THE TWO HEADS OF FRENCH CIPHER INTELLIGENCE AND THE BACONIAN BI-LITERAL CIPHER DECIPHERED BY ELIZABETH WELLS GALLUP REVEALING BACON IS SHAKESPEARE

By A Phoenix

May 2024

THE TWO HEADS OF FRENCH CIPHER INTELLIGENCE AND THE BACONIAN BI-LITERAL CIPHER DECIPHERED BY ELIZABETH WELLS GALLUP REVEALING BACON IS SHAKESPEARE

From before the turn of the twentieth century there had been a growing consensus among German, and to a lesser extent, Dutch academics that Bacon was in fact the secret author of the Shakespeare works. The endorsement of Gallup's decipherments by General Cartier had the striking effect of vigorously renewing the debate in post war France. Opinion, as it had been in Germany and Holland was divided, with opposing views warmly expressed in numerous articles, some it has to be said more scholarly than others. General Cartier's endorsement of the bi-literal cipher was also not to go unnoticed in the close knit world of cryptology. Two years after his series of articles two French army officers Andre Lange and E. A. Soudart the '*Former heads of the Cipher Bureau at General Headquarters*', published in French a *Treatise on Cryptology*. The historical cryptographic treatise is listed by Professor Galland in *An Historical and Analytical Bibliography of the Literature Of Cryptography*:

This excellent general text on cryptography gives considerable information concerning the history of cryptography, theories of ciphering, examples and methods of deciphering codes, and a bibliographical list of about 100 items, pp. iii-xv. It is one of the best of modern French works on the subject.[1]

This French work originally published in 1925 with a new edition in 1935 is virtually unknown to and unread by the English speaking world and notice of it does not appear in the Friedman's *The Shakespearean Ciphers Examined*. The motivation and purpose for producing *Traite De Cryptographie* were concisely stated by Lange and Soudart senior members of French Cipher Intelligence in their preface:

There exist, to our knowledge, very few works dealing with Cryptography and Decrypting. Several are notable. But, in addition, as such works, to be consulted with profit, require a fairly extensive knowledge of foreign languages, the mass of information which they contain makes them hard to read for those who desire to obtain enough of the general principles to embark upon the details of practice. Besides, none of these books treats the subject in its entirety: Each treats only one of the sides. Outside of a brochure by Kerckhoffs, on military cryptography, published in 1883, which is not up to date as to the systems now in use, we know of no methodical exposition, at once compact and complete, of the science of Cryptography and the art of decrypting.

The work hereinafter given has for its object the bridging of this gap. Ten years spent in cipher work, during the World War at G. H. Q., and after the war for our personal edification, have led us to undertake this task. The complexity of the questions treated has made it necessary for us above all to be clear, and to reject deliberately technical expositions susceptible of making the demonstrations heavy and tiresome. Nevertheless, one will find in the following chapters sufficient information to permit those interested to carry their researches further, notably a bibliography more complete than any heretofore published, together with the publishers of the more important references. The bibliography alone is of inestimable value, most of the works listed being today out of print (unfindable).

We have written this book for the general public, always so open to all that touches on science. We have written it also, more especially, for officers, and, let us add, as much for Reserve officers as for those on the active list. One must not forget that it is the Reserve officers who performed most of the cipher work for the general staffs during the entire period of the World War, and that the Cipher Bureau at G. H. Q. was headed by Reserve officers from February 1917 until demobilization. Those who read this may perhaps in their turn be called to fill the posts which their elders once had the honour to hold. This

TRAITÉ

DE

CRYPTOGRAPHIE

PAR

ANDRÉ LANGE ET E.-A. SOUDART

ANCIENS CHEFS DE LA SECTION DU CHIFFRE
AU GRAND QUARTIER GÉNÉRAL

AVEC 100 TABLEAUX ET ILLUSTRATIONS DANS LE TEXTE

NOUVELLE ÉDITION

PARIS
LIBRAIRIE FÉLIX ALCAN
108, BOULEVARD SAINT-GERMAIN, 108
1935

Tous droits de reproduction, de traduction et d'adaptation
réservés pour tous pays.

book will be, we believe, of some help in their beginnings, and we hope will enable them to avoid the difficulties which we had when we started.

We think that cryptographic studies should be of interest to every Frenchman. The services rendered in the war by decrypting units have shown the worth of cryptanalysis. Since the war, a recrudescence of interest has taken place along these lines. May the explanations to follow bring a modest, but efficacious, contribution to these attractive studies.[2]

The treatise is divided along three distinct lines: historical exposition, cryptography by means of letters and numerals, and cryptography by means of figures and symbols. In the first part devoted to an historical survey of cryptography, on reaching the seventeenth century, the two French authors in summarising General Cartier's articles provided the French reader with a clear concise description and demonstration of the Bacon Bi-literal Cipher. The two French cipher experts acknowledge that most of the information relating to Bacon's cipher is taken from the articles written by General Cartier. They also reveal they were aware that in the eighteenth century, Horace Walpole in "Doutes historiques" (historical doubts) had questioned whether William Shakespeare was the true author of the works bearing his name and that later writers had attributed the Shakespeare works to Bacon before starting with reference to Mrs Gallup's bi-literal decipherments 'The most recent decryptings seem to confirm this hypothesis':[3]

The seventeenth century is the period in history during which cipher reached its highest degree of perfection. It is not a century of inventions, since at this time the great systems were already in existence. The art of cryptography and that of decrypting were nevertheless at this time the object of so great an interest on the part of the kings and princes, that great minds did not scorn to make deep studies of these sciences, and the ciphers of the period acquired in consequence a great reputation for security, since some among them have resisted up to our time all the efforts of cryptanalysts.

In the first half of this century, in the times of Elizabeth, James I, and Louis XIII, lived Bacon, Rossignol, and Cospi. The first, philosopher and savant, as well as politician and orator, has written works in the plain text of which is hidden an enciphered text, of which the decrypting is at present hardly started….

Sir Francis Bacon, Baron of Verulam, better known under the name of Chancellor Bacon or Lord Bacon, member of the Council under Elizabeth, the Lord Chancellor under the reign of James I (1561-1626), was the inventor of a cryptographic system to which he gave his name and by means of which he introduced into his works texts of ciphers. The study of these texts undertaken many years ago by specialists and continued in our time under the direction of General Fabyan, U.S.A., has brought out results which have recently been revealed by General Cartier, and tend to bring in a new light on an historical problem which has long occupied public opinion, namely the possible identification of Lord Bacon with William Shakespeare.

The process of Lord Bacon was first mentioned by him in the 1605 edition of his work "Advancement of Learning" which consisted of only two volumes, and was described very explicitly in the larger edition of 1623 of the same work, published in Latin under the Title "De dignitate et augmentis scientiarum," comprising nine volumes. General Cartier thinks that at the time of the first publishing, Bacon, fearing that the discovery of his cipher might cost him his head-the English tribunals, at this time, considered the mere fact of having corresponded in secret characters as an aggravating circumstance-preferred not to mention his system except in vague terms without describing its characteristics. Eighteen years later, experience having shown him that nobody had appeared to doubt the explanation which he had made of his cipher and desiring that the story which he had hidden with so much care and which one recognized to be the secret history of his life and of his time, should not

the English tribunals, at this time, considered the mere fact of having corresponded in secret characters as an aggravating circumstance—preferred not to mention his system except in vague terms without describing its characteristics. Eighteen years later, experience having shown him that nobody had appeared to doubt the explanation which he had made of his cipher and desiring that the story which he had hidden with so much care and which one recognized to be the secret history of his life and of his time, should not remain forever unknown, he gave a detailed description of a cipher called by him "biliteral" cipher, accompanied by very explicit example, so that there should be no doubt on the manner in which it should be used. Here is adescription of this cipher, similar to that which Bacon used to encipher his disclosures:

CIPHER TABLE OF LORD BACON (1603)

A—aaaaa	G—aabba	N—abbaa	T—baaba
B—aaaab	H—aabbb	O—abbab	U ou V—baabb
C—aaaba	I ou J—abaaa	P—abbba	W—babaa
D—aaabb	K—abaab	Q—abbbb	X—babab
E—aabaa	L—ababa	R—baaaa	Y—babba
F—aabab	M—ababb	S—baaab	Z—babbb

The system consists of two successive operations:

First, encipherment of the plain text to render it invisible, in replacing each letter of this text by a group of 5 letters, taken from the cipher table which was established by combining in 24 different ways (as many times as there are letters in the English alphabet) any 2 letters of the alphabet, for example "a" and "b".

TYPOGRAPHICAL ALPHABETS "A" AND "B" OF LORD BACON [1]

CAPITALS		LOWER CASE	
Alphabet	Alphabet	Alphabet	Alphabet
"a"	"b"	"a"	"b"
A	A	a	a
B	B	b	b
C	C	c	c
D	D	d	d
E	E	e	e
F	F	f	f
G	G	g	g
H	H	h	h
I	I	i	i
K	K	k	k
etc.			

[1] See Mercure, No. 581, pp. 296–297, for the true alphabets.

Second, insertion of the enciphered text so obtained in the visible plain text, by replacing each of the letters "a" and "b" composing the 5 letter groups of the enciphered text, by the letters of 2 different typographical alphabets, 1 alphabet for the letter "a," and 1 for the letter

"b," the alphabets being such that the difference between the characters was perceptible only to the eyes of the initiated, the visible plain text presenting a harmless appearance to the uninitiated.

As one may imagine, the differences between the letters of the "a" and "b" alphabets are so small that it is impossible, if one has not been initiated, to suspect in the visible plain text the existence of a second text.

Here is an English text as an example:

"In all duty or rather piety towards you I satisfy every body except myself" in which we desire to insert the following hidden plain text:

"All is lost."

We construct the following table, with the understanding that for ease in reading we shall represent, in the visible text, the letters of the "a" alphabet by lower-case letters and those of the "b" alphabet by capital letters:

a	l	l	i	s
a a a a a	a b a b a	a b a b a	a b a a a	b a a a b
i n a l l	d U t Y o	r R a T h	e R p i e	T y t o W

l	o	s	t
a b a b a	a b b a b	b a a a b	b a a b a
a R d S y	o U I s A	T i s f Y	E v e R y

In recopying the true typographical alphabet, we obtain the following text:

"in all duty or rather piety towards you I satisfy every"

. . . . . .

in which, at first sight, and if typographical necessities had not required us to underline with a dot the letters of the "b" alphabet, it would be impossible to suspect the existence of a cryptogram.[3]

The process of Lord Bacon has been mentioned by Kluber,[4] Vesin,[5] and Fleissner von Wostrowitz.[6] A hundred years later (1685), a German author Frederici [7] described a similar system, of which he stated that he was not the inventor and of which the original, according to him, dated back to a period before that of Bacon. In reality, this system is that of Bacon's, slightly modified, and in which by means of the use of 3 forms of characters "a" "c" and "t" grouped in 3's, the visible plain texts necessary to hide the invisibile texts are much shorter.[8] Here, as an example, is the cipher table of Frederici (1685).

---

[3] The text of the above example was taken from the 1857 Latin edition of Bacon's "De dignitate et augmentis scientiarum" published at London. It was reproduced in the article of General Cartier cited above.

[4] "Kryptographik, Tubingue, 1809 (J. B. Cotte)."

[5] "Crptographie devoilee," Paris, 1857.

[6] "Handbuch der Kryptographie" Wien, 1881 (Vienna).

[7] "Cryptographia oder Geheime Correspondenz" Hambourg, 1685.

[8] "Cardan (1557), Vigenere (1587), Selenus (1624), and John Wilkins (1641) have described similar systems.

remain forever unknown, he gave a detailed description of a cipher called by him "bilateral" cipher, accompanied by very explicit example, so that there should be no doubt on the manner in which it should be used….

The process of Lord Bacon has been mentioned by Kluber, Vesin, and Fleissner von Wostrowitz. A hundred year later (1685), a German author Frederici described a similar system, of which he stated that he was not the inventor and which the original, according to him, dated back to a period before that of Bacon. In reality, this system is that of Bacon's slightly modified….

Bacon's system, according to the data given by Gen. Cartier, was used by Bacon in his "Novum Organum" and in the works of his contemporaries, Bright, Burton, Peele, Spenser, Ben Jonson, and Shakespeare. According to recent information, the decrypting done on the above texts by Mrs. Gallup and Mrs. Wells will have brought to light a "Life of Bacon," by himself, containing matter of the greatest interest concerning the history of England at the time of Elizabeth and concerning the true identity of Shakespeare.

Frederici's system, besides, would have served to encipher the inscription of 1616, on Shakespeare's original tombstone, in the church at Stratford-on-Avon.

…The systems of Bacon and Frederici are double substitutions of which the only difficulty, once the key is known, is the identification of the typographical character used. The operations of encipherment and decipherment, theoretically simple, are in practice extremely long and complicated, which explains the difficulties which the cryptanalysts have had to overcome and the time which it has taken them to obtain results….Let us add that the researches should not be limited to the books printed in England at the time of Bacon and Shakespeare, but should cover as well the editions of the seventeenth century, which reveal upon minute examination the different typographical forms which are the base of the above-mentioned cryptographic systems.[4]

1. Joseph S. Galland, *An Historical and Analytical Bibliography of the Literature of Cryptology* (Evanston, Northwestern University, 1945), p. 108.

2. Andre Lange and E. E. Soudart, *Treatise on Cryptography An English Translation Of The Original Traite De Cryptographie* (Laguna Hills, California, Aegean Park Press, 1981), preface.

3. Ibid., p. 15.

4. Ibid., pp. 12-15.