concerning Bacon and his Bi-literal Cipher the rest of the text ('aaaab' is counted as 5) comprises 287 words Fra Rosicrosse in kay cipher which minus the block 'aaaab' 287-5=282 Francis Bacon in kay cipher. If the number 282 is added to the numerical equivalent of the missing W in simple cipher (21): 282+21=303 which when the null '0' is dropped it leaves 33: Bacon in simple cipher. Thus, we have in a combination of kay and simple cipher Francis Bacon, Shakespeare, Brother of the Rosy Cross.

# CRYPTOGRAMS AND THEIR SOLUTION

(Continued from Page 21)

(TO BE CONTINUED)

rt of Spain and the
in France. The King
who discovered the
phered with fifty dif-
signs, and turned the
ver to His Majesty.
arths learned of this
evenge by accusing the
of having the devil in,
nd denounced Viète as
ck magic before the
ibunal at Rome. For-
ate, he was as clever at
e was at cryptography,
neck by explaining how

eenth century was not
pher experts. During the
King's troops under the
the Prince of Condé, at
Malmont—which was de-
e Huguenots—the Prince
point of withdrawing, due
mined resistance of the de-
en a messenger bearing a
atch from the town was
ine Rossignol, the Prince's
rd, solved the message in
. It was an appeal to the
of Montauban, telling them
arrison was almost out of
, and that the town must
if a supply was not immedi-
. The Prince of Condé re-
e cipher and its solution to
mander of the town, with the
at if conditions were as stated
es of life was scarcely worth
he commander of the garrison
point and surrendered.
(the oldest and simplest ciphers
d in military operations is the
Julius Cæsar cipher. In this
ter of the alphabet is repre-
by another letter of the alpha-
e, two, three, or four spaces,
preceding or following the
l letter. In its simplest form, B
A, C equals B, D equals E, and
Though the invention of this
is attributed to Cæsar, it is
that it was used by the Phœni-
and Carthaginians. It continued
for hundreds of years, and in a
fied form was used by the Ger-
in 1870-71 and by the British
during the South African War.
Allan Poe's Gold Bug is the
famous cryptogram in fiction.
the letters are represented by
ary symbols. This method of se-
communication dates back to the
Egyptians, who used single
ters to disguise treaties on
the author of the famous
may be roundly asserted

that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve," ran a cipher column in his newspaper, defying his readers to devise a cryptogram which he could not read. Just how much Poe knew about the principles of cipher as developed 100 years later, during the World War and after, is not known, but he was clever enough to decipher all messages submitted to him except two which were unfair examples of the art. It is comforting to know that Poe, despite his genius, made mechanical errors. The frequency table for his cipher in the Gold Bug, as originally published, did not agree with the cryptogram. In writing the story, Poe found it necessary to make a slight change in the cryptogram, but failed to make the necessary changes in the frequency table which gave the number of occurrences of each symbol.

### Seeking Ciphers in Shakspere

Philip II. of Spain, in 1572, used a curious-looking cipher for correspondence with his brother, John of Austria. The original is in the archives at Simancas, Spain. It is a large table made up of the letters of the alphabet, consonant-vowel digraphs such as *ba, be, bi, bo, bu,* and common trigraphs such as BLE, CRE, PRE. The cipher symbols are letters and one and two figure combinations modified by ? , . ! and the like. To encipher "cryptography" it is first divided C R Y P TO GRA P H Y, and enciphered equals 1 14 18 9 16? 4.. 9 5 18. I should like to see the modern telegrapher copy this over the wire.

There are extant several hundred cipher pages of the Elizabethan period. In one the Queen of England is "Aries" and the King of Spain, "Scorpio." In another cipher the Pope is "Beware" and the Emperor, "Doubt." Father Creighton and Father Parsons are "Weasel" and "Ferret." In still another cipher we find the Queen Mother as "Mean" and the French King, Henry III., "Ignorant." French cavalry are "ells of velvet," and guns, "barrels of salt."

During the World War we found this same type of secret communication among spies. "Uncle has recovered" is "We are no longer under suspicion," and "Uncle is ill" is "We are under suspicion." Sometimes more definite information is conveyed. "Please go to Seifridge's and buy me six blouses on Friday next" means: "Six raiders will bomb Mannheim on Friday next."

More has, perhaps, been written about the biliteral Baconian cipher, attributed to Lord Bacon, than any other single form of secret communication. In this cipher the entire alphabet may be expressed by the two letters *a* and *b* in combinations of five.



One of the theories of the Baconians is that the wise men of the past did not dare write their scientific discoveries for fear of being put to death. Thus they left to posterity their knowledge by means of the biliteral cipher. This was done by using two different kinds of type in printing their literary efforts. This theory flourishes because of the fact that books of this period were actually printed with different-shaped type. Those with thin edges are called *a*'s, by the Baconians, and those with thicker lines are *b*'s. Thus, if there are four letters with thin edges—*a*'s—and one with heavier lines—*b*—we have *aaaab*, which equals the letter *b* in the biliteral cipher. Continuing in this fashion, many students have given the world some curious readings. Excavations have actually taken place in England for hidden treasure as a result of these decipherments. One reading from the original of one of Shakspere's plays, if we are to believe the decipherer, is a message from Francis Bacon, who states he is the rightful author and the illegitimate son of Queen Elizabeth. I should add what, no doubt, the reader already knows! The type are different because they were made from imperfect molds during the early forms of printing, and the so-called *a* letters and the *b* letters are so nearly alike that the decipherer may use his own imagination in his selection. Hence these curious decipherments.

Count de Mirabeau, French orator and statesman during the French Revolution, invented a very ingenious cipher, especially for that period. It follows:



The order of the letters may be changed at will. In this cipher each letter is represented by two figures. Instead of writing 32, 22, 34; 31, 44, 34 for "cipher," the figures are written in two columns:

| | | |
|---|---|---|
| 3 | 2 | 3 |
| 2 | 2 | 4 |

Since the figures 6, 7, 8, 9, 0 do not occur, these may be used as nulls—figures that have no meaning—in order to disconcert the hostile decipherer. With the use of nulls, the word "cipher" may read 6 3 2 5 3 7 4 3
1 2 2 1 1 2 1 4
The two horizontal lines are now sent as the message: 6325 3743, 1221, 1214. The advantage of this ingenious system is that it has the appearance of code and would, because of this, offer some difficulty of solution.

### Unsolved Codes of the Revolution

The revolutionary ciphers are of varied types, so varied indeed that many writings of Jefferson, Madison and Monroe remain undeciphered, though many attempts have been made to read them. There are also in the Government archives many passages in diplomatic correspondence that still remain a mystery. The attempts at decipherment have been made by historians; to my knowledge, no professional analyst has ever undertaken the task. One of the methods during this period is a table of alphabets used with a key. In a letter to Madison from Edmund Randolph we find: "Let the key word be the name of the Negro boy who used to wait on our common friend, Mr. Jas. Madison." The Negro boy's name was Cupid.

Dictionaries were also used during this period, a numeral indicating the page number, A or B the column, and Roman numerals the line. A code word would then read: "45 A xxiv." Special codes were also made up consisting of letters, syllables, names of persons, places, and the like, and each given a number. This type of small code eventually led to the modern codes used by governments and the business world. Governments, for the most part, are interested in secrecy only. The business world, interested more in economy, uses codes containing 100,000 or more words and phrases which are represented by arbitrary five-letter groups such as *bahad, fakaw, gicod, Slido.* The cable regulations permit ten letters of this type as one chargeable word. The sentence "When can you ship one thousand bags of coffee?" may be encoded: *Slido*—when can you ship?—and *fakaw*—one thousand bags of coffee. *Slido* and *fakaw*, the two code words representing these phrases, are now joined together—*slidofakaw*—and sent as one cable word. Here we have nine words reduced to one.

In written dispatches during the Civil War, the Confederates used arbitrary signs after the manner of the Charlemagne alphabet—shown on

Article written by Herbert O. Yardley head of the US Cipher Bureau (MI-8) conveying the secret message in Kay and Simple Cipher Francis Bacon, Brother of the Rosy Cross, is Shakespeare

SIMPLE CIPHER

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

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

B A C O N

2 1 3 14 13=33

KAY CIPHER

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

27 28 29 30 31 32 33 34 35 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

F R A N C I S B A C O N

32 17 27 13 29 35 18 28 27 29 14 13=282

F R A R O S I C R O S S E

32 17 27 17 14 18 35 29 17 14 18 1 8 31 = 287

REFERENCES

1. Herbert O. Yardley, *The American Black Chamber* (first published in 1931: reprinted at Laguna Hills, California: Aegean Park Press, n. d.), p. 222.

2. Ibid., p. 222-23

3. Ronald W. Clark, *The Man Who Broke Purple* (London: Corgi Books, 1978), p. 59.

4. David Kahn, *The Codebreakers The Story of Secret Writing* (New York: Scribner, 1967, 1996), pp. 304-5.

5. Herbert O. Yardley, *The American Black Chamber* (first published in 1931: reprinted at Laguna Hills, California: Aegean Park Press, n. d.), p. 224.

6. Ibid., p. 224.

7. Herbert O. Yardley, 'Cryptograms and Their Solution', *The Saturday Evening Post*, 21 November 1931, p. 63.