ÍNDEX

Apartat Pàgina

INTRODUCCIÓ

En els últims 150 anys, i en especial en les dues últimes dècades, la reducció dels temps de transmissió de la informació a distància i d'accés a la mateixa és un dels reptes essencials de la nostra societat. En el decurs de la historia els mitjans de comunicació han anat avançant en paral·lel amb la creixent capacitat dels pobles per a configurar el seu món físic i amb el seu creixent grau de interdependència.

L'home sempre ha buscat satisfer les seves necessitats de forma còmoda i rentable; per això, ha incorporat tècniques que fan la vida en societat molt més planera. El primer avanç important de la societat va ser la millora en el camp de l'agricultura, donant pas així a la societat agrícola. Aquesta evolució continuà cercant el

benestar humà fins que, a principis del segle XIX situem, la invenció de la màquina de vapor, la qual obre el període de la societat industrial. No obstant, la vida en societat ha continuat millorant amb noves invencions. Tant importants han estat els avenços en el darrer segle que els experts parlen ja d'una nova era, molt més desenvolupada que l'era agrícola o industrial. La revolució de les telecomunicacions i de la transmissió de dades ha empès al món cap al concepte d'*aldea global*. Penso que hem de concordar que ens trobem a l'era de la informació.

En aquesta era que ens ha tocat viure, la informació circula arreu del món a una velocitat vertiginosa. Actualment tenim al nostre abast formes potentíssimes per a comunicar−nos com el telèfon, el correu, la premsa, la televisió, la radio... i els ordinadors. De totes aquestes, una de les possibilitats de comunicació més emprades són els ordinadors, degut a la seva connexió mundial en una gran xarxa com és internet. Internet permet una comunicació eficaç i amb un ampli ventall de possibilitats, com: videoconferència, canals de tertúlia, intercanvi d'arxius, etc. Aquesta eina pràcticament nova i encara per potenciar requereix una atenció especial ja que necessita més que cap altra l'existència d'una certa seguretat. Aquesta utilitat dels ordinadors permet la comunicació entre dos punts, pràcticament qualsevols−−>[Author:d], del món. No obstant, posem per cas que un missatge surt d'Espanya amb destinació a Austràlia; doncs bé, des del moment en que el missatge surt des de l'ordinador espanyol i assoleix el seu destí, passa un determinat temps més que suficient per a que *els pirates de la xarxa* interceptin el missatge. A més, el missatge passa per una gran quantitat d'ordinadors arreu del món els quals no tenen perquè rebre el missatge si no volem que així sigui. És aquí, als ordinadors, però especialment a internet, on intervé amb més incidència la criptografia moderna i també serà el camp on es centri aquest treball.

Molts dels grans fets que han succeït a la història no haurien esdevingut si no s'hagués mantingut informació important en secret. Això, ho hem comprovat tant en guerres, on s'utilitzaven llenguatges en clau; com a governants o reis molt coneguts que empraven alguna mena de llenguatge codificat per a mantenir confidencialment els assumptes d'Estat. Els cèsars de l−−>'Imperi Romà, per exemple, van recórrer a la criptografia per comunicar els assumptes d'Estat. També està el cas d'un rei que va emprar un codi secret per intercanviar informació i missatges, Felip II. Sí, ja al segle XVI Felip II va utilitzar la substitució múltiple per mantenir correspondència amb el Duc d'Alba. [Author:d]

D'aquesta forma, veiem que en el decurs de la història sempre ha existit, lligada a l'escriptura, la necessitat de confondre el missatge, d'ocultar−lo per tal que resti en profund secret. Així que és interessant investigar des de quan es remunta l'art de l'encriptació, investigació que he dut a terme per a realitzar aquest treball.

Al llarg de les últimes dècades l'home s'ha esforçat per establir i millorar la criptografia per al seu ús al món de les computadores. No obstant això, també cal mencionar l'esforç oposat que han fet altres per tal que la seguretat de la informació no estigui a plena disposició de l'usuari. En la qüestió de la necessitat de la criptografia a nivell d'usuari es produeix una bifurcació d'opinions, d'una banda l'Estat i empreses que monopolitzen internet, entre d'altres, estan totalment en contra de que l'usuari tingui al seu abast eines segures d'encriptació, i d'altra banda, els usuaris, encapçalats pels revolucionaris *hackers*, que demanen una àmplia facilitat d'accés a sistemes criptogràfics. És d'aquesta disjuntiva d'on sorgeix tot un camp de qüestions polítiques, ètiques i legals sobre l'ús de mètodes de protecció de dades.

Tots aquests aspectes són tractats en aquest treball que duu com a tema general: criptografia i seguretat computacional. Tractaré primerament el terme criptografia i altres relacionats com −−>*encriptació*, *codificació*[Author:d], ja que un cop explicats el lector podrà anar més orientat a l'hora de llegir aquest treball i comprendre'l. També faré una exposició sobre l'ús i les finalitats de la criptografia.

Una altre apartat clau serà el de la història de la criptografia des de l'antiguitat fins als nostres temps. Per últim, els mètodes d'encriptació existents actualment, ocuparan una part primordial del treball. Com a annex, el treball adjunta un programa per codificar i descodificar arxius de text en format MS−DOS. Aquest programa es basa en la substitució múltiple mitjançant una clau demanada a l'usuari.

SIGNIFICAT DE CRIPTOGRAFIA I PARAULES RELACIONADES

Segons el Diccionari de la Real Acadèmia Espanyola de la Llengua, la paraula criptografia prové del grec *ððððóð*, que significa ocult, i **ðððð*, que significa escriptura. La seva definició és: art d'escriure amb clau secreta o d'una forma enigmàtica. Òbviament la criptografia fa anys que deixà de ser un art per convertir−se en una tècnica, o més bé en un conglomerat de tècniques, que tracten sobre la protecció − ocultament davant observadors no autoritzats − de la informació.

Un altre terme relacionat amb l'anterior és criptograma, el qual el Diccionari de la Real Acadèmia defineix com document xifrat. En aquesta definició apareix una paraula que cal tenir molt present, xifrat, que, a la forma d'infinitiu, significa escriure en xifra. D'aquesta darrera definició podem deduir que quan emprem en aquest document la paraula xifra ens estarem referint a escriptura secreta, o dit d'una altra manera, el missatge ocult.

En alguns textos en comptes d'utilitzar la paraula criptografia utilitzen criptologia. Si bé ambdues paraules són sinònims, personalment, els trobo sinònims parcials, mai totals. Hem de distingir aquestes paraules examinant la seva etimologia. La paraula criptologia prové de *kryptós*, ocult, i *lógos*, paraula. Per tant, criptologia és la **ciència** que s'encarrega d'ocultar paraules. En canvi, com mencionàvem abans, criptografia prové de les paraules ocult i escriptura, fent així que el seu significat sigui l'**estudi** de les tècniques mitjançant les quals podem emmascarar el missatge contingut en un escrit.

La criptografia així estudia els processos de xifrat o desxifrat dels missatges, així com l'anàlisi dels criptogrames per a descobrir la clau i el text original. Aquest camp d'estudi de la criptografia es designat per un mot en concret, criptoanàlisi. El criptoanàlisi, principalment, cerca trencar la xifra, és a dir, a partir de la xifra trobar el text original.

El dissenyador del sistema criptogràfic rep el nom de criptògraf, i el seu sistema que dissenya, criptosistema o sistema secret. El criptògraf té un oponent, el qual realitza just el treball antitètic, es tracta del criptoanalista el qual tracta, mitjançant diverses tècniques, trencar el secret del sistema aconseguint la xifra i/o el missatge original.

En aquest treball, apareixen paraules com codificar i descodificar, encriptar i desencriptar. Pel que fa a codificar només he de dir que es tracta d'un molt bon sinònim per al terme xifrar, tot i que es tracta d'un sinònim parcial. Aquest mot, codificar, i el seu oposat, descodificar, els utilitzo per evitar reiteracions contínues. Amb el mateix objectiu empro encriptar i desencriptar, paraules les quals no estan acceptades encara per la Real Acadèmia de la Llengua ja que pertanyen, ara per ara, a la terminologia anglosaxona. Respecto les opinions d'aquells que no volen emprar, si no és necessari, paraules foranes; no obstant, les utilitzo per dues raons: perquè l'extensió del treball requereix evitar totes les repeticions possibles i per augmentar la riquesa lèxica de cada individu.

Una altra paraula relacionada al tema d'aquest treball és esteganografia − o ús de *canals subliminals* − consisteix en ocultar a l'interior d'una informació, aparentment innòcua, un altra tipus d'informació (xifrada o no). Aquest mètode ha guanyat bastant importància últimament degut a que permet burlar diferents sistemes de control. Com es de suposar, existeixen tants mecanismes per portar a terme aquest *camuflatge* com la nostra imaginació ens permeti.

Aquest treball adjunta una pràctica d'un missatge encriptat mitjançant una tècnica esteganogràfica apareguda en una pel·lícula.

Si en qualsevol moment del treball apareix una paraula que requereixi qualsevol tipus d'explicació o aclariment, aquesta serà feta mitjançant una nota a peu de pàgina o una breu especificació entre parèntesi.

ÚS I FINALITATS DE LA CRIPTOGRAFIA

Sorgeix una pregunta fonamental que plantejar−nos, abans de continuar analitzant aquest document: *per què necessitem la criptografia?*

És necessari tenir clara aquesta qüestió perquè potser no mereix la pena que dedicar part del nostre temps i de les nostres energies en examinar el tema de la criptografia.

Com ja hem esmentat a la introducció, la manipulació de la comunicació en algunes ocasions pot ocasionar conseqüències de vital importància, com ha estat al cas d'alguna de les guerres entre les grans potències. També a les comunicacions digitals apareixen els mateixos perills. Per tant, necessitem la criptografia per evitar la manipulació de les nostres comunicacions, i així evitar possibles conseqüències desastroses.

Convé tenir en compte que, a les comunicacions digitals, el text, missatge o document no viatja directament d'emissor a receptor, sinó que, al cas dels ordinadors, passa per una sèrie d'ells, permetent així la intercepció del missatge per qualsevol individu aliè a la comunicació.

No obstant, és necessari analitzar totes les funcions, capacitats i possibilitats que ofereix la criptografia. La criptografia cerca:

* Garantir l'autenticitat d'origen del document, és a dir, que el missatge prové de la persona o entitat de qui ha de provenir. En els documents escrits sobre paper, això s'aconsegueix mitjançant la signatura analògica de l'emissor. Als documents digitals això es pot aconseguir amb la signatura digital. Evidentment, la signatura digital és una seqüència de bits, per tant, ha d'haver algun procés que reveli que la signatura no ha estat modificada ni falsificada. Com s'analitzarà més endavant, aquesta autenticació s'aconsegueix amb la criptografia de clau pública.

* Garantir l'autenticitat del contingut i integritat del document digital. Consisteix en assegurar que el document no ha estat modificat per cap individu o factor extern a la comunicació. Als documents digitals la manipulació dels bits que composen el missatge pot fer−se sense deixar rastre. Per aquest factor també és necessària la criptografia simètrica o de clau secreta mitjançant el procés MAC (Message Authentication Code).

* Evitar el rebuig interessat dels missatges per part dels comunicants. El problema sorgeix davant la possibilitat de que l'emissor o el receptor d'un determinat missatge intenti eludir (si li convé) la emissió o recepció d'aquest. Als documents escrits sobre paper es pot evitar això mitjançant un correu certificat amb acusament de recepció, o bé signant el document en presència de testimonis. No obstant, als documents digitals transmesos telemàticament suprimeixen els testimonis en ser un ordinador qui comunica amb un altre. La criptografia moderna ha posat a punt igualment protocols que permeten impedir el retop interessat per part dels comunicants.

* Garantir la inalterabilitat dels documents digitals, ja que és concebible que l'emissor o receptor d'un determinat document pretengui que sigui distint de l'original. Per evitar−lo la criptografia moderna ha desenvolupat dues tècniques bàsiques. Una és la tècnica dels compromisos, que obliga l'emissor a enviar el missatge amb un apèndix o compromís. L'altra tècnica és la notarització electrònica, mitjançant la qual cada missatge està associat amb tots els anteriors enviats pel mateix emissor, de forma que la falsificació requereix el canvi de tots els missatges previs.

* Evitar el problema de la falta de simultaneïtat en les signatures digitals de contractes. En no existir simultaneïtat pot donar−se el cas que l'últim a signar es llenci enrera i no signi. La criptografia moderna ha corregit també aquest problema mitjançant una tècnica denominada transferència trascordada, amb la qual tant l'emissor com el receptor tenen la mateixa probabilitat de posseir una signatura vàlida del contracte.

* Verificar la identitat dels comunicants. També aquest problema ha estat solucionat gràcies al PIN (Personal Identification Number), que ve a ser el DNI digital.

HISTÒRIA DE LA CRIPTOGRAFIA

L'art de la criptografia és gairebé tan −−>anti[Author:d]c com l'escriptura. La necessitat de controlar la comunicació de la informació ve lligada amb tota probabilitat a les formes més elementals de la societat, ja que és en aquestes on apareixen interessos que defensar o protegir.

Es pot determinar com un dels primers mètodes d'encriptació el que anomenem actualment valisa diplomàtica, és a dir, un recipient enviat per algun missatger cap a l'element receptor. En ser un mètode pioner, òbviament disposava de poca seguretat. La possibilitat de vulnerar aquest mètode era substancialment elevada. Només s'havia de capturar el missatger i obtenir la informació que aquest transportava.

Aquest mètode va anar evolucionant per tal d'evitar aquest elevat grau de vulneració. Per això, el que es va fer va ser ocultar la informació transportada, mitjançant el canvi de símbols del missatge, per tal que en cas que el missatger fos enxampat, no es pogués desvelar el secret. Malauradament, aquesta solució requeria una coordinació prèvia entre els participants d'aquesta comunicació perquè els símbols es permutessin pel seu original corresponent.

La criptografia i els egipcis

És molt difícil situar els inicis de la criptografia i els primers mètodes utilitzats. No obstant, ja a l'antic Egipte es van emprar sistemes criptogràfics, i prova d'això són els jeroglífics no estàndard escrits en les parets de les piràmides i algunes tombes. Això data de 4000 anys enrere i el sistema es basa en figures geomètriques i dibuixos, que conformaven un missatge no desxifrable. Aquest sistema, podria ésser realment complex ja que una forma geomètrica indefinida podria dir moltes coses i, alhora, no dir res.

La criptografia grega

No podem parlar de escriptura secreta o xifrada fins el primer cop del qual es té constància històrica. Aquest primer ús el datem al segle V a.C. Com esmentàvem a la introducció la criptografia ha jugat un paper important als assumptes d'Estat, fins i tot, a les guerres.

Precisament, aquesta primera forma de criptografia va sorgir arrel d'una guerra: la guerra del Peloponès. Aquesta va ser una de les primeres grans guerres entre civilitzacions, en concret, entre Atenes i Esparta.

En aquesta guerra, el general Lysandro va rebre en una llista una sèrie de lletres amb aparent falta de sentit. Aquesta llista en ser enrotllada en un determinat rodet de fusta mostrava en l'eix longitudinal els símbols disposats de tal manera que podia llegir−se el missatge, que en aquesta ocasió va suposar la salvació d'un imperi i d'un general. El xifrat a més d'incloure els símbols que composaven el missatge incloïa també uns altres símbols innecessaris que al desxifrar, és a dir, enrotllar el missatge al rodet, desapareixien. Plutarco, biògraf i assagista grec del segle primer, denomina aquest mètode escítal lacedemoni.

La criptografia durant l'Imperi Romà

Un altra mètode dels primers dels quals es té coneixement està datat de l'època dels romans. Aquesta tècnica romana s'efectuava secretament substituint uns símbols per uns altres en el conjunt dels que composaven el missatge, obeint a una certa regla fixa.

També aquest sistema requeria l'acord previ entre emissor i receptor, ja que havien d'estar d'acord en el procediment emprat per ocultar la informació, permetent únicament la seva comprensió als posseïdors del

susdit procediment. A aquest sistema, un dels primers utilitzats d'escriptura secreta, se li denomina mètode Cèsar, i es situa cronològicament al segle I a.C.

L'emperador Cèsar escrivia els seus cònsols, generals i a altres mitjançant una tècnica que consistia a substituir cada lletra del missatge per una altra seleccionada d'una forma fixa. Sens dubte, el mètode Cèsar concentrava el seu ús al camp militar i diplomàtic.

La criptografia des del segle I fins al segle XIV

El temps comprès des de la utilització del mètode Cèsar fins els segles XIII i XIV presenta una important manca de documents que informin sobre l'ús de sistemes d'encriptació en aquest període. En qualsevol cas, és presumible que van continuar utilitzant−se, sobretot en èpoques de guerres. Segurament, els sistemes més utilitzats van ser la substitució de les lletres del missatge per símbols especials i preestablerts.

La criptografia renaixentista

Es posseeixen nombrosos testimonis de l'ús de la criptografia durant l'etapa renaixentista tant a Espanya com a la resta d'Europa. No obstant, aquest ús estava restringit a l'ambient diplomàtic.

Fins al segle XIV i l'època del Renaixement hi ha un buit en el progrés de l'escriptura secreta, al igual que ocorre en uns altres camps de les ciències o de les arts, ressorgint amb Cicco Simonetta, conseller i secretari dels ducs Sforza en Milán entre 1375 i 1383. La seva obra *Liber Zifrorum* es considerada per alguns com la primera obra sobre criptografia que es coneix. A la seva obra estudia i analitza diversos sistemes fonamentals en substitucions simples de lletres i representacions múltiples amb addició de símbols convencionals. Cent anys abans, però, el filòsof i naturalista anglès Roger Bacon (1214−1294), qui per la seva gran aportació a la ciència va ser reconegut com *Doctor Mirabilis* exposà totes les observacions i coneixements de la seva època inclòs un sistema de xifrat de informació denominat *xifrat bilitera*. Aquest xifrat consistia en substituir parelles de símbols del missatge per un o més símbols convencionals.

Els primers en entendre clarament els principis de la criptografia i aclarir les normes del criptoanàlisi van ser els àrabs. Ells van idear i van emprar xifrats de substitució i transposició i van descobrir la freqüència de distribució de les lletres, i amb estudis criptoanalítics, el probable text original. Com a resultat, al voltant l'any 1412, al−Kalka−shandï va poder comprendre un respectable, tot i que elemental, tractament de diversos sistemes criptogràfics a la seva enciclopèdia *Subh al−a'sh* i va donar instruccions explícites sobre com dur a terme els anàlisis criptogràfics a partir del text xifrat i la freqüència de repetició de lletres amb nombrosos exemples que il·lustraven la tècnica.

Una empenta clau a la criptologia, fou donada per Lleó Battista Alberti (1404−1472), nascut a Gènova i educat a Bolonia, que fou secretari pontíficic de la cort romana. Se'l considera el pare de la criptologia i va ser un gran impulsor dels anàlisis criptoanalítics.

El xifrat d'Alberti és un xifrat de substitució simple que es efectuat amb un aparell que consta de dos cercles concèntrics amb un eix comú, dividits en 24 caselles. En l'anell major trobem 20 lletres de l'alfabet, és a dir, totes excepte cinc (H, J, K, U, Y). En l'anell menor hi ha 23 lletres, les 20 anteriors més l'H, la J i la Y. El xifrat s'efectua enfrontant una casella de l'anell exterior amb una altra qualsevol de l'anell interior. Aquesta parella constitueix la clau del xifrat, i amb aquesta correspondència entre ambdós anells es produeix el xifrat. Òbviament, aquest invent requeria canviar la clau amb freqüència per tal d'augmentar−ne la seva seguretat.

Al 1480, Lavinde va escriure el seu *Trattati in cifra*, al qual ell va descriure el primer disc de xifrat. Aquest manual es troba actualment als arxius del Vaticà. Lavinde era secretari oficial de les comunicacions secretes del Papa Clement VII, i el seu sistema de xifrat consistia en utilitzar determinats codis per a substituir paraules del missatge en clar. Aquest tipus de xifrat va ser bastant emprat en el segle XV i XVI no només per les Corts

sinó per unes altres entitats. En aquesta època, tant Venècia com la Cúria Romana empraven codis secrets. Es coneix una carta que l'ambaixador de Venècia va enviar a la cort d'Àustria, a la qual es van emprar codis de tal forma que es van substituir paraules per lletres o per unes altres paraules de significat totalment distint.

Posteriorment, l'any 1563, Giambattista della Porta va proporcionar una forma modificada d'aquest xifrat en forma d'un tauler quadrat a l'obra *De furtivis literarum notis*. Les innovacions de Giambattista van ser més tard estudiades i emprades per Blaise de Vigenère.

Durant el segle XVI, l'historiador i religiós benedictí alemà Trithemius, qui posseïa com a veritable nom Johannes Heindenberg, va publicar la seva obra *Poligraphiae*, a la qual a més d'afirmar que Carlomagno xifrava les seves comunicacions, va aportar una sèrie de mètodes que estaven basats, un en un sistema de diversos alfabets, denominat pel propi autor com *Tabula recta*, i un altre en una substitució de lletres per paraules, a l'inrevés que el mètode de Lavinde.

Dintre del Renaixement italià, en el qual situàvem abans els avenços d'Alberti, van convergir altres estudiosos de la criptografia com Giovanni Belasso i Girolamo Cardano qui a més dels seus estudis en el camp de les matemàtiques i de la física va aportar al camp de la criptografia un sistema basat en una carta o tarja amb forats perforats, de tal manera que proporciona el missatge en clar en col·locar−lo sobre un determinat text preconcebut. Aquest procediment apareix en la seva obra *De rerum varietate*, i posteriorment en les seves obres complertes publicades a Lyon el 1666 amb el nom de *Hieronymi Cardani Opera*.

A Espanya, al igual que la resta d'Europa, la criptografia d'aquests anys estava molt lligada al camp de la diplomàcia. Es tenen documents encriptats datats de l'època dels Reis Catòlics, així com també altres documents amb informació de l'Estat i de particulars. Al territori espanyol l'activitat criptoanalítica i la intercepció de missatges va ser prou intensa. Per exemple, van desxifrar−se les correspondències de Lluís de Requessens, Governador dels Països Baixos. De totes les claus distintes usades en aquest període destaquen les claus utilitzades per Felip II, així com també per D. Juan d'Àustria i el Duc d'Alba. Felip II va adonar−se'n de la importància de la criptografia per ocupar el seu càrrec, per això, segons corrobora una carta del 1556 una de les seves primeres accions com a rei de l'Estat espanyol va ser canviar la clau que emprava Carles V ja que resultava notòriament insegura. També cal esmentar l'ús que va fer Santa Teresa a la seva correspondència de la substitució per símbols.

		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y