

---

# xifratge maçònic

Autor:

Data de publicació: 03-09-2014

Salta a la navegacióSalta a la cerca

El xifratge pigpen utilitza símbols gràfics assignats d'acord amb una clau similar al diagrama anterior. [1]

El xifratge pigpen (també conegut com el xifratge maçònic, el xifrat dels Maçons, el xifrat Napoleó i el xifratge tic-tac-toe)[2] és un xifratge geomètric simple per substitució, que intercanvia lletres per símbols que són fragments d'una quadrícula. La clau d'exemple mostra una manera en què les lletres es poden assignar a la quadrícula.

## Contingut

### Inseguretat

Tot i que Pigpen podria ser considerat com un xifratge divertit per utilitzar, no ofereix gairebé cap seguretat. El seu ús de símbols en lloc de lletres de cap manera impedeix la criptoanàlisi, i aquest xifratge no és diferent de qualsevol altre xifratge simple de substitució monoalfabètic. Pitjor encara, perquè és molt conegut i immediatament reconeixible, és sens dubte un dels pitjors xifratges que es poden triar des del punt de vista de la seguretat. De fet, el coneixement de Pigpen és tan omnipresent que un interceptor podria no necessitar trencar realment aquest xifratge, sinó simplement desxifrar-lo, de la mateixa manera que ho faria el destinatari previst.

L'ús freqüent de Pigpen entre els escolars per ocultar informació dels seus professors (per exemple, en notes de passada) és especialment irònic en aquest sentit, ja que tots els professors van ser una vegada nens mateixos, nens que molt bé podrien haver utilitzat Pigpen!

A causa de la simplicitat de Pigpen, s'inclou molt sovint en els llibres infantils sobre xifratges i escriptura secreta. [4]

### Història

Es creu que el xifratge és un xifratge antic[5][6] i es diu que es va originar amb els rabins hebreus. [7] Thompson escriu que, "hi ha proves que suggereixen que els templers van utilitzar un xifratge de ploma de porc" durant les Croades Cristianes. [9][10]

Parrangan i Parrangan escriuen que va ser utilitzat per un individu, que podria haver estat un maçó, "al segle XVI per salvar les seves notes personals". [11]

---

El 1531 Cornelius Agrippa va descriure una forma primerenca del xifratrosicruc, que atribueix a una tradició cabalística jueva existent. [12] Aquest sistema, anomenat "La Càbala de les Nou Cambres" per autors posteriors, va utilitzar l'alfabet hebreu en lloc de l'alfabet llatí, i es va utilitzar per al simbolisme religiós més que per a qualsevol propòsit criptològic aparent. [13]

Les variacions d'aquest xifratge van ser utilitzades tant per la germandat rosroscruciana[14] com pels maçons, encara que aquests últims van utilitzar el xifratge pigpen tan sovint que el sistema s'anomena freqüentment xifratge del maçó. Hysin afirma que va ser inventat pels maçons. [15] Van començar a utilitzar-lo a principis del segle XVIII per mantenir els seus registres d'història i ritus privats, i per a la correspondència entre els líders de les lògies. [3][16][17] També es poden trobar làpides de maçons que utilitzen el sistema com a part dels gravats. Una de les primeres pedres del Cementiri de l'Església de la Trinitat a Nova York, que es va inaugurar el 1697, conté un xifratge d'aquest tipus que es desxifra per "Recordar la mort" (cf.

L'exèrcit de George Washington tenia documentació sobre el sistema, amb una forma molt més aleatòria de l'alfabet. Durant la Guerra Civil dels Estats Units, el sistema va ser utilitzat pels presoners de la Unió a les presons confederades. [14]

### Exemple

Utilitzant la clau de xifrat pigpen que es mostra a l'exemple anterior, el missatge "X MARCA L'ESPOT" es representa en text xifrat com

### Variants

Els elements centrals d'aquest sistema són la quadrícula i els punts. Alguns sistemes utilitzen les X, però fins i tot aquests es poden reorganitzar. Un mètode d'ús comú ordena els símbols com es mostra a la imatge anterior: quadrícula, quadrícula, X, X. Un altre sistema d'ús comú ordena els símbols com quadrícula, X, quadrícula, X. Una altra és quadrícula, quadrícula, quadrícula, amb cada cel·la que té una lletra de l'alfabet, i l'última té un caràcter "•";. Les lletres de la primera quadrícula no tenen punts, les lletres de la segona tenen un punt cadascuna, i les lletres de la tercera cadascuna tenen dos punts. Una altra variació d'aquesta última s'anomena xifratge de Newark, que en lloc de punts utilitza d'una a tres línies curtes que poden estar projectant-se en qualsevol longitud o orientació. Això dona la il·lusió d'un nombre més gran de caràcters diferents dels que realment existeixen. [18]

Un altre sistema, utilitzat pels rosrosiucs al segle XVII, utilitzava una sola quadrícula de nou cèl·lules, i d'1 a 3 punts a cada cel·la o "ploma". Així que ABC estaria a la ploma superior esquerra, seguit per DEF i GHI a la primera línia, després grups de JKL MNO PQR a la segona, i STU VWX YZ a la tercera. [2][14] Quan es xifra, la ubicació del punt en cada símbol (esquerra, centre o dreta), indicaria quina lletra d'aquesta ploma estava representada. [1][14] Els sistemes més difícils utilitzen una forma no estàndard de l'alfabet, com escriure'l cap enrere a la quadrícula, amunt i avall a les columnes,[4] o un conjunt de lletres completament aleatoritzat.

El xifratge templer és un mètode que es diu que va ser utilitzat pels templers i utilitza una variant d'una creu maltesa. [19] Aquest és probablement un xifratge utilitzat pels neotempers (maçons) del segle XVIII, i no el de l'orde religiós dels cavallers templers dels segles XII-XIV durant les Croades. [20]

### Notes

^ Jump up to:un b Wrixon, pp. 182–183

^ Jump up to:un b Barker, pàg. 40

^ Jump up to:un b Wrixon, p. 27

^ Jump up to:un b Gardner

^ Bauer, Friedrich L. "Passos de xifratge: substitució simple". *Secrets desxifrats: Mètodes i màximes de criptologia* (2007): 43.

^ Newby, Peter. "La Maggie tenia un porquet". *Maneres de paraula* 24.2 (1991): 13.

^ Blavatsky, Helena Petrovna. *Glossari teosòfic*. Societat Editorial Teosòfica, 1892, pg 230

^ Mathers, SL MacGregor. *La Càbala es va donar a conèixer*. Routledge, 2017, pg 10

^ Thompson, Dave. "Criptografia de corba el·líptica". (2016)

^ MacNulty, W. K. (2006). *Maçoneria: símbols, secrets, significat*. Londres: Tàmesi & Hudson, pg 269

- 
- ^ Parrangan, Dwijayanto G., i Theofilus Parrangan. "Nou algorisme simple per detectar el significat de Pigpen Chiper Boy Scout ("Pramuka"). *Revista Internacional de Processament de Senyals, Processament d'Imatges i Reconeixement de Patrons* 6.5 (2013): 305-314.
  - ^ Agripa, Henry Cornelius. "Tres llibres de filosofia oculta, o de". *JF* (Londres, Gregory Moule, 1650) (1997): 14-15.
  - ^ Agripa, Corneli. "Tres llibres de filosofia oculta", <http://www.esotericarchives.com/agrippa/agripp3c.htm#chap30>
  - ^ Jump up to:un b c d Pratt, pp. 142-143
  - ^ Hynson, Colin. "Codis i xifratges". 5 a 7 Educador 2006.14 (2006): v-vi.
  - ^ Kahn, 1967, p.~772
  - ^ Newton, 1998, p. 113
  - ^ Glossari de criptografia
  - ^ McKeown, Trevor W. "Xifrat dels templers" [freemasonry.bcy.ca](http://freemasonry.bcy.ca). Consultat el 2016-11-07.
  - ^ Guénon, René (2004). *Estudis sobre maçoneria i compagnonnage*. Traduït per Fohr, Henry D.; Bethell, Cecil; Allen, Michael. Sofia Perennis. p. 237. 0900588518 de l'ISBN 978.

## Referències

- Barker, Wayne G., Ed. (1978). *Història dels codis i xifratges als Estats Units abans de la Primera Guerra Mundial*. Premsa de l'Egeu Park. Isbn 0-89412-026-3.
- Gardner, Martin (1972). *Codis, xifratges i escriptura secreta*. Isbn 0-486-24761-9.
- Kahn, David (1967). *Els desxifradors de codis. Historia de la escriptura secreta*. Macmillan.
- Kahn, David (1996). *Els desxifradors de codis. Historia de la escriptura secreta*. Scribner. Isbn 0-684-83130-9.
- Newton, David E. (1998). «El xifratge del maçó». *Enciclopèdia de criptologia*. Isbn 0-87436-772-7.
- Pratt, Fletcher (1939). *Secreto y urgent: historia de los codificas y xifrats*. Premsa de l'Egeu Park. Isbn 0-89412-261-4.
- Shulman, David; Weintraub, Josep (1961). *Glossari de criptografia*. Premsa criptogràfica. p. 44.
- Wrixon, Fred B. (1998). *Codis, xifratges i altres comunicacions criptiques i clandestines*. Black Dog & Leventhal Publishers, Inc. ISBN 1-57912-040-7.

## Enllaços externs

A Wikimedia Commons hi ha contingut multimèdia relatiu a: Xifrat pigpen

Eina de xifrat pigpen en línia per al desxiframent de missatges petits.

Eina de xifrat pigpen en línia per desxifrar missatges petits.

Tipus de lletra de tipus true del codi xifrat

Desxifrar un criptograma ominós en una tomba de Manhattan presenta una variant de xifrat pigpen

L'escriptura eliana sovint es considera una variant de Pigpen.