El codi secret de l'emperador Carles V

Autor:
Data de publicació: 04-02-2023

El 1547 l'emperador Carles V —per a nosaltres Carles I d'Espanya i V d'Alemanya— va enviar una carta xifrada a Jean de Saint-Mauris, el seu ambaixador a la cort francesa, confiant-li un missatge secret. Llevat del destinatari de la missiva, presumiblement els espies i criptoanalistes al servei del monarca francès Francisco I, i per tant, també el rei gal, ningú més hauria tingut accés a la informació continguda en la misteriosa carta, que avui dia es conserva a la Biblioteca Stanislas de Nancy (França). Ningú... fins ara.

09 febrer 2023

El codi secret de l'emperador Carles V

Cultura | Història | Humanitats | Recerca

Finestra al Coneixement

Periodisme Científic

Temps estimat de lectura 4

El 1547 l'emperador Carles V —per a nosaltres Carles I d'Espanya i V d'Alemanya— va enviar una carta xifrada a Jean de Saint-Mauris, el seu ambaixador a la cort francesa, confiant-li un missatge secret. Llevat del destinatari de la missiva,

presumiblement els espies i criptoanalistes al servei del monarca francès Francisco I, i per tant, també el rei gal, ningú més hauria tingut accés a la informació continguda en la misteriosa carta, que avui dia es conserva a la Biblioteca Stanislas de Nancy (França). Ningú... fins ara.

LA INVESTIGACIÓ

Ha estat un equip d'investigadors, encapçalat per la criptògrafa francesa Cecile Pierrot, de l'Inria (Institut National de Recherche a Informatique et en Automatique), el que ha aconseguit finalment desxifrar el codi l'emperador després de sis mesos d'intens treball. Després d'intentar-ho en va pel seu compte, Pierrot va reclutar dos col·legues, un expert en anàlisi complexa i un informàtic expert en lògica algorítmica. Junts van formular múltiples hipòtesis a tall d'algoritmes que després van testar amb el suport de potents computadores. Però ni tan sols així van aconseguir vulnerar l'enigmàtic codi. Per la qual cosa no els va quedar més remei que recórrer a l'ajuda de Camille Desenclos, un historiador expert en els entrebancs polítics i els sistemes criptogràfics de l'època, per donar amb alguna pista o indici històric que els facilités una porta d'accés a la xifra de Carles V.

La complexitat del codi regi rau en el en el el benenteix en el qual combina dos jocs de símbols (simples i complexos) per representar les diferents lletres de l'alfabet. Crèdit: Biblioteca Stanislas (Nancy, França)

Finalment, va ser Desenclos qui va donar amb la pista definitiva en investigar en la correspondència conservada de Saint-Mauris i descobrir una altra carta escrita amb el mateix sistema de xifrat en els marges del qual hi havia apuntats fragments transcrits. Armats amb la seva particular pedra Rosetta, els criptoanalistes francesos a la fi van poder desxifrar el codi i, d'aquesta manera, esbrinar que el missatge de l'emperador confiava al seu ambaixador les seves sospites que Francisco I conspirava per assassinar-lo, instinant-lo que l'investigara.

EL CODI

El xifrat de l'emperador —presumiblement ideat pels experts criptògrafs de la Cancelleria Imperial— consistia en un nomenclador. Aquest sistema de codificació es basa en un alfabet xifrat, que s' utilitza per codificar la major part del missatge, i es complementa amb una llista de paraules codificades i altres símbols amb un significat concret, tal com es pot apreciar en l' esquema adjunt, exposat per Cecile Pierrot durant la presentació dels seus resultats:

Codi xifrat de l'Emperador Carles V. Crèdit: Biblioteca Stanislas (Nancy, França)

La complexitat del codi regi rau en el en el el benenteix en el qual combina dos jocs de símbols (simples i complexos) per representar les diferents lletres de l'alfabet, segons com s'integrin en les paraules. Així, quan una consonant va seguida d' una vocal, és representada amb el símbol complex corresponent amb el signe diacrític que representa aquesta vocal. Amb la dificultat afegida que, en aquest cas, atès que la lletra E no té cap marca diacrítica associada, totes les És del missatge que segueixen a una consonant desapareixen o s' ometen. Els símbols simples s' empren, en el cas de les vocals, quan aquestes són la lletra inicial de la paraula o quan segueixen una altra vocal; i en el cas de les consonants quan no van immediatament seguides d' una altra vocal.

Però a més, el codi també inclou símbols nuls, i d' altres que representen personatges rellevants de l' escena política, que caldria esperar que fossin esmentats en un missatge enviat o remès a algun alt càrrec. Tot això per dificultar la criptoanàlisi.

Joc 1: Un missatge real

A la vista del nomenclador en què es basa el codi de Carles V, desxifrar el següent missatge hauria de resultar un joc de nens

LA CONNEXIÓ CRIPTOGRÀFICA ENTRE CARLES V I MARÍA ESTUARDO

Un nomenclador molt similar emprava, d'altra banda, María Estuardo, reina d'Escòcia, per comunicar-se amb els seus seguidors en el seu enfrontament amb la reina Isabel i que, en última instància, seria la causa de la seva execució.

El nomenclador de María Estuardo. Crèdit: Simon Singh

Joc 2: Un altre inquisitiu missatge secret per a l'ambaixador Saint Mauris

Però aquesta no és l'única ni la més tràgica connexió criptogràfica entre la corona espanyola i María Estuardo. El

successor de Carles I, Felip II, també emprava xifres en la seva correspondència amb el seu germanastre, Don Juan de Austria. Almenys una d'aquestes cartes, en la qual es descrivia un pla per envair Anglaterra, va ser interceptada pels espies de Guillermo de Orange i desxifrada pel seu criptoanalista de capçalera: Philips van Marnix. Un pla que Guillermo va compartir amb els seus aliats anglesos i que, en gran mesura, va acabar de convèncer el ministre de defensa anglès de la necessitat de crear una Escola de Xifres —la precursora de l'actual GCHQ (Goberment Communications Headquarters) britànic i de tantes altres agències d'intel·ligència nacionals—. Com a secretari de l'Escola es va designar el lingüista Thomas Phelippes qui, precisament, poc després seria l'encarregat de desxifrar el nomenclador de María Estuardo i, amb això, treure a la llum els seus plans de conspiració, pels quals seria condemnada a mort: el 8 de febrer de 1587 va ser decapitada a la gran sala del Castell de Fotheringhay.

Joc 3: Una xifra a base de Xs, Is i Vs

Ara que ja ets expert en la xifra de Carles V el desafiament es presenta com un missatge secret codificat amb una xifra original que ret homenatge a l'emperador Carles V.

El missatge:

SOLUCIONS

Joc 1:
Dios salve al rey (d'Anglaterra, of course)

Joc 2:

Qué han averiguado nuestros informantes en la corte

Joc 3:

En aquest cas el missatge està xifrat amb una senzilla xifra del Cèsar (un tipus d'un xifrat per substitució, en el qual una lletra en el text original és reemplaçada per una altra lletra que es troba un nombre fix de posicions més endavant en l'alfabet) on la lletra V ocupa la cinquena posició. I, a continuació, cada lletra és substituïda pel número romà que correspon a la seva posició en l' alfabet xifrat:

La xifra:

La solució:

UNA CIFRA DEL CESAR CON NÚMEROS ROMANOS PARA EL EMPERADOR DEL SACRO IMPERIO ROMANO GERMANICO