Xifratge de Bacon

Autor:
Data de publicació: 03-09-2016

El xifratge de Bacon o codi de Bacon (en anglès Baconian cipher) és un mètode de codificació de missatges esteganogràfic ideat per Francis Bacon el 1605. [1] [2] [3] Un missatge xifrat s'amaga en la presentació del text, més que en el seu contingut.

D'acord amb Sir Francis Bacon, existeixen tres propietats que ha de tenir un xifratge:

1) Ha de ser facil d'escriure i de llegir

2) Ha de ser confiable i que no pugui ser desxifrat

3) Si és possible lliure de sospita.

Aquesta última condició fa que el codi Bacon suposi un híbrid entre els sistemes criptogràfics i els esteganogràfics compartint característiques d'ambdós. Atès que, si un missatge arribés a caure en mans incorrectes, aquest no podria ser desxifrat tot i ser examinat per experts.[4]

Codificació
Per codificar un missatge, cada lletra de text pla és reemplaçada per un grup de cinc lletres 'A's' o 'B's'. El reemplaçament es fa d'acord amb l'alfabet del codi Bacon, mostrat aquí sota:

a AAAAA	g AABBA	n ABBAA	t BAABA
b AAAAB	h AABBB	o ABBAB	u-v BAABB
c AAABA	i-j ABAAA	p ABBBA	w BABAA
d AAABB	k ABAAB	q ABBBB	x BABAB
i AABAA	l ABABA	r BAAAA	i BABBA
f AABAB	m ABABB	s BAAAB	z BABBB

Nota: Una segona versió del codi Bacon empra un codi únic per a cada lletra. D'aquesta manera, la I i la J tindrien el seu propi codi.

L'escriptor ha d'emprar dos diferents tipus de lletra per al seu codi.

Després de preparar un fals missatge amb el mateix nombre de lletres "A i B" del missatge real, es trien dos tipus de lletra, un per a representar les A's i un altre per a les B's. Llavors, cada lletra del fals missatge ha de ser presentada amb el tipus de lletra apropiat, segons correspongui a una A o a una B.[5]

Per exemple, suposant que es vol encriptar el missatge:

te espero a las cinco
Un cop codificat utilitzant el codi Bacon:

BAABA AABAA AABAA BAAAB ABBBA AABAA BAAAA ABBAB AAAAA ABABA AAAAA BAAAB AAABA ABAAA

ABBAA AAABA ABBAB
Si s'eliminen els espais:

BAABAAABAAAABAABAAABABBBAAABAABAAAAABBABAAAAAABABAAAAAABAAABAAABAABAAAABBAAAAAB
AABBAB
Després cal construir un missatge fals que tingui el mateix nombre de lletres que el missatge encriptat original o veritable:

BAABAAABAAAABAABAAABABBBAAABAABAAAAABBABAAAAAABABAAAAAABAAABAAABAABAAAABBAAAAAB
AABBABNODESEOVERTEMASMEHASDECEPCIONADOPREFIEROESTARSOLOADIOSSSSSSSSSSSSSSSSSS
SSSSSSSSSSS
Els estils de lletres seran majúscules per a les B i minúscules per les A. El resultat seria :

BAABAAABAAAABAABAAABABBBAAABAABAAAAABBABAAAAAABABAAAAAABAAABAAABAABAAAABBAAAAAB
AABBABNodEseoVerteMasMehaSdECEpciOnaDoprefIErOestarsOlOadiossSsssSsssSssSsssssSSssssSsssSSsS
Finalment col·locant els espais:

No dEseo Verte Mas Me haS dECEpciOnaDo prefIErO estar sOlO adiossSsssSsssSssSsssssSSssssSsssSSsS
D'aquí que el mètode pugui ser considerat com esteganogràfic.

Per poder decodificar el missatge, s'empra el mètode invers. Cada "tipus de lletra 1" en el fals missatge ha de ser reemplaçat amb la lletra A, i cada "tipus de lletra 2" amb la lletra B. L'alfabet de Bacon és llavors utilitzat per a recuperar el missatge original. Qualsevol mètode d'escriptura que permeti emprar dues representacions diferents per a cada caràcter pot ser emprada per al Codi Bacon. El propi Francis Bacon va preparar un Alfabet Biliteral per poder escriure a mà, amb lletres minúscules i majúscules de dues formes alternatives. Aquest alfabet va ser publicat com a il·lustració en la seva obra De Augmentis Scientiarum (L' Augment de les Ciències).

Codificació múltiple
D'acord amb Martin Gardner, (en el seu llibre en castellà Rosquillas anudadas y otras amenidades matemáticas), aquest xifrat pot emprar-se per enviar diversos missatges al mateix temps. Això es deu al fet que l'elecció dels símbols que han de representar les A's i les B's del xifrat poden ser diferents. En el seu llibre, diu que, no obstant això, no poden enviar-se més de cinc missatges diferents al mateix temps.i en dona alguns exemples.[6]

Bacon i Shakespeare
Alguns defensors de la teoria baconiana de l'autoria de Shakespeare, com Elizabeth Wells Gallup, han afirmat que Bacon va utilitzar el xifrat per codificar missatges que revelaven la seva autoria al Primer Folio . No obstant això, els criptòlegs nord-americans William i Elizebeth Friedman van refutar les afirmacions que les obres de Shakespeare contenen xifres ocultes que revelen l'autoria secreta de Bacon o de qualsevol altre candidat al seu The Shakespeare Ciphers Examined (1957). L'anàlisi tipogràfica del Primer Foli mostra que s'utilitzaven un gran nombre de tipus de lletra, en comptes de les dues necessàries per al xifrat, i que les pràctiques d'impressió de l'època haurien fet impossible la transmissió d'un missatge amb precisió. La làpida de Friedman incloïa un missatge al xifrat de Bacon que no s'havia detectat durant molts anys. [1]

Afirmacions no demostrades
Les afirmacions següents no estan confirmades, hi ha controvèrsia entre els diferents estudiosos del tema , però existeix un corrent de pensament que afirma que ho estan, com també afirmen que va ser l'autor de les obres de Shakespeare.Aquesta última asseveració, negada en el llibre de William & Elizabeth Friedman: The Shakespearean Ciphers Examined, Cambridge University Press, 1957,[7] però defensada per Andrew Stevens Peck, al seu llibre: Francis Bacon Tudor Equals William Shakespeare.[8] Per a major informació. Vegeu el llibre de Martin Gardner (en castellà) Rosquillas anudadas y otras amenidades matemáticas on es fa l'anàlisi matemàtica més detallada del xifratge.[6]

Ressenya històrica[8]
Per encàrrec del rei Jaume I d'Anglaterra, Sir Francis Bacon va realitzar la revisió de la primera versió de la Bíblia protestant. En ella, Bacon va introduir una sèrie de codis secrets que amagaven missatges relacionats amb els coneixements ocults de rosacreus i maçons. Aquests Codis, a més a més ofereixen paral·lelismes amb les obres de Shakespeare i amb el número 33. [8]

Jaume I va autoritzar la traducció i publicació de la primera versió protestant de la Bíblia en anglès. Quaranta-set homes

van començar el 1607 una tasca que els ocuparia dos anys i set mesos per reescriure la Bíblia, preparant-la per ser impresa. El 1609 els traductors van lliurar els seus manuscrits al rei perquè aquest donés la seva aprovació. La tasca d'unificar els textos procedents de tantes mans va ser encomanada a Bacon. Es deia que el rei havia portat la maçoneria escocesa a Anglaterra. D'altra banda, Bacon era un maçó iniciat, fundador de la Societat Secreta Literària Rosacreu i de la Lògia dels Maçons Especulatius, ambdues el 1580. Bacon a l'edat de setze anys, va ser convidat a París per la reina María Estuard perquè estudiés les filosofies àrab, egípcia, hindú i grega. Durant la seva estada en aquesta ciutat va inventar un sistema de codis secrets que podrien ser incorporats a un document sense aixecar sospites. La seva iniciació maçònica data d'aquesta època europea.[9]

Abans de tornar a Anglaterra va estar també a Itàlia i a Espanya i als 20 anys es va dedicar completament a l'estudi de les lleis. Gràcies als seus coneixements dels secrets apresos amb els maçons, va decidir reactivar les societats secretes britàniques fundant les dues ordes esmentades. Els primers textos anglesos de la Bíblia van romandre en mans de Bacon durant gairebé un any i segons l'escriptor britànic Alfred Dodd en el seu llibre The Martyrdom of Francis Bacon (El martiri de Francis Bacon):[10]

"... va reunir els diferents estils dels traductors donant-los la unitat, el ritme i la música de la prosa shakespeariana, escrivint els prefacis i creant l'esquema global de la versió autoritzada de la Bíblia".

El treball de Bacon no va consistir en una revisió i correcció, sinó que va incorporar informació secreta codificada, tant en l'Antic Testament com en el Nou Testament; documentació sobre la base del secret maçònic i que es refereix a una altra història del cristianisme diferent de la descrita en la versió romana de la Bíblia. Una vegada finalitzat el seu treball, el rei Jacobo I i Bacon van mantenir una sèrie de reunions per tractar assumptes relacionats amb la seva publicació, i també per incloure una "dedicatòria al rei" per exprés desig del monarca, així com la frase: "Apta per llegir a les Esglésies", que hauria de figurar a la primera pàgina. Amb aquestes paraules el monarca volia deixar clar que l'Església d'Anglaterra comptava amb el seu permís per analitzar la nova Bíblia que substituïa a les anteriors en grec o llatí. Aquest mandat va ser interpretat com un intent de distanciar entre les bíblies catòlica i protestant. És també interessant ressaltar que la versió protestant de la Bíblia conté set llibres menys que les versions catòliques; és a dir, seixanta-sis. Al món anglosaxó actual, es tendeix a pensar que la Bíblia del rei Jacobo I és la "original", i per tant, autèntica, i que totes les revisions posteriors són falsificacions. Els documents originals en grec, arameu i hebreu ja no existeixen i les bíblies actuals han sofert cinc revisions des de la primera compilació.No se sap el que va ser escrit en la majoria dels originals escrits, de manera que les paraules "autoritzat" i "original", aplicaves a qualsevol versió de la Bíblia, no signifiquen, necessàriament, "autèntica" o "veritable"

Exemples del codi[8]
Una vegada creat el mètode que permetés la transmissió de missatges per a la posteritat, Bacon i uns altres com ell, van promoure la distribució de certs documents, especialment preparats, que incorporaven criptogrames amb profunds secrets sobre la religió, el misticisme i la filosofia. D'aquesta manera, els maçons i rosacreus medievals disseminaven els seus ensenyaments per tot el món sense aixecar sospites, ja que els textos que contenien aquests criptogrames podien ser examinats sense revelar la presència de secrets. En l'edició de 1612 de la Versió autoritzada de la Bíblia del rei James, sobre el títol: To the Christian Reader (Per al Lector Cristià) hi ha un disseny de gossos, consells i arquers. El mateix que en l'edició en foli d'una obra de Shakespeare. No obstant això, és l'edició en quart de la Biblia de 1612 la que presenta un major interès, ja que a la pàgina de títols hi ha dos complexos dissenys d'encapçalament emprats per Bacon en llibres previs apareguts al 1593 i al 1594. L'elecció d'aquests dissenys no obeïa a cap capritx; es tractava de relacionar certs llibres i crear connexions entre ells. Més clares eren les lletres A majúscules, clara i fosca (A.A) del disseny inferior, també repetit en diverses obres de Shakespeare. Aquesta relació directa entre la Bíblia i les obres del genial dramaturg anglès va ser passada per alt durant molt temps, malgrat contenir una informació xifrada que encara no ha estat desxifrada en l'actualitat.

L'examen de desenes de "folis" i "quartilles" de Shakespeare, revela una infinitat de signatures acròstiques. La forma més senzilla era coneguda com "el codi de lletres majúscules", pel qual un nom, en aquest exemple el de Bacon, quedava amagat en les primeres lletres de línies consecutives. En l'acte 1, escena II de la Tempestat, hi ha un exemple de l'acròstic de Bacon.

Begun to tell me what I am but stopt,

And left me to a bootlesse inquisition

CONcluding, stay; not yet...

No és només el nom BACON el que és important, sinó que la forma dibuixada per aquestes lletres és una "L". Aquesta

lletra connecta amb altres dins l'obra fins a combinar 33 lletres consecutives. Aquestes lletres formen paraules completes amb un contingut específic. Aquest acròstic de 33 lletres es coneix amb el nom de Codi Bacon i apareix tant en les obres de Shakespeare com en la Bíblia de 1612.

Bacon i el número 33 (Segons Andrew Stevens Peck)[8]
Gran part de la informació xifrada per Bacon en les obres teatrals i en la Bíblia se centren en el nombre maçònic 33.

En el prefaci del llibre, The Advancement and Proficience of Learning (publicat el 1640), Bacon aporta una pista en escriure:

"La glòria de Déu oculta alguna cosa i la dels Reis és esbrinar-ho"

Això condueix al Llibre dels reis de l'Antic Testament, que inclou més codis que utilitzen el número 33. El que Bacon volia que se sabés és que el primer Temple de Salomó va tenir 33 anys de màxima esplendor (segons el comput bíblic). El rei David havia de regnar 33 anys a Jerusalem i Jesucrist havia de morir als 33 anys. No obstant això, l'Evangeli i el moviment original de l'Església van registrar que el rabí Jesús Cunobeline tenia molts més anys que 33 (Joan 8:57). Si els registres de l'Església són correctes perquè el número 33 va ser triat per simbolitzar la durada de la seva vida? Potser perquè en les societats secretes es necessitaven 33 anys místics per arribar al mestratge. Passar per set iniciacions, l'última de les quals, una amenaça per a la vida, requereix 33 graus de consciència. Bacon volia recalcar que els maçons i altres societats secretes de l'època, pensaven que Jesús va ser un iniciat del grau 33 en els misteris sagrats. La dedicatòria de l'obra "Shakespeare folio 1623",[11][12] diu:

Dedicat a "la parella de germans" (els bessons Judes Khrestus i el rabí Jesús?).

Aquí la frase té 33 lletres i a més a més dirigeix a l'interessat directament a la pàgina 33 on hi ha una altra seqüència de 33 lletres: "Jesus Christ, Initiation, Great Pyramid" (Jesucrist, iniciació, Gran Piràmide"). L'existència d'aquesta informació codificada en el foli de Shakespeare de 1623 és una prova de la relació editorial de Bacon amb la Bíblia i les obres teatrals de Shakespeare. En paraules de Tony Bushby, autor de The Bible Fraud:[13]

"Qualsevol que desentranyi el Shakespeare folio 1623[12] probablement faci el descobriment literari més important de tots els temps. El miracle serà trobar la persona capaç de trencar el vel i revelar els secrets d'aquest tom"

Bibliografia

Rosquillas anudadas y otras amenidades matemáticas (1986) (Editorial Labor, 1987; ISBN 84-335-5108-6)
The Advancement of Learning, Sir Francis Bacon, The Online Library of Liberty, Liberty Fund Inc.
Key to the Bi-literal Cipher of Francis Bacon, Charles Loughridge, Denver, Colorado, (Digitalizat per Microsoft, cedit per la Universitat de Califòrnia)
The Bible Fraud, Tony Bushby, 2001
Masonic references in non-fiction, Web de la Gran Logia de Columbia Britanica y
Yucon, http://www.freemasonry.bcy.ca/fiction/non-fiction.html
The Mystery of Francis Bacon, William Smedley's
Archaeological Conspiracy at Williamsburg: The Mistery of Bruton Vault, David Allen Rivera, 2007
God's Secretaries, Adam Nicolson
Francis Bacon and the James 1st Bible, A. E. Loosley
William Friedman and Elizabeth Friedman, The Shakespearian ciphers examined, Cambridge University Press, 1957
J.R. Carrell, "The Shakespeare Secret",2007 - A great story with surprising twists and turns, explaining a lot about Shakespeare an his time, but also contains a fantastic myth.

Referències

? Bacon, Francis. The Proficience and Advancement of Learning Divine and Humane, 1605.
? Bacon, Francis. Of the Advancement and Proficience of Learning. Oxford University, 1640, p. 257–271.
? Dupuy, Jr., Paul J. «The Advancement of Learning». An Authorship Analysis - Francis Bacon as Shake-speare. Shake-n-Bacon. Arxivat de l'original el 2017-03-18. [Consulta: 18 març 2017].
? [enllaç sense format] http://estudiosdeunprofano.blogspot.com.es/2010/01/en-esta-oportunidad-voy-complementar-mi.html
? Helen F. Gaines. Cryptanalysis: A Study of Ciphers and Their Solution. Courier Corporation, 18 novembre 2014. ISBN 978-0-486-80059-2.

? Anar a :6,0 6,1 Martin Gardner. Knotted Doughnuts and Other Mathematical Entertainments. W.H. Freeman, 1986. ISBN 978-0-7167-1799-7.
? William F. Friedman; Elizabeth S. Friedman The Shakespearean Ciphers Examined: An Analysis of Cryptographic Systems Used as Evidence that Some Author Other Than William Shakespeare Wrote the Plays Commonly Attributed to Him. Cambridge University Press, 14 abril 2011, p. 170–. ISBN 978-0-521-14139-0.
? Anar a :8,0 8,1 8,2 8,3 8,4 Andrew Stevens Peck. Francis Bacon Tudor Equals William Shakespeare. Nova Publishers, 2001, p. 31–. ISBN 978-1-56072-734-7.
? Loughridge Charles. Key to the Bi-Literal Cipher of Francis Bacon. Hardpress Limited, gener 2013. ISBN 978-1-313-31623-1.
? Alfred Dodd. The Martyrdom of Francis Bacon. Rider & Company, 1945*.
? Alexander Dyce. A few notes on Shakespeare, with occasional remarks on the emendations of the manuscript-corrector in mr. Collier's copy of the folio 1632, 1853, p. 35–.
? Anar a :12,0 12,1 William Shakespeare; Samuel Ayscough; Nicholas Rowe The Dramatic Works of William Shakespeare: With Explanatory Notes. To which is Added a Copious Index to the Remarkable Passages and Words. J. Stockdale, 1807, p. 29–.
? Tony Bushby. The Bible Fraud: An Untold Story of Jesus Christ. Pacific Blue Group, 1 gener 2001. ISBN 978-0-9579007-1-4.

Enllaços externs

Francis Bacon and The Advancement of Learning (en anglès)
Baconian Cipher Tool (Purple Hell)
Bacon's Cipher Information/Examples
Baconian Cipher Converter (free download)
Excerpts from Bacon's writing and cipher illustrations Arxivat 2016-09-17 a Wayback Machine.
Cryptographic Shakespeare by Penn Leary Arxivat 2016-09-17 a Wayback Machine.
Francis Bacon's Ciphers Arxivat 2007-01-27 a Wayback Machine. at the Philosophical Research Society