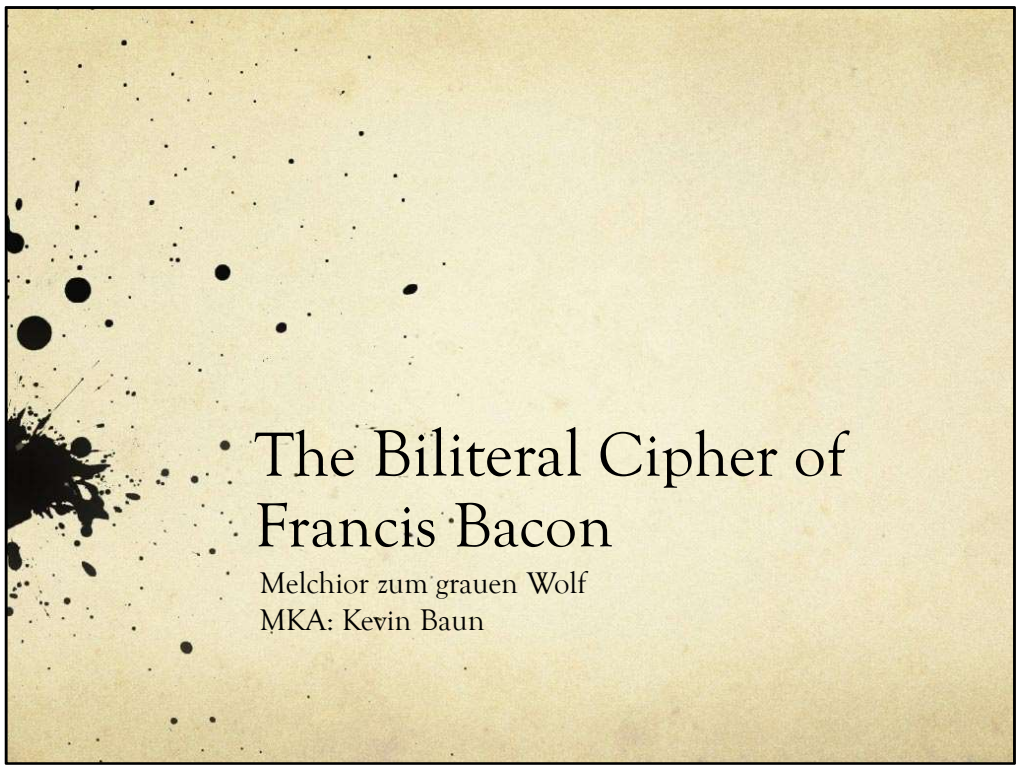


Thank you for your interest in learning more about the Biliteral Cipher of Francis Bacon. I may be reached at melchior@houseblueheron.com if you have any questions, comments, or generalized plans for global domination.

This document is available via my website (http://crypto.houseblueheron.com/). I welcome your comments or questions.

Outline

- Who was Francis Bacon?
- Who was Francis Bacon, REALLY?
- Foundation Ciphers
- What is the biliteral cipher?
- How do you en/decrypt a message using this cipher?
- Potential uses & modern adaptation.
- References.

Before we can address the bilateral cipher itself we need to briefly touch on who Francis Bacon was, was not, and some of the factors around his life leading to his use of and development of secret writing.

As we will discuss, Bacon mentions several different categories of cipher before outlaying this particular system of writing. Most, if not all, of those systems were not inventions of Bacon but they clearly influenced his thinking and need to be addressed, at least in a cursory manner, to have a full understanding of how more complex systems, such as the bilateral ciphers work.

The second half of this document describes the biliteral cipher in detail and provides some simple examples of how to use it.

Who was Francis Bacon?

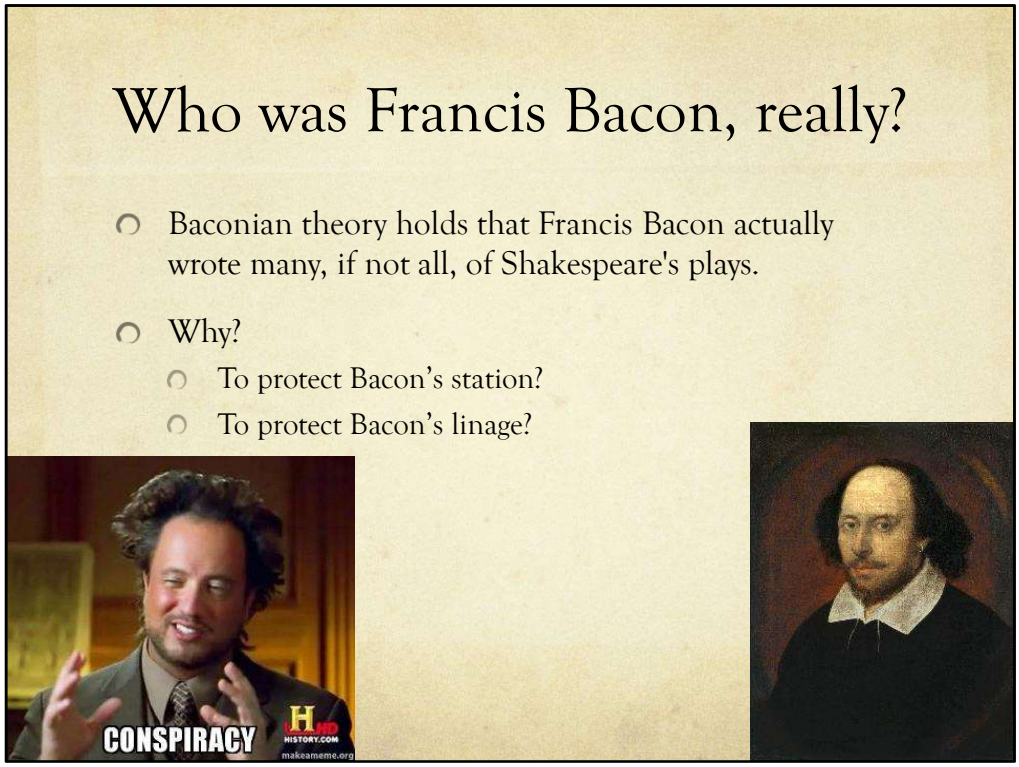
- English poly-math and nobleman.
- Born 1561. Died 1626 (Pneumonia)
- PROLIFIC writer
  - Science
  - Philosophy
  - Religion
  - Judicial
- Leading figure in establishing the New World colonies & some of Canada.
- President of Rosicrucian fraternity .....

(22 January 1561 – 9 April 1626)

Bacon was, unquestionably, a person of note and renown. What follows are just a few of his accolades: appointed to the Queen's council (1597), knighted (James I - 1603), Attorney General (1613), Regent of England (briefly in 1617), Lord Chancellor (1618), Baron Verulam (1618), 1st Viscount St Alban (1621). Being a prominent member of both Elizabeth and James' courts he also published a tremendous amount of material. Much of it related to his work as a jurist, however, he also wrote at length on other topics such as: philosophy, statesmanship, science, and yes, cryptography.

Strong advocate of the scientific method, remember that that early 1600 was a time of tremendous growth in scientific thought. His writings on science and the power of direct experience. He is now thought of as the father of empiricism[1] (idea that knowledge comes from actually experiencing it with your senses) this is one of the foundational schools of thought in epistemology along with rationalism, and skepticism.

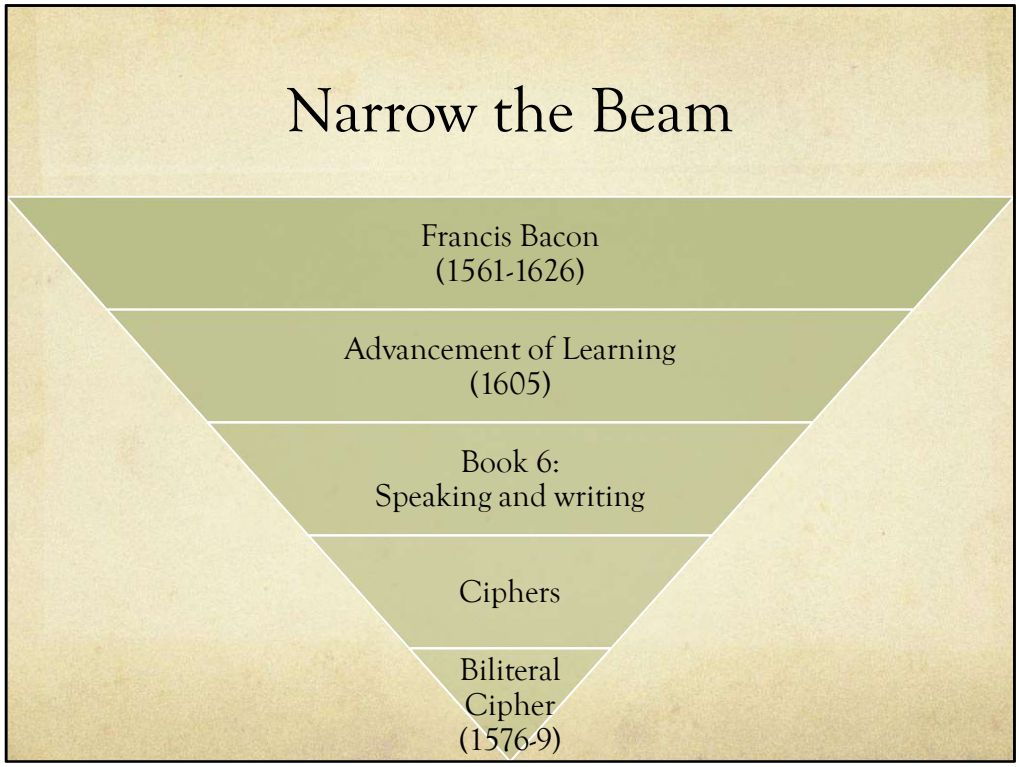
1) This is normally someplace I would put a citation but if you open literally any textbook on the topic of scientific method or philosophies you will find this kind of notation on Bacon. As such it is considered to be common knowledge within the field. I'm happy to provide direct references if you like. ☺



Mark Twain was on board, see essy ‘ Is Shakespeare Dead?’
Friedrich Nietzsche, see ‘"NIETZSCHE on the Shakespeare Authorship".’

“Orville Ward Owen and Elizabeth Wells Gallup: Owen's book Sir Francis Bacon's Cipher Story (1893–95) claimed to have discovered a secret history of the Elizabethan era hidden in cipher-form in Bacon/Shakespeare's works. The most remarkable revelation was that Bacon was the son of Queen Elizabeth. According to Owen, Bacon revealed that Elizabeth was secretly married to Robert Dudley, Earl of Leicester, who fathered both Bacon himself and Robert Devereux, 2nd Earl of Essex, the latter ruthlessly executed by his own mother in 1601.[15] Bacon was the true heir to the throne of England, but had been excluded from his rightful place. This tragic life-story was the secret hidden in the plays.

Elizabeth Wells Gallup developed Owen's views, arguing that a bi-literal cipher, which she had identified in the First Folio of Shakespeare's works, revealed concealed messages confirming that Bacon was the queen's son.”
- https://en.wikipedia.org/wiki/Baconian_theory_of_Shakespeare_authorship



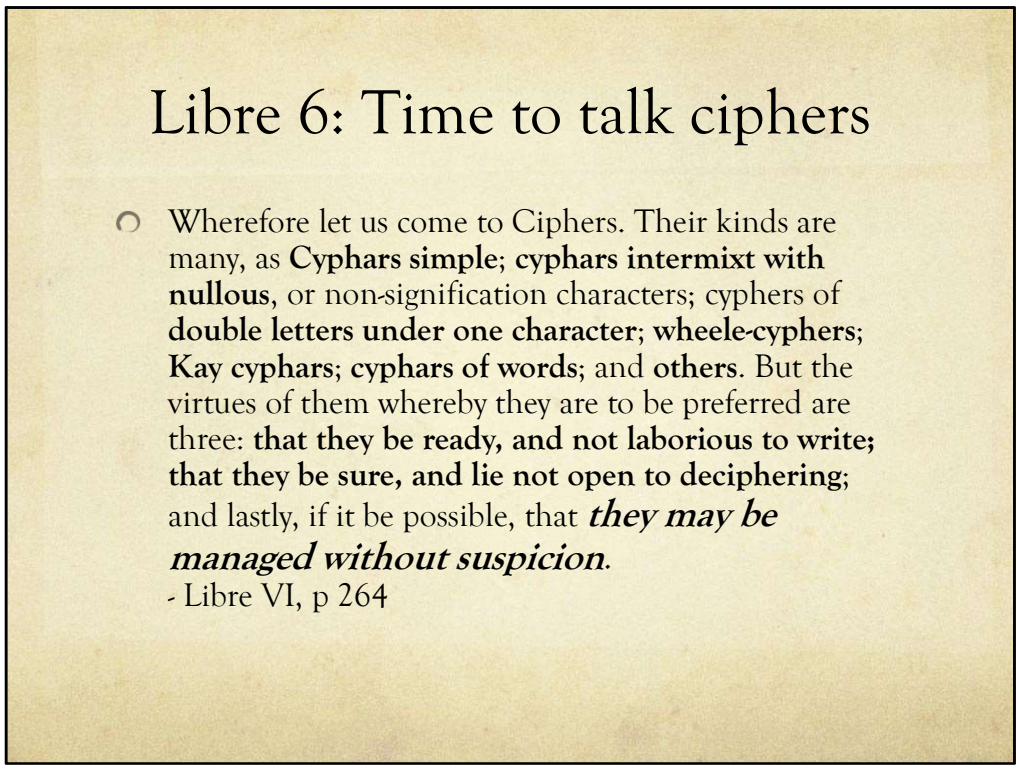
OK. Now that we know a little bit about who Francis Bacon was and the circles he moved in we will narrow the focus of the discussion to that of the specific cipher in question.

We will/have discussed the person, his seminal work, touch on the chapter of interest, then focus in on both the ciphers and the specific ciphers of interest.

Then we will narrow in on the biliteral cipher itself.

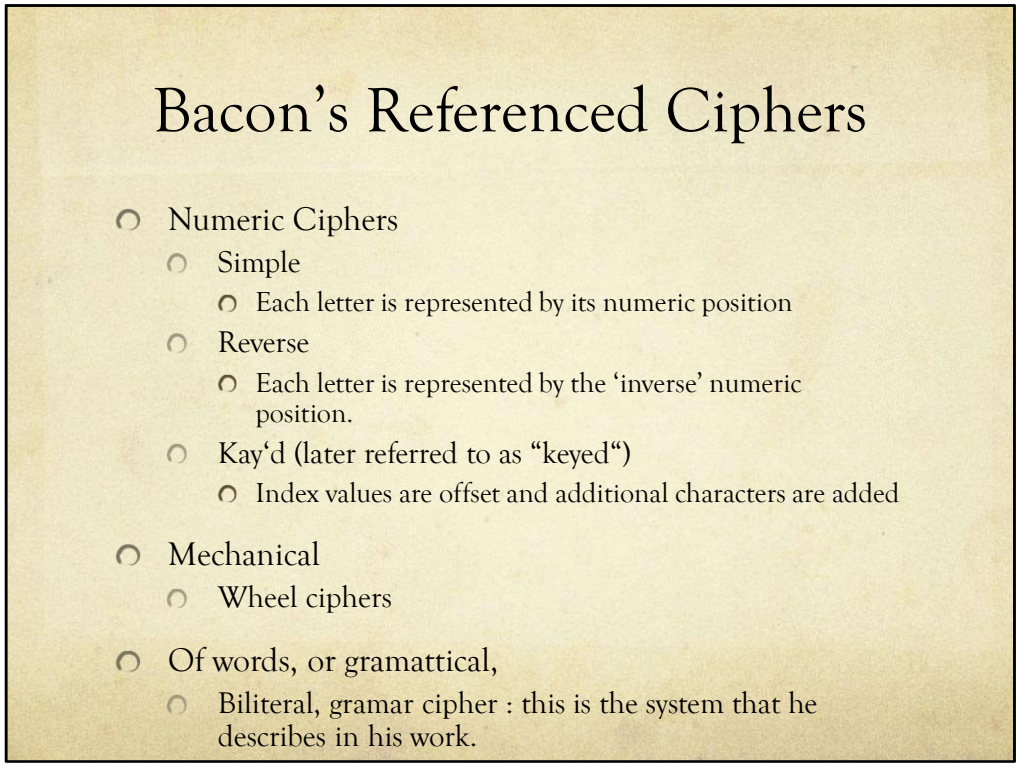
Here we have the frontispiece and dedication page from the 1640 edition of The Advancement of Learning. The 9 books contained within cover a wide range of topics in philosophy, science, courtly behavior, etc but Bacon wastes no time letting us know that we are working in a world of codes. For example: each of these pages contains 287 characters. Likewise, page 287 (“mis-numbered” as 215) also contains 287 characters. Using the Kay cipher, to be discussed in a few more pages, 287 is the value of ‘Fra. Rosi. Crosse.’

This is a fairly typical example of how Bacon is believed to hidden messages throughout his works. It is my personal opinion that early researchers of Bacon suffered a degree of cognitive awareness bias. In brief: humans have amazing pattern matching computers inside our skulls and once we have a precomputed ‘model’ of what to look for we are much more likely to be aware of it.



In modern language this reads:

Now let us speak of ciphers. There are many kinds of ciphers: simple, intermixed with null or un-used characters, where single characters take the place of multiple characters, wheel ciphers, kay cyphers, ciphers of words themselves and many others. There are three things that make a good cipher: ready & easy to write, strong, and clandestine.



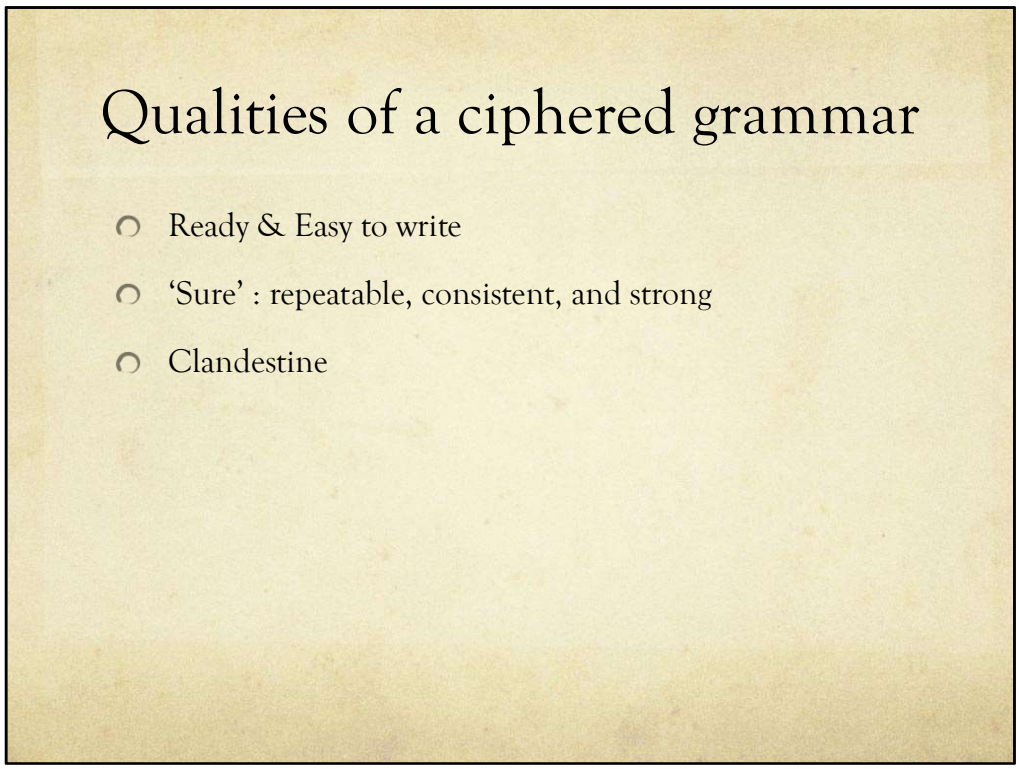
https://en.wikipedia.org/wiki/Bacon%27s_cipher

Later editions refined this method, expanding the alphabet and such, but the basic idea is the same.

Yes the letters are in plain sight but you still need to know the mechanism of decipherment.

K = 10 ... Z = 24, & = 25, et = 26, A = 27, I/J = 35

Numeric ciphers have been around since at least the ancient kabbalists used such systems to calculate the names of angels and such (see atbash & gemateria)



§ Wherefore let us come to Ciphers. Their kinds are many, as Cyphars simple; cyphars intermixt with nullous, or non-signification characters; cyphers od double letters under one character; wheele-cyphers; Kay cyphars; cyphars of words; and others. But the virtues of them whereby they are to be preferred are three: **that they be ready, and not laborious to write; that they be sure, and lie not open to deciphering**; and lastly, if it be possible, that **they may be managed without suspition**.

Simple Cipher

- A = 1 … Z = 24
  - Remembering that I/J and U/V are single values.
  - A T LAN T I A
  - 1 19 11 1 13 19 9 1

A	B	C	D	E	F	G	H	I/J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U/V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24

We see this outlined in detail in Johannes Trithemius's 1499 work Steganographia, being the first part (prelude?) Of Polygraphia, the first work published in the west to be dedicated to cryptography.

Reverse Cipher

- A = 24 … Z = 1
  - Remembering that I/J and U/V are single values.
  - A T L A N T I A
  - 24 6 14 24 12 6 16 24

A	B	C	D	E	F	G	H	I/J	K	L	M
24	23	22	21	20	19	18	17	16	15	14	13
N	O	P	Q	R	S	T	U/V	W	X	Y	Z
12	11	10	9	8	7	6	5	4	3	2	1

The modern 26 character alphabet works just fine using this technique

Kay'd Cipher

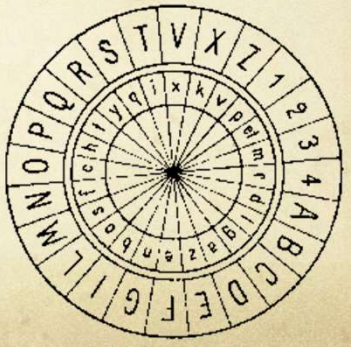
A	B	C	D	E	F	G	H	I/J	K	L	M	N
27	28	29	30	31	32	33	34	35	10	11	12	13
O	P	Q	R	S	T	U/V	W	X	Y	Z	&	ET
14	15	16	17	18	19	20	21	22	23	24	25	26

Notice the use of the two extra characters.

1466 – Alberti, cipher disk

- 'Tattati in cifra'
- Polyalphabetic cipher
- Remained unbroken until the 1800s
- Confederates used this same tech.

A Confederate cipher disk. (Courtesy of The Museum of the Confederacy, Richmond, Vir-



"Wheeled" ciphers, as described by Bacon were described in detail by Alberti. This is a mechanism for encoding and decoding based on offsets, or in this case the rotation of alphabets, physically, withinthemselves.

http://www.recursive.nl/papers/telematica.html
https://cryptome.org/jya/cydisk.htm

Primary Source (1605 - Latin)

nec etiam adhuc visa nobis res digna est, quæ pereat. Habet enim gradum ciphræ altissimum: nimirum ut *omnia per omnia* significari possint: ita tamen, ut scriptio quæ involvitur, quintuplo minor sit, quam ea cui involvatur: Alia nulla omnino requiritur conditio, aut restrictio. Id hoc modo fiet. Primo, universæ literæ *Alphabeti* in duas tantummodo literas solvantur, per transpositionem earum. Nam transpositio duarum literarum, per locos quinque, differentiis triginta duabus, multo magis viginti quatuor, (qui est numerus *Alphabeti* apud nos) sufficiet. Hujus *Alphabeti* exemplum tale est.

Exemplum *Alphabeti Biliterarii*.

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

Neque leve quiddam obtinet hoc modo perfectum est. Etenim ex hoc ipso patet modus, quo ad omnem loci distantiam, per objecta, quæ vel visui, vel auditui subjici possunt, sensa animi proferre, & significare liceat: si modo objecta illa duplicis tantum differentiæ capacia sint, veluti per campanas, per buccinas, per flammeos, per sonitus tormentorum, & alia quæcunque.

cunque. Verum ut inceptum persequamur, cum ad scribendum accingeris, Epistolam interiorem in *Alphabetum* hoc *Biliterarium* solves. Sit epistola interior,

Exemplum *Solutionis*.

F	V	G	E
Aabab.	*baabb.*	*aabba.*	*aabaa.*

Præsto simul sit aliud *Alphabetum biforme*, nimirum, quod singulas *Alphabeti communis* literas, tam capitales, quam minores, duplici forma, prout cuique commodum sit, exhibeat.

Exemplum *Alphabeti biformis*.

F	V	G	E
aabab.	*baabb.*	*aabba.*	*aabaa.*

Manere te volo donec venero.

Tum demum epistolæ interiori, jam factæ *biliteratæ*, epistolam exteriorem *biformem* literatim accommodabis, & postea describes. Sit epistola exterior;

Manere te volo, donec venero.

Exemplum *Accommodationis*.

N	O	P	Q
abbaa.	*abbab.*	*abbba.*	*abbbb.*
R	S	T	V
baaaa.	*baaab.*	*baaba.*	*baabb.*
W	X	Y	Z
babaa.	*babab.*	*babba.*	*babbb.*

Apposuimus etiam exemplum aliud largius ejusdem ciphræ, *scribendi omnia per omnia*.

Epistola interior, ad quam delegimus *Epistolam Spartanam*, missam olim in Scytale.

Perdita res. Mindarus cecidit. Milites esuriunt. Neque hinc nos extricare, neque hic diutius manere possumus.

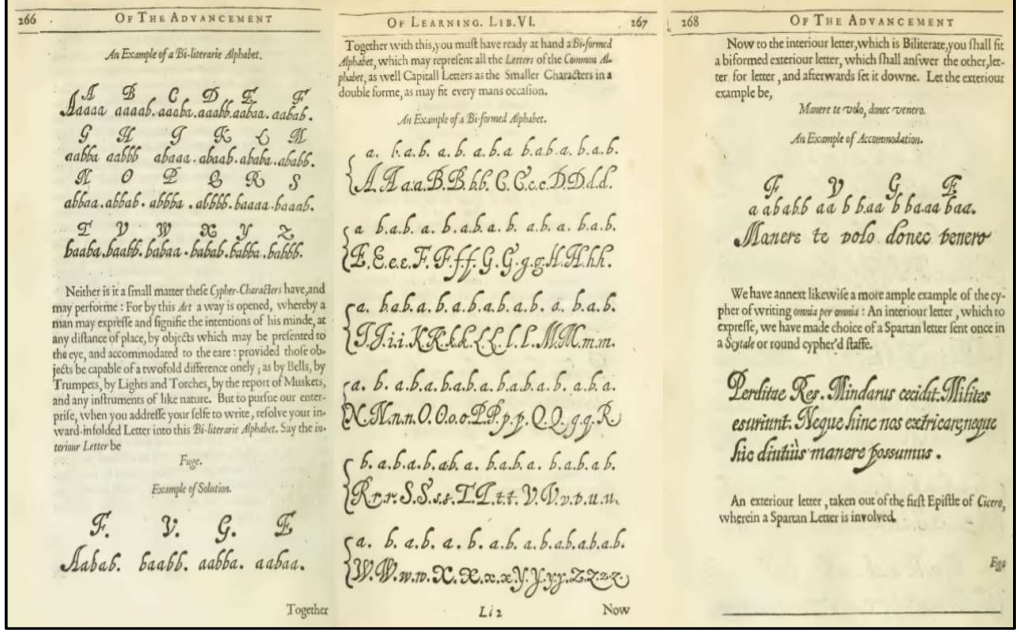
a. b. a. b. a. b. a. b. a. b. a. b. a. b. A. A. a. a. B. B. b. b. C. C. c. c. D. D. d. d. a. b. a. b. a. b. a. b. a. b. a. b. a. b. E. E. e. e. F. F. f. f. G. G. g. g. H. H. h. h. a. b. a. b. a. b. a. b. a. b. a. b. a. b. I. I. i. i. K. K. k. k. L. L. l. l. M. M. m. m. a. b. a. b. a. b. a. b. a. b. a. b. a. b. a. b. N. N. n. n. O. O. o. o. P. P. p. p. Q. Q. q. q. a. b. a. b. a. b. a. b. a. b. a. b. a. b. R. R. r. r. S. S. s. s. T. T. t. t. V. V. v. v. a. b. a. b. a. b. a. b. a. b. u. u. W. W. vv. vv. X. X. x. x. a. b. a. b. a. b. a. b. Y. Y. y. y. Z. Z. z. z.

Epistola exterior, sumpta ex epistola *prima Ciceronis*, in qua *epistola Spartana* involvitur.

Ego omni officio, ac potius pietate erga te, cæteris satisfacio omnibus. Mihi ipse nunquam satisfacio. Tanta est enim magnitudo tuorum erga me meritorum, ut quoniam tu, nisi perfecta re, de me non conquieseris; ego, quia non idem in tua causa efficio, vitam mihi esse acerbam putem. In causa hac sunt. Ammonius Regis Legatus aperte pecunia nos oppugnat. Res agitur per eosdem creditores, per quos, cum tu aderas, agebatur. Regis causa, si qui sunt qui velint, qui parati sunt, omnes ad Pompejum rem deferri volunt. Senatus Religionis calumniam, non religione, sed malevolentia,

https://archive.org/details/dedignitateetaug00bacguat
De_augmentis_scientiarum.pdf
Alphabeti Biliterarii
Libre VI

Primary Source (1640 - English)



266 OF THE ADVANCEMENT

An Example of a Bi-literarie Alphabet.

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

Neither is it a ſmall matter theſe *Cypher-Characters* have, and may performe: For by this *Art* a way is opened, whereby a man may expreſſe and ſignifie the intentions of his minde, at any diſtance of place, by objects which may be preſented to the eye, and accommodated to the eare: provided thoſe objects be capable of a twofold difference onely; as by Bells, by Trumpets, by Lights and Torches, by the report of Muskets, and any inſtruments of like nature. But to purſue our enterpriſe, when you addreſſe your ſelfe to write, reſolve your inward-infolded Letter into this *Bi-literarie Alphabet*. Say the *interiour Letter* be

Fuge.

Example of Solution.

F. V. G. E.
aabab. baabb. aabba. aabaa.

Together

OF LEARNING. LIB. VI. 267

Together with this, you muſt have ready at hand a *Bi-formed Alphabet*, which may repreſent all the *Letters* of the *Common Alphabet*, as well Capitall Letters as the Smaller Characters in a double forme, as may fit every mans occation.

An Example of a Bi-formed Alphabet.

a. b.a.b. a. b. a.b.a b.a.b.a. b.a.b.
A.A a.a.B.B b.b. C.C c.c.D.D d.d.

a b.a.b. a. b.a.b.a. b. a.b. a. b.a.b.
E.E e.e.F.F f.f. G.G g.g.H.H h.h.

a. b.a.b.a. b.a.b.a.b. a. b.a.b.
I.I i.i.K.K k.k.L.L l.l.M.M m.m.

a. b. a.b.a.b.a.b.a.b.a.b. a.b.a.
N.N n.n.O.O o.o.P.P p.p.Q.Q q.q.R.

b.a.b.a.b.a.b. a. b.a.b.a. b.a.b.a.b.
R.r.S.S s.s.T.T t.t. V.V v.v.u.u.

a. b. a.b. a. b. a.b. a.b.a.b.a.b.
W.W w.w.X.X x.x.Y.Y y.y.Z.Z z.z.

Li 2 Now

268 OF THE ADVANCEMENT

Now to the interiour letter, which is Biliterate, you ſhall fit a biformed exteriour letter, which ſhall anſwer the other, letter for letter, and afterwards ſet it downe. Let the exteriour example be,

Manere te volo, donec venero.

An Example of Accommodation.

F V G E
a ab abb aa b baa b ba.aa baa.
Manere te volo donec venero

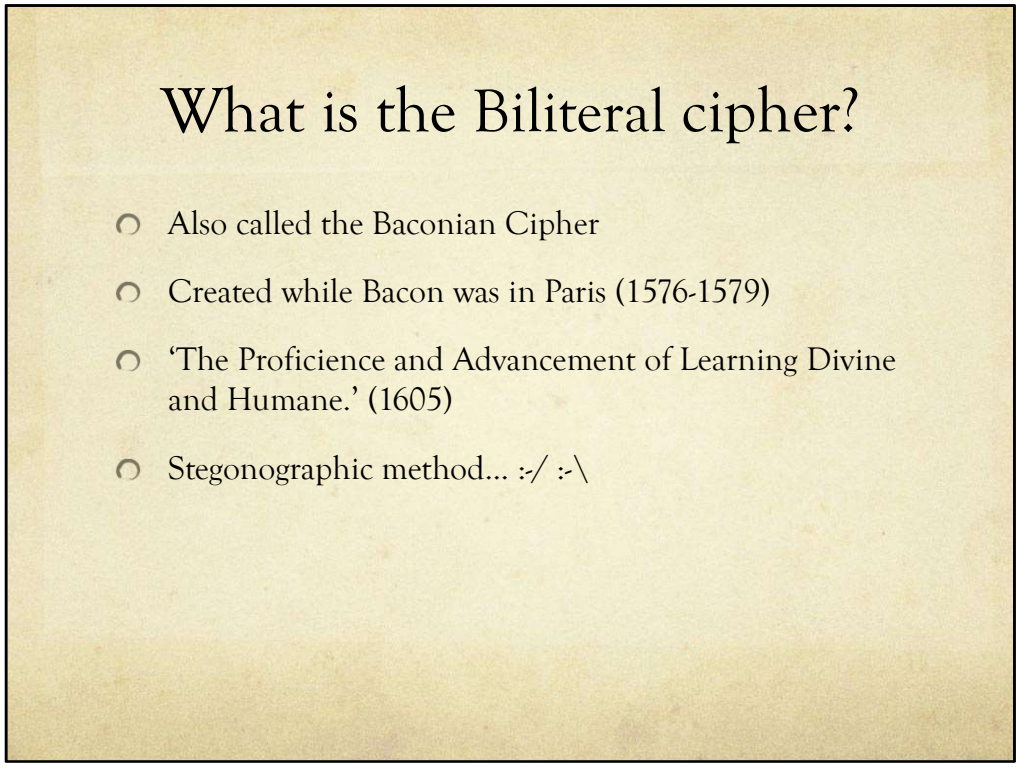
We have annext likewiſe a more ample example of the cypher of writing *omnia per omnia*: An interiour letter, which to expreſſe, we have made choice of a Spartan letter ſent once in a *Scytale* or round cypher'd ſtaffe.

Perditae Res. Mindarus cecidit. Milites eſtriunt. Neque hinc nos extricare, neque ſic diutiùs manere poſſumus.

An exteriour letter, taken out of the firſt Epiſtle of *Cicero*, wherein a Spartan Letter is involved.

Epa

https://archive.org/details/ofadvancementp00baco
ofadvancementp00baco.pdf
Libre VI
- 257 (375)



https://en.wikipedia.org/wiki/Bacon%27s_cipher

Later editions refined this method, expanding the alphabet and such, but the basic idea is the same.

Yes the letters are in plain sight but you still need to know the mechanism of decipherment.

A quick note on binary

- "for the transposition of two letters by five placeings will be sufficient for 32 Differences, [...]"
- A 5 bit binary number
  - 11111 =
    - 16 + 8 + 4 + 2 + 1 =
      - 31 + 1 (zero)
- So, while he did not present it as a mathematical system he clearly understood the mechanism and so beat Leibniz to the creation of 'binary' by 100 years.

It's not necessary to fully understand binary math, as will be discussed later, however this is the system used to define the cipher 'space' so it's worth a quick refresher.

Cheat Sheet

Letter	Script Pattern	Binary
A	aaaaa	00000
B	aaaab	00001
C	aaaba	00010
D	aaabb	00011
E	aabaa	00100
F	aabab	00101
G	aabba	00110
H	aabbb	00111
I, J	abaaa	01000
K	abaab	01001
L	ababa	01010
M	ababb	01011
N	abbaa	01100
O	abbab	01101
P	abbba	01110
Q	abbbb	01111
R	baaaa	10000
S	baaab	10001
T	baaba	10010
U, V	baabb	10011
W	babaa	10100
X	babab	10101
Y	babba	10110
Z	babbb	10111

This chart shows the letter to be enciphered, Bacon's code (which can be read as 'use alphabet a, b, a, a, a) and the binary representation of those alphabets.

Bacon is credited in some circles with the first binary system, as you can see using the above chart. Gottfrid Leibniz, however, is officially credited with the popular base 2 system as he is the first to publish it as its own counting system (1689) in 'Explication de l'Arithmétique Binaire.' Parallels are then drawn through the I Ching, which is a long story and worthy of its own time and place.

It is suffice to say that while Bacon made use of the binary system described here he did not acknowledge it as its own system of counting or arithmetic.

How does encryption work?

- Convert letters into binary representation.
- Find a new message of equal length to the total number of characters in the binary representation.
- Use a different type for the 'Ones' and the 'Zeros'.
- A = aaaaa : A= 00000 : coder
- B = aaaab : B= 00001 : coder
- Run :: Down for the count.
- baaaa baabb abbaa : down for the count

Here I use a color as the first example. It's worth pointing out that the Owen Ellis theories heavily lean on the coloring of type in early printings of Shakespear.
The second example uses another obvious set of types but this time the

How does decryption work?

- Break the message up into groups of 5 characters.
- Check the type of each character to determine is you have a 'One' or a 'Zero'.
- Reestablish the 5 char 'chucks'
- Reconstruct the message.

down for the count it is time to stay put now

As discussed in the intro.

Did you see it?

down for the count it is time to stay put now

down f**o**r t**he** c**ou**nt it is t**i**m**e** to stay p**u**t **no**w

baaa aba abb abbaa aa aa abab aa aaaa aba bba

baaaa baabb abbaa aaaaa babaa aaaaa babba

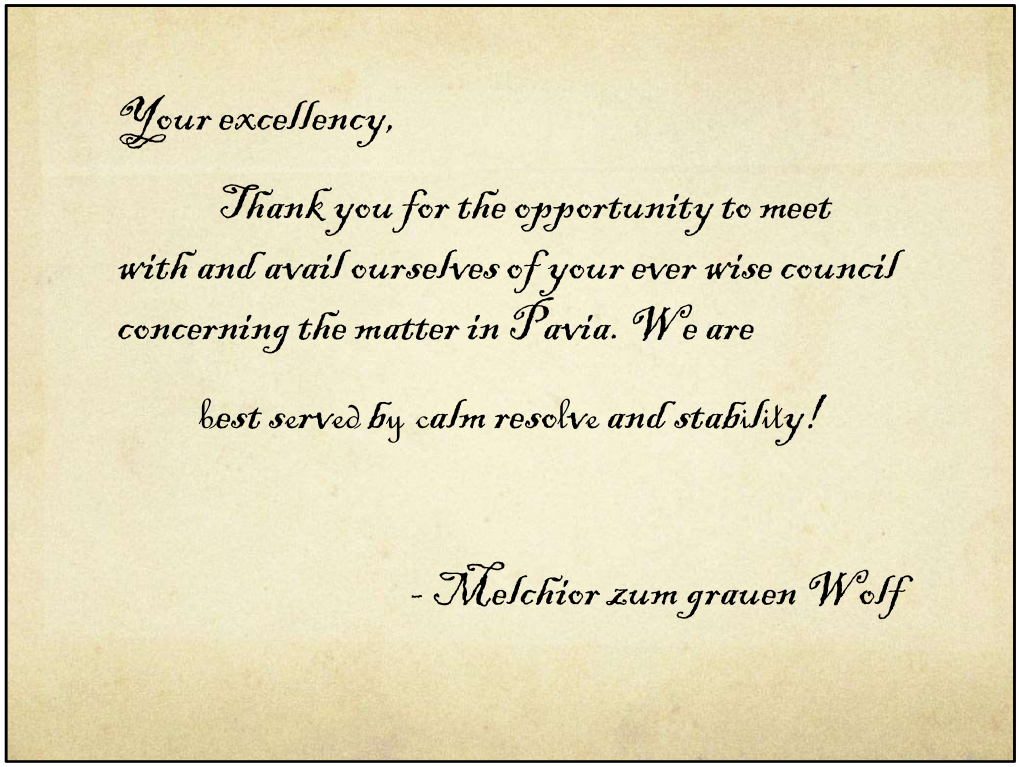
run away

run away

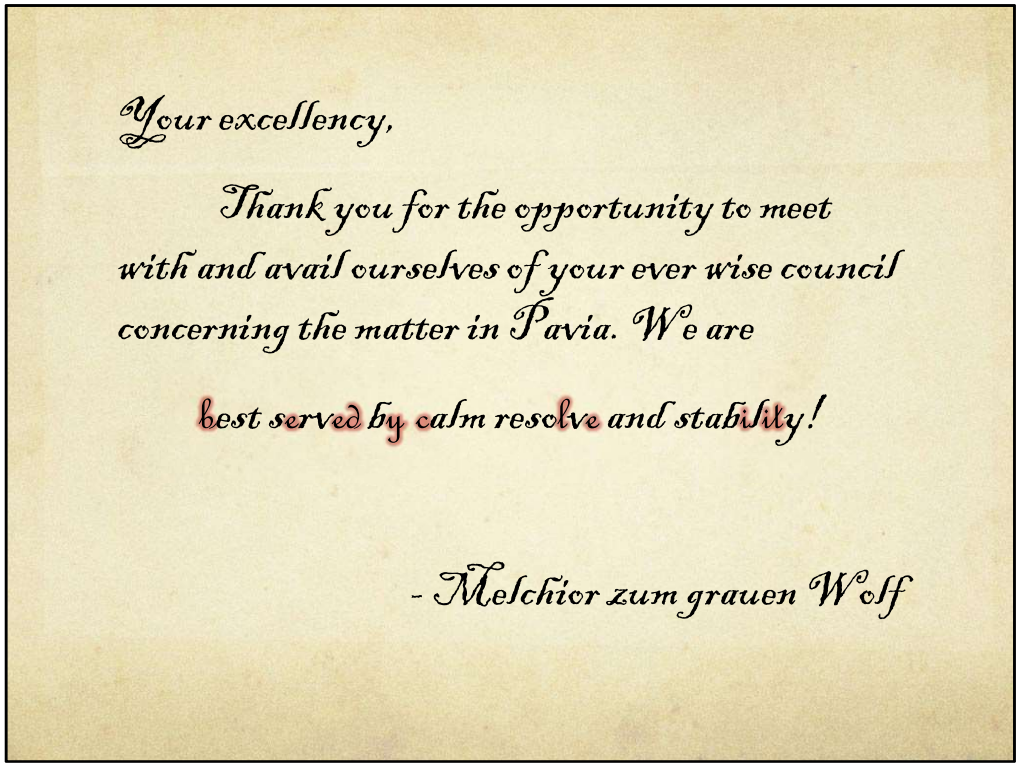
baaaa baabb abbaa aaaaa babaa aaaaa babba

baaaa ba abb abbaa aa aa abab aa aaaa ababba

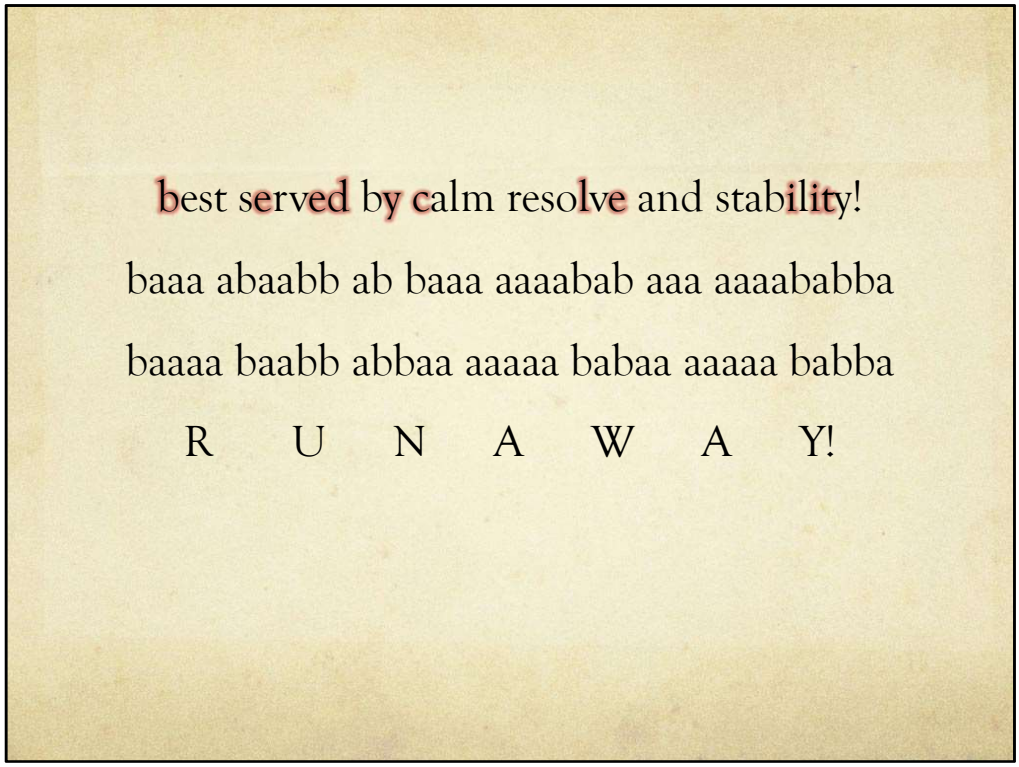
Down for the count It is time to stay put now



This is an intentionally simplified example, similar to those found within Bacon's work. This message shows an outer message which is whole to the casual observer. I've broken the last passage out to make it easier for us to parse but Bacon goes to some length to point out that this system of writing should be done in such a way that it will not draw attention to itself from a casual observer.



Did you notice that some of the letters in the final section of the message use a different script? This is what Bacon is referring to with the term ‘bi-litateral’.



Here we can see the characters plainly. First we identify the alternate script, as on the previous slide. Second we set a value of ‘b’ for all characters that use the alternate script. Thirdly we re-assemble the ‘bits’ into groupings of 5. Finally, each of those 5 bit groupings is converted to its clear-text, deciphered value.

Potential uses?

- Hiding messages in Shakespeare, for one ☺
- There is little modern value.
- Simple and very efficient for period uses.
  - Consider a calligrapher that switched a font for the ‘a’s and ‘b’s
- Very well known in certain circles but would go largely unnoticed by the untrained eye.

Modern Variant

A aaaaab 000001	B aaaaba 000010	C aaaaabb 0000011	D 000100	E 000101	F 000110	G 000111
H 001000	I 001001	J 001010	K 001011	L 001100	M 001101	N 001110
O 001111	P 010000	Q 010001	R 010010	S 010011	T 010100	U 010101
V 010110	W 010111	X 011000	Y 011001	Z 011010	0 011011	1 011100
2 011101	3 011110	4 011111	5 100000	6 100001	7 100010	8 100011
9 * 100100	& 100101	Et 100110	Null 100111	…	…	…
…	…	…	…	…	…	[63] 111111

By expanding the cypher key space by just one character, from 5 to 6 we double the amount of space in our encipherment system from 32 to 64. Remember that 11111 (bbbbb) is the binary equivalent of 31 and 111111 (bbbbbb) is 63. Remember that the 0 value adds 1 to each set so the actual space is 32 and 64. In this case the zero value 000000 (aaaaaa) is simply a null value. If one were to choose to not extend the system beyond simple letters and numbers the space of 36 makes a convenient perfect square. Using a 7x7 square provides for all numbers and letters with 13 additional positions to use for words, special characters, or entropy.

Bacon makes specific reference to the number of ‘spaces’ available within the set for ‘differences’ being 32 so it is clear that this was a binary representation and so the extension of a single bit is wholly compatible with his approach.

The resources listed above are internet focused to make the information easy to find. These sources are not *always* the best option, however, so if you are interested in learning more about this form of cipher then I would like to recommend you to the following works.

Bacon, Francis (1605). The Proficience and Advancement of Learning Divine and Humane.

Bacon, Francis (1640). Of the Advancement and Proficience of Learning. Translated by Wats, Gilbert. Oxford University. pp. 257–271.

Donnelly, Ignatius. (1888). The Great Cryptogram. Chicago: R. S. Peale & Co.

Dupuy, Jr., Paul J. "The Advancement of Learning". An Authorship Analysis - Francis Bacon as Shake-speare. London: Shake-n-Bacon. Chapter 1. Archived from the original on 2017-03-18. Retrieved 2017-03-18.

Eriksen, Kjell (Producer), & Friberg, Jørgen (Director). (2009). Shakespeares skjulte koder - Sweet swan of Avon [Television series DVD]. Norway: Videomaker.

Friedman, William F. & Friedman Elizabeth S. (1957). The Shakespearean Ciphers Examined. Cambridge: Cambridge University Press.

Gaines, Helen Fouché, Cryptanalysis: a Study of Ciphers and Their Solutions (1989), page 6]

Gallup, Elizabeth Wells. (1899). Biliteral Cypher of Sir Francis Bacon.

Hall, Manly Palmer. (1928). The Secret Teachings of All Ages.

Kahn, David (1996). The Code-breakers (2nd ed.). New York: Scribner. pp. 882–888. ISBN 0-684-83130-9.

Loe, Erlend & Amundsen, Petter. (2006). Organisten. Oslo: J.W. Cappelens Forlag.

Nate E. Shebell. (2012). Petter Amundsen, Oak Island and the Treasure Map in Shakespeare - Part I. wordpress.com.

Owen, Orville Ward. (1893-5). Sir Francis Bacon's Cipher Story. Detroit: Howard Publishing.

Tingstad, Richard. (2010). Summary of most convincing Bacon ciphers in Shakespeare. rictin.com.

Biliteral can mean: "written in two different scripts", Oxford English Dictionary