
WEST-
OST-
BERLIN
MURO
BERLIN
quetes en la
para facilitar
de miles de
entales • Se
ntaron todas
estricciones
Advertencia
cú contra la
n del país •
ero también
Dos escenas de un día histórico
alemanes del Este se ayudan
por encima del Muro de Ber
mientras otros intentan abrir
IDENTITY CARD
CATZ
TONY
Place of residence
Place of business
Occupation Farmer
Race Jewess
Height 5 feet
Colour of eyes
Colour of hair
Build
Special peculiarities

-

“This is going to be an interesting job, Mata Hari, seducing Prussian Officers…”
M. Batey

“Real Mathematics has no effect on war”
G. H. Hardy

“Si piensas que la criptografía es la solución a tu problema, es que realmente no conoces tu problema”
Peter G. Neumann

“Imagination is more important than knowledge”
A. Einstein

“La Guerra es un arte, y como tal, no es susceptible a una explicación por una fórmula fija”
G. Patton

“Machines take me by surprise with great frequency”
A. Turing

Dedicat a la meva família, i en memòria de Mavis Batey

INDEX

1. Introducció, objectius i justificació del treball

El primer contacte que vaig tenir amb la criptografia va ser a l'estiu del 2012, quan la *Fundación Española para la Ciencia y la Tecnología* i *el Ministerio de Eduación, Cultura y Deporte* em van atorgar una beca, gràcies a la qual, els estudiants becats vam poder passar una setmana a una Universitat de l'estat espanyol, gaudint de les investigacions d'un projecte, que nosaltres havíem escollit prèviament. I és que, cal reconèixer, que al principi el projecte "Más que Núm3ros" no em va cridar especialment l'atenció, però un cop ja me l'havien assignat, vaig descobrir que aquest era un tema que realment em motivava. Durant la setmana que vaig passar al País Basc, vam tractar dos temes: criptografia i probabilitat. Els dos em van captivar, però el primer em va cridar més l'atenció. Allí vaig poder endinsar-me en aquest món matemàtic ple de misteris, un món que utilitzaven ja els antics romans i que ha arribat fins als nostres dies, passant per mètodes criptogràfics al Vaticà i Guerres Mundials. I és que, sense saber-ho, actualment no disposaríem d'un munt de coses si no hagués sigut per la criptografia: targetes de crèdit, contrasenyes, codis de barres, DNI, missatges secrets... Literalment, la criptografia és la clau.

Amb aquest treball vull arribar a conèixer els principals mètodes criptogràfics antics, i alhora tenir una visió prou detallada dels més actuals, com l'RSA. Per aconseguir-ho i poder seguir correctament un fil històric ordenat, creo una novel·la, la qual em permetrà que el que estudio sigui més fàcil d'entendre i alhora més entretingut i original. Així doncs, a l'inici del meu treball, ens situem a un cafè de Berlin, l'any 1964. Ens posem a la pell d'una dona alemanya que, mitjançant tot el que va aprendre de criptografia durant la Segona Guerra Mundial a Anglaterra, ajudarà alguns individus a creuar el mur de Berlin.

Per tal de relacionar aquesta part històrica (i les explicacions de criptografia que comporten) i l'actualitat, recreo el personatge de l'Elisabeth al cap de molts anys, al 2013. Llavors ella ja té 92 anys, i és convidada a una gala per commemorar la tasca que van fer tots els personatges anònims que van col·laborar amb els aliats durant la Segona Guerra Mundial.

Un altre aspecte que vull tractar amb aquest treball és la repercussió que té la criptografia en la societat: vull saber si la gent n'ha sentit a parlar, si saben realment el que és. Per això, al meu treball hi ha un apartat que s'anomena *Curiositats de la Criptografia*. En ell s'hi pot trobar aquesta ciència aplicada en camps no-científics, com per exemple en el cinema, la literatura, museus, art...

La meva principal dificultat a l'hora d'abordar aquest treball de recerca va ser la criptografia actual. Els únics coneixements criptogràfics que tenia jo eren els que vaig rebre durant la meva estada al Campus Científic. Allí només vam tractar els aspectes i mètodes més bàsics d'aquest tema, com ara el xifrat de Cèsar, o el de Vigenère. No vam arribar als mètodes més actuals, com RSA o ASCII. Aquests eren els que realment a mi em preocupaven en un principi, ja que conceptualment són els més difícils d'entendre perquè van lligats completament a la informàtica. Podem afegir una altra preocupació, i és que la part pràctica del meu treball de recerca era l'elaboració de petits programes informàtics que permetessin xifrar i desxifrar un text. Quan se'm va plantejar aquesta idea, jo no em veia capaç de moure'm per programes gaire complexos i no creia que me'n sortís. El que en un principi jo buscava era un treball sobre matemàtiques, i vaig tenir la sensació de que estava molt relacionat amb la informàtica i durant un temps em vaig desconcertar. Afortunadament, més tard vaig tornar a trobar el que buscava en un inici en aquesta petita investigació, i això em va permetre seguir endavant i adonar-me'n de que realment m'agradava aquest tema.

La metodologia que he seguit amb aquest treball va ser, en un primer lloc, documentar-me molt sobre el tema. Per a fer això, vaig fer recerques a internet i vaig consultar llibres de diverses biblioteques.

Quan ja em sentia familiaritzada amb els principals aspectes i el vocabulari específic, vaig decidir començar el treball. Vaig anar redactant petits apartats per tal d'anar formant l'estructura desitjada.

El que també vaig fer, i que considero que em va ser molt útil, va ser contactar amb diverses personalitats relacionades amb el tema de la criptografia, com per exemple, els escriptors dels llibres que llegia, criptògrafs de professió, o inclús un museu dedicat exclusivament a aquest tema, situat a Maryland, EEUU.

Dins d'aquest apartat, m'agradaria anomenar una persona que m'ha ajudat molt, i sense la qual el meu Treball no tindria ni la mateixa informació, ni seria igual. Aquest és en David Juher, un professor del Departament d'Informàtica i Matemàtica Aplicada de la Universitat de Girona i doctor en Matemàtiques per la UAB l'any 2003. Alhora, també he pogut contactar amb Ignacio Luengo y he tingut la sort de rebre contesta de Bletchley Park, un centre d'Anglaterra que va tenir molta importància durant la Segona Guerra Mundial, i en el que està basada la meva part novel·lada. També vull agrair al David Moyano, el meu tutor, per la orientació i l'ajuda que m'ha ofert quan l'he necessitat.

2. Introducció teòrica

Criptologia (del grec *criptos*=ocult i *logos*=tractat, ciència) és el nom genèric que s'utilitza per designar dues disciplines diferents però complementàries: la Criptografia i la Criptoanàlisi.

La Criptografia s'encarrega del disseny, de l'emmascarament d'un determinat missatge per tal que sigui confidencial, i d'aquesta manera, només el puguin entendre les persones autoritzades.

La Criptoanàlisi, per altra banda, és la part de la Criptologia que s'encarrega de trencar els procediments de xifrat, i d'aquesta manera aconseguir recuperar la informació original.
Aquestes dues disciplines s'han desenvolupat paral·lelament, ja que tot mètode de xifrat va acompanyat de la seva Criptoanàlisi corresponent.

Antigament, la Criptografia era un mètode reservat a l'àmbit militar i a diplomàtics, perquè eren els que realment la necessitaven i els que en feien us. Aquesta filosofia ha fet un canvi dràstic si la comparem amb l'actualitat, ja que ara, aquesta disciplina és a l'abast de tothom i més que això, tota la població la necessita. El desenvolupament de les comunicacions electròniques i l'aparició dels ordinadors, fan possible la transmissió de grans fluxos d'informació confidencial que cal protegir d'alguna manera. En aquest punt és quan veiem que la Criptografia passa a ser una necessitat real de l'home que, preocupat, veu que les seves dades privades estan poc protegides. Una amenaça per a la seva intimitat.

La primera data de la que disposem referent a la criptografia és del segle V a.C, durant la guerra entre Atenes i Esparta, quan ja s'utilitzava un sistema per emmascarar els missatges per tal de que l'enemic no els pogués entendre. Era prou bàsic, i actualment ens pot semblar molt fàcil d'interceptar, però en aquella època era prou factible. Es basava únicament en l'alteració de les lletres del missatge mitjançant estris, com una vara i una tira.

Més endavant, al segle II a.C, Polybios, un historiador grec, va dissenyar una graella de 5x5 que permetia intercanviar lletres per d'altres. Aquesta modesta creació va esdevenir la base de moltes altres posteriors.

Tan sols un segle més tard trobem una altra data important en la historia de la Criptografia, quan el conegut Juli Cèsar dóna nom a una de les tècniques antigues més conegudes actualment, el Xifrat de Cèsar. A diferència del que utilitzaven els

espartans, aquest consisteix en la substitució de les lletres per altres caràcters seguint una regla fixa.

Al segle XV s'escriu la que es considera per molts com la primera i més antiga obra que existeix sobre Criptografia, *Liber Zifrorum*, escrita per Cicco Simoneta, conseller i secretari de la cancelleria dels ducs Sforza a Milà. En ella, s'estudien diversos sistemes basats en la substitució de lletres i diverses representacions amb símbols.

Pels voltants de l'any 1466, el que és considerat el pare de la Criptografia, Alberti escriu una altra obra criptogràfica i crea el sistema polialfabètic, que consisteix bàsicament en un mètode de xifrat que alterna diversos alfabets.

Vigenère (1586), després de redactar el *Traicté des Chiffres*, arriba al que es coneix com a primer mètode de xifrat difícil de trencar. Gràcies a aquest fet, l'ús de la Criptografia s'escampa per tots els àmbits referents al poder i que requerissin l'amagatall de missatges, com per exemple secrets d'estat i assumptes militars o d'espionatge.

Les idees criptogràfiques i els avenços perduren durant el temps, i al s XIX tornem a estar davant un esdeveniment important, com són els SIS PRINCIPIS DE KERCKHOFFS, els quals resumeixen les propietats més importants que ha de posseir un bon sistema criptogràfic. Són les següents:

- Si el sistema no és teòricament irrompible, al menys cal que ho sigui en la pràctica.
- L'efectivitat del sistema no ha de dependre de que el seu disseny romangui en secret.
- La clau cal que sigui fàcilment memoritzable de manera que no calgui recórrer a notes escrites.
- Els criptogrames hauran de donar resultats alfanumèrics.
- El sistema ha de poder ser operable per una sola persona.
- El sistema ha de ser fàcil d'utilitzar.

Aquests enunciats, redactats i publicats l'any 1883, van ser modificats i retocats més tard per Claude Shannon, matemàtic americà del segle XX.

Com moltes altres àrees científiques, l'avanç de la Criptografia i l'ús va incrementar durant les dues grans guerres mundials. Aquesta ciència va ser molt necessària a l'hora d'establir comunicacions secretes militars i diplomàtiques, utilitzant noves tecnologies com per exemple la telegrafia i la radiotècnia.

A l'actualitat, degut als avenços informàtics, han sorgit noves aplicacions de la Criptologia per tal de poder manejar la gran quantitat d'informació que circula per les xarxes. Alhora, aquest gran desenvolupament de la ciència informàtica ha fet que canviïn radicalment els conceptes de seguretat que es tenien fins ara, ja que els mètodes que fins a la nostra era eren considerats segurs, al tractar-los amb ordinadors queden exposats a un nivell de risc altament elevat.

Per tal de combatre els possibles *hackers* i els múltiples atacs que aquests envien constantment a la xarxa, la Criptografia ha d'oferir solucions eficients per als quatre problemes fonamentals de seguretat que presenta Internet. Segons David Juher a *L'art de la comunicació secreta: el llenguatge de la criptografia*, són els següents:

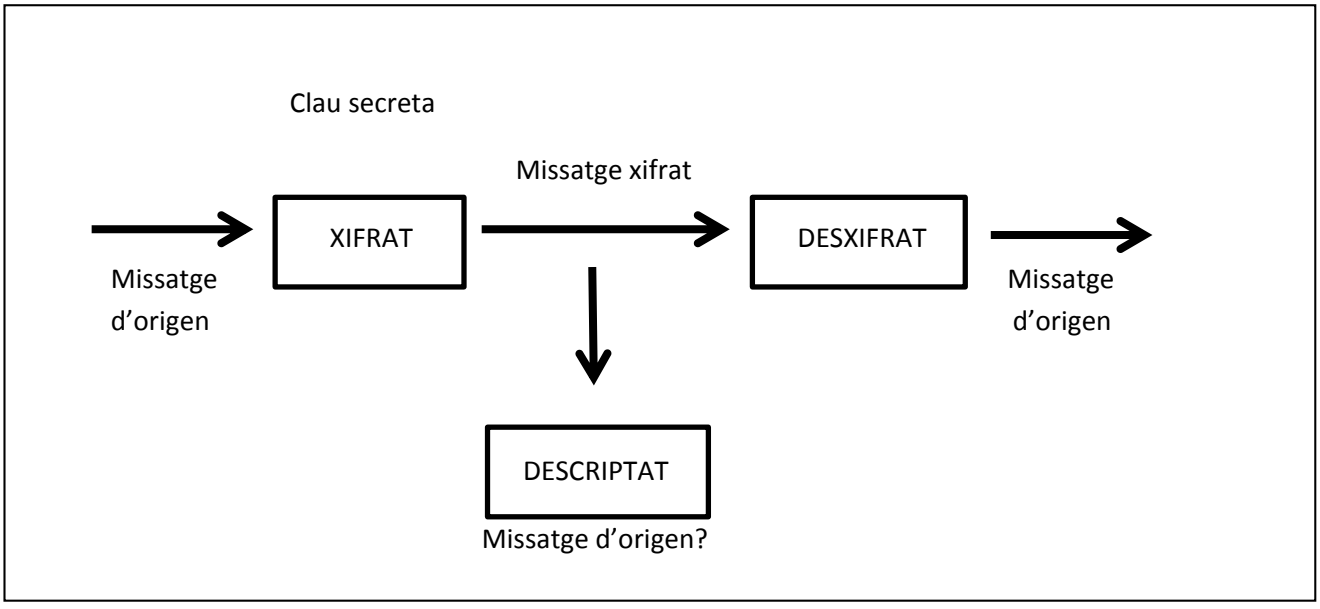
-Confidencialitat: l'assegurança de que el missatge no el pugui llegir ni comprendre ningú més que el seu destinatari

-Integritat: l'arribada completa del missatge transmès, sense canvis ni mancança de dades

-Autenticitat: la identificació real de l'emissor. A Internet, és senzill fer-se passar per alguna altra persona, ja que en les operacions que es realitzen no hi ha cap tipus de contacte "real". Un possible remei a aquest problema seria la signatura digital: un document signat per un individu no pot ser refutat.

-No-repudiació: complementarietat de l'autenticitat. Un cop el missatge és rebut i comprovat, l'emissor no pot negar ser-ne l'autor.

Esquema fonamental d'un procés criptogràfic:

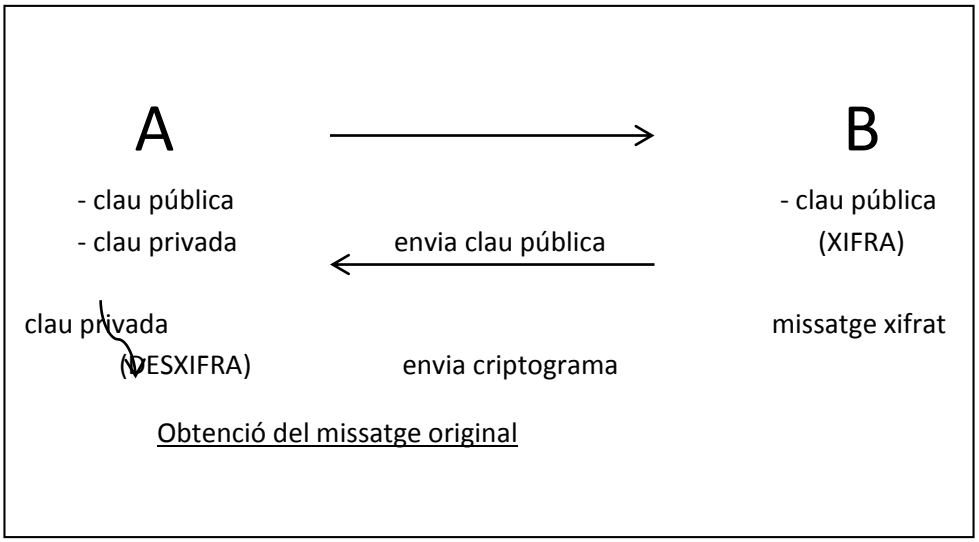


Podem classificar els mètodes criptogràfics segons el tipus de clau que tenen. D'aquesta manera, obtenim:

- Mètodes simètrics: són aquells en els quals la clau del xifrat correspon amb la del desxifrat. Evidentment, aquesta clau ha de ser secreta, per tant, l'emissor i el receptor han hagut d'acordar quina seria.
- Mètodes asimètrics o de clau pública: són aquells en els quals la clau del xifrat és diferent de la del desxifrat. En aquest tipus de criptografia es generen dues claus, una de privada i una de pública. Aquestes claus són nombres primers de molt alta magnitud, per tant és *impossible* desxifrar el text a base de força bruta.

  Un exemple de mètode asimètric:

  El personatge A genera un parell de claus: una d'elles pública i l'altra privada. La primera d'elles, la pública, l'envia al personatge B, que quan la rebi la utilitzarà per xifrar el missatge que vol transmetre. Un cop aquest criptograma arribi a A, mitjançant la clau privada aconseguirà desxifrar-lo i així arribar al missatge original.



Una altra manera de classificar els mètodes criptogràfics és observant quin procediment bàsic fan servir. N'hi ha dos tipus:

- Substitució: el principi de substitució consisteix en establir una correspondència entre les lletres de l'alfabet original i elements de l'altre conjunt, que tant poden

ser el mateix alfabet com un altre. Per tant, es basa en *substituir* les lletres originals per altres elements.

Nosaltres n'estudiarem el *Xifrat de Cèsar* i el *Xifrat de Vigenère*, tots dos molt coneguts. Com a màquina de xifrar, escollim el ***Disc d'Alberti.***

- Transposició (o permutació): els mètodes criptogràfics que segueixen aquest principi no experimenten cap canvi per altres signes, senzillament es canvia l'ordre dels elements del missatge, de manera que el criptograma contingui els mateixos símbols del text clar però en diferent ordre.

  Respecte a aquest principi, estudiarem el *Mètode de Blocs* i el *Mètode de Caixes*. La màquina de xifrar per representar aquest tipus de criptografia creiem que pot ser l'*Escítala espartana*.

Referint-nos a mètodes criptogràfics actuals, estudiarem l'algorisme RSA (Rivest, Shamir i Adleman) i el codi ASCII (American Standard Code for Information Interchange). Tots dos corresponen a la base de les operacions més corrents que es fan actualment per internet, com per exemple la compra online, o la transmissió de dades personals per inscriure's a algun lloc.

L'RSA és un exemple de mètode de Criptografia de clau pública, que com s'ha dit abans, es diferencia dels de clau privada pel fet que es necessiten dues claus diferents per xifrar i desxifrar. Aquestes dues claus són nombres d'una elevada magnitud. Aquests mètodes busquen plantejar a l'atacant problemes matemàtics difícils de resoldre, a diferencia dels de clau pública. El ROT13 em servirà per contrastar amb l'RSA dos mètodes actuals però un simètric i l'altre asimètric.

Com a màquina de xifrat, estudiaré la famosa màquina ENIGMA, un dels millors invents ideats al segle XX. Aquesta màquina va adquirir la fama que té actualment pel fet que va ser la utilitzada pels alemanys durant la II GUERRA MUNDIAL. Per la seva construcció, es van basar en treballs realitzats per Arthu rScherbius, creador d'una màquina comercial de rotors que canviaven lletres per altres .A causa de la seva falta de diners per poder invertir, es va veure obligat a associar-se amb Willie Korn. Entre els dos, en van millorar el disseny i l'any 1923 tenien a les seves mans una nova màquina pràcticament inviolable.

PART 1

3. Novel·la 1

Clac, clac. Clac, clac. Tot i que ja tinc una certa experiència en aquests temes, segueixo estant nerviosa com el primer dia. El ritme dels meus talons picant al mosaic de les rajoles, característic del meu tic nerviós, va compassat amb el timbre del tramvia.
- Només un cafè, gràcies.

Mentre veig com s'allunya la cambrera, faig una visió panoràmica del local. És petit però prou acollidor com per passar-hi una tarda de fred; imagino que el seu èxit és degut al lloc on està situat: ser al bell mig de Berlin, a Kurfürstendamm, aporta molts clients. De fons, a la ràdio, se sent el "Can't buy me love, everybody tells me so, can't buy me love, no no no" dels Beatles, el gran descobriment musical de l'època. A l'armari de costat, un calendari publicitari de Coca Cola: 25 de novembre de 1964. El dia acordat. Hi penso, i comprovo l'hora. Encara és aviat perquè ell arribi. La cambrera torna amb el meu cafè, i una xocolatina Milka. Remeno amb la cullera, i bec un glop de la tassa, de tal manera que deixo la marca del meus llavis vermells a la vora. Un corrent d'aire fred mou els meus cabells rossos i enlacats: algú ha obert la porta. Aixeco la mirada discretament i veig un individu que busca amb la mirada a algú. Duu una bufanda de ratlles que no s'adequa al seu estil mudat. És ell. Ha arribat abans d'hora. Em veu i s'apropa a la meva taula. Es treu el barret, i s'asseu a costat meu.
- Són 6. Ja sé que és més dels que estàvem acostumats a portar, però és estrictament necessari. La partida hauria de ser d'aquí tres dies. Hi ha pressa.

Sis! Com podríem fer-ho? Els altres cops només havíem portat a una persona, com a molt a dues alhora. Sis? Superava les nostres possibilitats: al cap i a la fi, no érem exactament uns professionals.

El jove de la bufanda ratllada, Eberhard Köhler, desplega una petita llista en un paper una mica arrugat sobre la taula. En ell consten sis noms de persones, i he suposat que eren els nostres objectius.

- Un metge, un escriptor, un futbolista, dues professores i una biòloga. Aquests són els que hem de passar.

Llegeixo atentament els noms i cognoms, però no en conec cap d'ells. Bec un altre glop de cafè, ja fred. Així doncs, el nostre objectiu seria passar sis individus de la banda comunista del mur, a la nostra. Suposo que seguiríem el mateix pla que les altres vegades: enviar un missatge a l'altra banda amb el nom de les persones i el punt de trobada, i durant la nit del dia acordat, tindria lloc el transportament.

- No et precipitis, Elisabeth. No podem fer-ho utilitzant el nostre mètode clàssic. Fa un parell de dies, els de la central van intentar portar cap aquí a una família utilitzant les nostres claus i mètodes de xifrat i els de control van interceptar el missatge i van aconseguir desxifrar-lo. Hem de canviar de tècnica, i també de tipus de xifrat. Això sí que és nou. Interceptat i desxifrat un missatge dels nostres. Fins ara havíem utilitzat el mateix mètode: enviar un missatge amb el nom de la persona en qüestió i una direcció xifrats amb una variació d'un dels mètodes clàssics més efectius, Vigenère. Aquest missatge acostumava a passar el mur sense problemes, ja que només era una recopilació de lletres sense sentit que enviàvem dins d'un llibre de Sopes de Lletres, com si es tractés del fulletó de respostes per resoldre aquests jocs d'enginy. L'Eberhard encén un cigarro.

- Està clar que no podem seguir utilitzant Vigenère, com a mínim durant una temporada. Tenim dues possibilitats: una és utilitzar algun tipus de mètode més antic, com ara mètodes bàsics de caixes o fins i tot l'escítala. No em miris així Elisabeth, ja sé que és jugar amb foc, que són fàcils de desxifrar. Però pensa-hi bé, si al control sospiten del missatge, pensaran que s'ha utilitzat algun mètode actual i no pensaran en algun com aquest, tan antic. L'altra possibilitat seria recórrer al clàssic Cèsar, o inclús al bàsic Morse.

Estava clar: si no volíem que ningú desxifrés el nostre missatge, hauríem de fer servir un mètode més antic dels que estàvem acostumats a utilitzar recentment. Acordem que per tal d'assegurar les nostres informacions, redactarem tres missatges. Un seria utilitzant el mètode de caixes, un altre amb Cèsar, i l'últim amb Morse. Tenim poc temps i molta feina. Així doncs, pago el cafè i marxem. Fora de la cafeteria, l'Eberhard em dona una còpia del paper que m'ha ensenyat abans. "Aquest cop encarrega-te'n tu del xifratge. Ja et trucaré". Es posa el barret, i l'home de la bufanda verda i groga marxa. Ràpidament vaig cap al pis per tal de començar amb la tasca. Un cop arribada allí, em trec la jaqueta i el mocador en un moment, i m'assec a la cadira del meu despatx petit i improvisat. A les parets, juntament amb aquell paper de flors extravagants, alguns quadres penjats: retalls de diari de màquines enigma, fotografies amb vells amics, i finalment una imatge amb ell, el meu germà, mort durant la Segona Guerra Mundial. Suposo que va ser la seva mort la que em va fer obrir els ulls i decidir actuar. Recordo que amb només 19 anys, vaig iniciar-me en el món de l'espionatge i els codis secrets. Per què em va interessar? No ho sabria dir. Quan van matar en Kristof, em vaig unir a un grup del que formava part el meu veí per ajudar amb qualsevol cosa que es pogués de la guerra. La guerra havia robat la vida al meu germà i no volia permetre que morissin més innocents. Sóc alemanya, però no

compartia aquells ideals. Sócària d'aspecte i de família, però això no em va importar a l'hora d'apuntar-me a la Resistència. Segons els nazis, jo era i segueixo sent, una traïdora. Durant un temps vaig tenir un lloc molt secundari a l'equip; em limitava a escoltar i mantenir el soterrani on ens reuníem. Un dia, vaig posar-me a ajudar-los més seriosament i van veure que tenia una certa facilitat a l'hora de xifrar missatges. Des d'aquell moment, la meva tasca habitual va ser substituïda per aquesta de nova. L'any 1940 vaig viatjar a Londres amb alguns membres de l'equip, a Bletchley Park. Sense aquell viatge no hagués arribat on sóc ara. Allí, convivint entre ments privilegiades i matemàtics, vaig tocar per primer cop una màquina Enigma. Recordo aquest moment com si fos ahir mateix. També recordo el soroll tan peculiar d'aquelles sales, on molta gent treballava sense parar. Corrien amunt i avall, parlaven, llegien, investigaven, fumaven... tot amb el so de les màquines d'escriure i la radio de fons, per mantenir-se al dia de les notícies. Comparat amb aquell extens edifici, el nostre soterrani a Berlin no tenia res a veure. Allí, vaig tenir la gran sort de conèixer Dilly Knox, conegut actualment com un dels criptògrafs més importants d'aquella època. Anar a Bletchley Park va obrir-me les portes d'una nova visió del món i de la guerra. Res estava perdut si trobàvem la clau correcta.

Em trec el paper de la bossa i l'analitzo bé. Sis noms. A costat, tres direccions. Comença el joc.

Segueixo les instruccions que m'ha donat l'Eberhard: cal redactar tres missatges, dues persones i una adreça per missatge.

Gerard Breuer	ReinhardtStraβe
EldwinRohde	
Gisela Berg	OranienburgerStraβe
Serilda Lehner	
Ernestine Kittel	BehrenStraβe
Heller Weigand	

Començo la meva feina. Els dos primers noms, el futbolista i el metge, els encripto utilitzant el mètode de Cèsar senzill. Faig servir la clau 3, la clàssica. Aquest mètode

no presenta cap dificultat i ho faig prou ràpidament. També encripto la direcció. Ja tinc un missatge llest.

Gerard Breuer JHUDUG EUHXHU

Eldwin Rohde HOGZLQ URKGH

ReinhardStraβe EHKUHQ VWUDBH

Agafo els dos següents noms. Les dues professores. Decideixo encriptar aquests utilitzant el mètode de les caixes. Feia temps que no utilitzava aquest mètode, i això fa que tardi una mica més que amb el primer. La direcció també la xifro, igual que els noms. Preparat.

Utilitzo la clau LLIBRE.

L	L	I	B	R	E
5	4	3	1	6	2
G	I	S	E	L	A
B	E	R	G	S	E
R	I	L	D	A	L
E	H	N	E	R	O
R	A	N	I	E	N
B	U	R	G	E	R
S	T	R	A	β	E

EGDEIGA AELONRE SRLNNRR IEIHAUT GBRERBS LSAREEβ

Miro el rellotge. Són les 3 de la matinada ja. Quan començo a encriptar sempre em passa el mateix, no sóc capaç d'aturar-me. Es tracta d'un assumpte molt seriós, pràcticament de vida o mort, i vull estar segura de que està ben redactat. Per això ho reviso diverses vegades. Tanco aquell pis petit de lloguer i marxo cap a casa. Em poso el pijama i em desmaquillo. Vaig a veure el Max a la seva habitació. Com sempre, s'ha adormit destapat i amb el peluix a terra. L'agafo i li poso entre els braços, el tapo bé i li faig un petó. En Klaus també s'ha adormit, però al sofà. Pel que veig ha intentat esperar-me. El desperto i anem tots dos cap al llit. Fa fred.

L'endemà, després d'acompanyar al Max a l'escola, torno al meu despatx. He quedat amb l'Eberhard perquè m'ajudi: mai he dominat perfectament el codi Morse. Entrem i

ens asseiem davant la taula. Ell encén un cigarro. Entre els dos aconseguim encriptar la informació en poc temps.

Ernestine Kittel · –·· –· · ··· – ·· –· · –·– ·· – – · ·––·

Heller Weigand ···· · ·––· ·––· · ·––· ––· · ·· ––· ·– –· –··

BehrenStraβe –··· · ···· ·––· · –· ··· – ·– ··· ··· ·

Per assegurar-nos que ningú sospiti, transmetrem la informació de la següent manera: la primera l'enviarem dins d'un llibre de Jocs de paraules; la segona dins d'un manual de llengua i la tercera en forma de patró de roba: d'aquesta manera, les ratlles i punts passaran desapercebuts.

Quan ja ho tenim tot llest i preparat i després de prendre un cafè, el meu company marxa per enviar la carta, sense perdre més temps. La meva part ja ha acabat. A partir d'ara, se n'encarrega l'Eberhard.

Sona el telèfon. Estic preparant el sopar del Max. Deu ser la mare. Despenjo. - Elizabeth? Espero no haver-te espantat trucant tant tard, però és de vital importància. Necessitem la teva ajuda. Hi ha hagut un problema i no és segur enviar els missatges per correu tot i que estiguin xifrats. Ens podríem veure? T'espero d'aquí mitja hora al teu despatx.

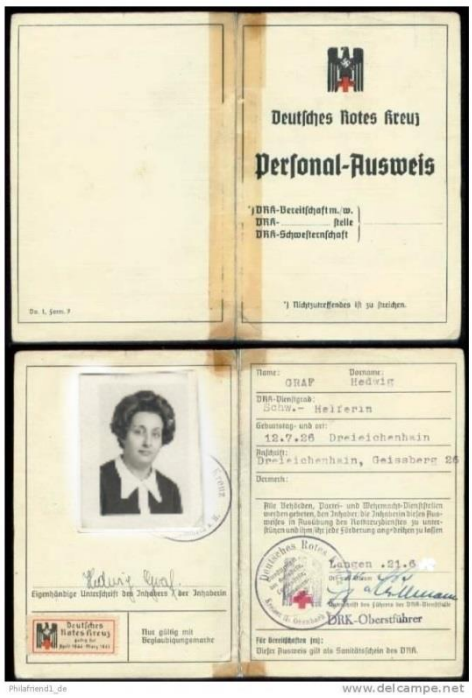
Què pot haver passat? Li vaig deixar ben clar a l'Eberhard quan va néixer el Max que no volia estar en perill, i que per això només m'encarregaria de xifrar. No participaria en altres assumptes més perillosos. Aviso al Klaus de que he de marxar, em vesteixo i surto per la porta.

Suposo que el fet que en Klaus també hagi sigut membre de la Resistència és el que fa que sigui tan comprensiu i entengui que jo arribi tan tard a casa per qüestions de feina. Precisament el vaig conèixer l'any 1940, durant el viatge a Anglaterra. Ell era un home molt atractiu de 24 anys que havia acabat la carrera de medicina, i era un dels que dirigien el nostre equip. La seva valentia i les seves poques ganes de conformar-se amb la injustícia em van cridar l'atenció. Bé, això i la seva mirada blava penetrant. Quan la guerra ja havia acabat, ens vam casar i llavors ell va deixar

la Resistència i tot el que això comportava. Em va dir que havia trobat un nou motiu per seguir vivint i que volia viure tranquil·lament i fugir del context de la guerra. La mort de tota la seva família d'origen jueu l'any 40 als camps d'extermini va fer que entrés a l'equip, sense por a morir ni a perdre el que li quedava. En Klaus no era l'únic jueu del nostre grup, però si el més valent i el que més es va entregar a la seva feina. Fa un temps, quan el mur de Berlin va ser construït, va demanar-me que m'aturés, que deixés de mantenir contacte amb els antics companys: s'acostaven temps difícils i no volia que jo estes en perill. Jo el comprenia perfectament, però el meu desig d'accedir a allò inaccessible, de combatre les injustícies, d'encriptar missatges que mai serien llegits, em va superar.

Kölher m'espera a la porta de sota casa, com m'havia dit pel telèfon. El reconec de lluny per la seva bufanda de ratlles i el cigarro a la ma. Pugem fins a la segona planta, i obro la porta. Al ser en lloc segur, ell comença a parlar.

- Elizabeth ja sé que em vas dir que tu ja no volies estar en situacions de risc i que no volies participar als transports, però aquest cop és molt important. Ens han delatat Eli. Algú s'ha assabentat del que dúiem entre mans i estan retenint tota la correspondència d'aquesta setmana. Sí, ja sé que és il·legal, però tant com tu com jo sabem que això a ells els hi és igual. Només hi ha un possibilitat per fer arribar els missatges al seu destinatari, i tu ets la única que ho pot fer.



Dotze hores més tard, aquí estic jo, a punt de jugar-me la vida per uns papers. Ja no recordava aquestes nits sense dormir, preparant-me amb l'ajuda dels de l'equip, estudiant el pla, el meu diàleg... bé, tota la meva actuació durant les properes hores. Aquest cop m'havia hagut de vestir d'una manera determinada i tot: m'hauria de fer passar per una infermera. Un cop al mes, un grup de infermeres creuaven el mur per tal de visitar un hospital de l'Alemanya Oriental. Durant unes hores hauria de ser una d'elles: hauria d'arribar al mur amb elles, creuar, i un cop a l'altra banda, algú m'estaria esperant a l'hospital en qüestió. Allí, podria entregar-li els tres missatges, i seguir amb el meu paper de infermera. Després, només hauria de tornar amb elles i ja s'hauria acabat.

Són les deu. Estic en mig d'un grup de sis infermeres aproximadament, al CheckPoint Charlie. Estem esperant a que ens permetin el pas a l'altra banda d'aquella alta paret que separava dos tipus de vida. Duc les cartes a la bossa, a conjunt amb l'uniforme. També porto documentació falsa que m'han proporcionat al grup. Sembla que ens deixen passar. Però... ens paren d'una en una i ens regiren el que portem. Intento no posar-me nerviosa, tot i que noto una suor freda per l'esquena. És el meu torn. Em demanen la bossa i l'obren. A dins, hi troben un llibre de Jocs d'Enginy, un manual de Francès i uns patrons per a un vestit. "I tot això?" em pregunta un home, estirant per la corretja a un gos gran. Li contesto que són llibres antics, donació d'una vella biblioteca per a l'hospital. L'home em creu, i me'ls torna. Dins dels llibres, hi ha els missatges encriptats. Afortunadament no se n'ha adonat.

A les dues del migdia, ja sóc a casa. Tot ha sortit bé. Hem pogut creuar totes juntes sense problemes. Un cop arribades a la porta de l'hospital, he reconegut l'home que estava esperant els meus documents. Li he fet entrega dels llibres i he marxat cap a dins de l'edifici amb les demés noies vestides de blanc. Al cap d'una hora, hem tornat totes al CheckPoint Charlie i hem creuat el mur sense dificultats. Era el primer cop que em jugava la vida des de que tenia el Max. Suposo que per això, a l' acabar, enlloc d'anar al soterrani com acostumava a fer abans, he corregut cap a casa per abraçar el meu fill.

Torno a ser amb l'Eberhard a FriedrichStraβe. Són les tres de la matinada i estem esperant el transport de les sis persones del costat oriental. Nosaltres no ens encarregarem de portar-los cap aquí, només esperem rebre notícies de que el pla ha sortit bé. Estem refugiats dins d'un portal. Tot i així, tenim fred. Des del nostre punt observem el CheckPoint Charlie. En cas de que els fugitius fossin descoberts, immediatament avisarien als policies fronterers d'aquest punt de control i nosaltres ho veuríem. Tot està tranquil. Veiem un parell de guardes drets amb gossos descansant als seus peus. Tot sembla calmat i en silenci. De sobte, sentim unes passes darrera nostre. No distingim bé de qui es tracta, fins que no el tenim davant mateix. És en Hans, un noi jove recent incorporat al grup que de moment només s'encarrega de portar missatges i poc més.

- Tot ha sortit bé. Els sis fugitius/ refugiats ja estan en territori segur, tot ha anat segons l'acordat. De dos en dos, s'han reunit a les respectives direccions que vosaltres vau xifrar al voltant de mitjanit, on els esperava un dels nostres enviats allí. Llavors, cada grup de tres s'ha desplaçat fins a les ribes del riu Elba. Allí no hi ha mur, però si diversos paranys: primer una ampla franja de sorra curosament rastellada;

després una forta tanca metàl·lica amb filferro i pues, i una corda de trampa que activa els reflectors al ser tocada. Més enllà, hi ha una zona de mines. Tot i així, han aconseguit traspassar el riu. Ben amagats, han inflat un matalàs i han remat 150 metres en silenci fins a arribar a l'altra vora. Allí, han trobat una furgoneta de la policia occidental.

- És una nit molt freda però sortir a remar- els ha dit un dels agents al veure'ls arribar.

- No quan sis individus neden per fugir de l'Est- ha contestat la biòloga, amb un somriure.

Aquest cop tot havia sortit bé, no hi havia hagut problemes ni cap tipus de contratemps. Els sis individus ja estaven en territori segur, a l'Occident.

El mur de Berlin va separar famílies, amics, coneguts, i inclús treballadors del seu establiment de feina. Durant aquells anys, hi va haver diversos casos d'intents d'escapament, per no dir molts. Però no tots van sortir com el nostre, el d'aquella nit del 28 de novembre de 1964. Alguns intents senzillament van fracassar, però els pitjors van acabar amb la mort dels fugitius. Hi va haver un cas d'una família de vuit persones que després d'inflar un globus aerostàtic, van volar fins a arribar a terreny segur. Un altre cas va ser el de vuit berlinesos orientals que anaven a bord d'un vaixell turístic, i van emborratxar al capità i al maquinista i després van buscar un refugi a la part d'Occident. D'altres més valents, com Harry Deterling, va accelerar el seu tren des d'un soterrani per envestir a tota velocitat les barreres de l'estació Albrechtstraβe, i així obrir-se camí fins l'Oest acompanyat de 24 familiars i amics.

Actualment, el mur ja no existeix. El 9 de novembre de 1989 va ser demolit. Afortunadament, jo vaig ser allí per veure-ho, per veure l'altra banda d'aquella alta paret.

4. Mètodes de xifrat antics

4.1. Substitució

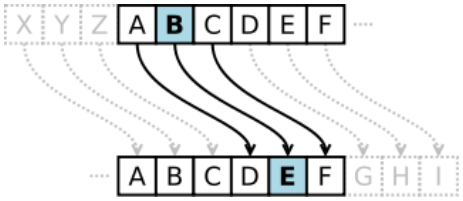
La criptografia per substitució consisteix en reemplaçar una o més entitats, generalment lletres, d'un missatge per una o més entitats diferents. Hi ha diversos tipus de xifrats de substitució:

- La substitució monoalfabètica consisteix en reemplaçar cadascuna de les lletres de l'alfabet per una altra de l'abecedari.
- La substitució polialfabètica consisteix en utilitzar una sèrie de xifrats monoalfabètics que són reutilitzats periòdicament.
- La substitució homòfona fa possible que cadascuna de les lletres del missatge del text es correspongui amb un possible grup de caràcters diferents.
- La substitució poligràfica consisteix en reemplaçar un grup de caràcters a un missatge per un altre grup de caràcters.

4.1.1. El Xifrat de Cèsar

El Xifrat de Cèsar és, sense dubte, un dels mètodes criptogràfics antics més coneguts i alhora un dels més senzills. Segons els historiadors, s'usava aquest mètode per protegir rutinàriament les seves comunicacions d'interès militar.

Bàsicament consisteix en substituir cada lletra del missatge clar per una que estigui a un determinat nombre fix de posicions al mateix alfabet. Així doncs, si posem pel cas que fem un desplaçament de 5, la A passaria a ser la *F*; la B seria la *G*... El desplaçament que usava Cèsar amb els seus missatges encriptats era de 3, per tant totes les A passaven a ser *D* i així fins al final de l'abecedari. Un cop s'arriba al final de l'abecedari, cal fer la volta i tornar a començar. D'aquesta manera, si seguim la norma d'un desplaçament de 3, les V queden substituïdes per *Y,* les W esdevindran *Z*, les X es convertiran en *A*, les Y en *B* i les Z en *C.*



Explicació de la substitució que utilitzava Cèsar

Interpretació matemàtica:

Podríem interpretar aquest desplaçament amb una fórmula matemàtica prou senzilla com la següent: *Yi=Xi+Zi*

on Y és la lletra que obtindrem

X és la variable que pot prendre qualsevol dels valors numèrics entre 0 i 25 (ADVERTÈNCIA: ens basem en l'abecedari català prescindint de la Ç i contant que A=0)

Z és el desplaçament que nosaltres escollim

D'aquesta manera, si volem fer un desplaçament de 3 (com antigament feia Cèsar) i volem veure que obtindrem amb la D=3, resolem:

Yi=3+3=6=G per tant, obtenim que la D quedaria substituïda per una G.

Tot i que aquesta fórmula és correcta, presenta certes limitacions. Per exemple, si x=Y, l'equació quedaria així:

Yi=24+3=27=? Problema: l'abecedari que utilitzem està format per 25 lletres, i segons la fórmula obtenim la vint-i-setena.

En aquest punt és, en el que ens és necessari introduir *l'aritmètica modular*. Necessitem introduir alguna petita correcció perquè quan la X equivalgui a nombres elevats, la Y que obtinguem tingui significat.

Notacionalment, l'aritmètica modular no ens causarà gaires canvis a l'equació que hem trobat. Senzillament, haurem d'introduir *mod(26)* al final d'aquesta. Matemàticament, podríem resumir la seva funció com "cal reduir el resultat fins a un valor entre 0 i 25, si aquest excedeix el límit determinat". Més ben dit, *el valor de k (mod n) coincideix amb la resta que queda quan dividim k entre n.*

Així doncs, per exemple, si busquéssim el valor de 68 (*mod 26*), hauríem de dividir 68 entre 26, i buscar-ne la resta que sobra.

Per tant, 68/26= 26+26+16

D'aquesta manera arribem a determinar que el valor final serà 16, és a dir la lletra Q.

- PROVA PRÀCTICA

Realitzarem una prova pràctica per a demostrar els resultats d'aquesta tècnica criptogràfica de Juli Cèsar. Agafarem com a exemple de missatge el mateix que hem utilitzat amb l'escítala, és a dir: "INVESTIGANT LA CRIPTOGRAFIA".

Utilitzarem exactament la clau que usava Cèsar, és a dir, un desplaçament de 3.

El nostre missatge és el següent:

I N V E S T I G A N T L A C R I P T O G R A F I A

Mitjançant la clau, determinem que canviarem cada lletra per la seva equivalent al desplaçar-la 3 llocs. Per tal de fer-ho més fàcil, crearem una graella que ens ajudarà a l'hora de xifrar el text. La primera fila contindrà l'abecedari català usual, prescindint de la Ç; a la segona fila constaran els nombres equivalents a cada lletra un cop ja estan ordenades alfabèticament; finalment a la tercera apareixeran les lletres un cop feta la transformació de Juli Cèsar.

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	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Seguint la graella, el missatge un cop xifrat quedaria de la següent manera:

L Q Y H V W L J D Q W O D F U L S W R J U D I L D

4.1.2. El Mètode de Vigenère

El mètode de xifratge proposat per el diplomàtic francès Blaise de Vigenère, que no es va difondre fins al segle XVIII, és un dels més característics i més ben aconseguits de la criptografia, ja que combina la simplicitat d'ús amb l'alta seguretat, dos factors molt importants a l'hora de buscar una bona tècnica per amagar els nostres missatges.

La clau en el mètode de Vigenère consisteix en una senzilla seqüència de nombres, de la llargada que es desitgi, tots compresos entre 0 i 25. El funcionament és molt senzill, com ja hem dit abans. Posem per cas que la nostra clau consta de 4 xifres i és la següent: (6,2,16,8). En primer lloc, caldrà que dividim el text original en blocs de 4 lletres, i cadascuna d'aquestes 4 lletres es xifraria seguint el mètode de Cèsar (cada una amb la seva clau pertinent).

- PROVA PRÀCTICA:

Realitzarem un exemple utilitzant el xifrat de Vigenère per tal de veure-ho més clarament. Com en els altres exemples, utilitzarem la nostra frase: “INVESTIGANT LA CRIPTOGRAFIA”

Escollim com a clau la mateixa d’abans, (6, 2, 16, 8). Seguint les instruccions, dividirem el missatge en blocs de 4.

INVE STIG ANTL ACRI PTOG RAFI A

Ara haurem de xifrar cada lletra utilitzant el sistema inventat per Cèsar. D’aquesta manera, podem crear aquesta taula per facilitar-nos la feina.

Alfabet	+6	+2	+16	+8	Alfabet	+6	+2	+16	+8
A	G	C	Q	I	N	T	P	D	V
B	H	D	R	J	O	U	Q	E	W
C	I	E	S	K	P	V	R	F	X
D	J	F	T	L	Q	W	S	G	Y
E	K	G	U	M	R	X	T	H	Z
F	L	H	V	N	S	Y	U	I	A
G	M	I	W	O	T	Z	V	J	B
H	N	J	X	P	U	A	W	K	C
I	O	K	Y	Q	V	B	X	L	D
J	P	L	Z	R	W	C	Y	M	E
K	Q	M	A	S	X	D	Z	N	F
L	R	N	B	T	Y	E	A	O	G
M	S	O	C	U	Z	F	B	P	H

Exemple de graella extreta del llibre *L’art de la comunicació secreta: el llenguatge de la criptografia* de David Juher.

Un cop ja tenim això fet, és molt senzill obtenir el missatge. Anant combinant les lletres arribarem al següent text xifrat

OPLU YVYO GPJT GEHQ VVEO XCVQ G

Per tal de fer el missatge més segur, prescindirem d'espais, ja que amb ells, algú que intercepti el missatge podria conèixer el nombre de xifres que hi ha a la clau, i així tenir més fàcil el seu desxiframent.

OPLUYVYOGPJTGEHQVVEOXCVQG

Aquest mètode presenta unes dificultats analítiques considerables, pel fet que algunes lletres queden xifrades de la mateixa manera tot i que les originals són diferents, i a l'inrevés, pot ser que disposem de dues A, però que una esdevingui una G i l'altra una Q.

4.2. Permutació

4.2.1. Mètode de Blocs i Caixes

Quan dues persones volen intercanviar informació confidencial barrejant les lletres del missatge, és a dir, mitjançant un mètode de permutació, cal que es posin d'acord prèviament en el procediment de la barreja.

Un d'aquests mètodes clàssics, que anomenarem "mètode de blocs" proposa que l'emissor i receptor es posin d'acord en una determinada ordenació dels nombres naturals entre 1 i *n*. Per tal de fer un exemple, prenem que *n*=6. Establim una ordenació de xifres, sis en aquest cas. Així doncs, escollim (4,6,1,5,3,2). Aleshores, el text que nosaltres vulguem xifrar el dividirem en blocs de sis lletres, i a cada un dels blocs aplicarem una permutació (4,6,1,5,3,2), és a dir, la quarta lletra es col·locarà en primer lloc, la sisena en segon lloc, la primera en el tercer, la cinquena en el quart, la tercera en el cinquè i la segona en el sisè.

- PROVA PRÀCTICA

D'aquesta manera, si volem xifrar el text: INVESTIGANT LA CRIPTOGRAFIA, obtindrem:

Text clarament escrit: INVESTIGANT LA CRIPTOGRAFIA

Text en blocs: INVEST IGANTL ACRIPT OGRAFI A

Blocs xifrats: ETISVN NLITAG ITAPRC AIOFRG A

Text xifrat: ETISVNNLITAGITAPRCAIOFRGA

Per a utilitzar aquest tipus de xifrat només cal que l'emissor i el receptor acordin una sèrie de nombres. Si el text que es desitja xifrar és extens, és preferible que aquesta cadena de nombres també sigui llarga per tal d'assegurar-ne la seguretat. No és recomanable deixar constància de la clau per escrit, perquè incrementaríem el risc de descobriment del missatge i això no ens interessa. Per això, per tal de recordar una clau llarga sense apuntar-la enlloc, podem transformar-la en lletres i d'aquesta manera serà més fàcil recordar un missatge que no una llista de nombres sense sentit.

5. Màquines de Xifrat Antigues

5.1. Escítala

Al parlar de Criptografia podem remuntar fins al temps dels espartans, i ja trobem els primers indicis de la preocupació d'amagar missatges. Un element d'aquella època que presenta un gran interès pels investigadors i que actualment és el que més apareix als llibres d'Història és l'*Escítala Espartana.*

Aquest instrument consisteix en dues vares de mateix gruix i una tira de papir o de cuir. El sistema consistia en entregar una vara a cadascun dels dos membres del procés de comunicació: emissor i receptor. L'emissor, per escriure el missatge, enrotllava la tira al voltant de la seva vara formant una espiral i llavors escrivia longitudinalment de tal manera que a cada volta d'aquella cinta aparegués una lletra cada cop. Un cop tot escrit, es desenrotllava de la vara la tira i s'enviava al destinatari. Ell, al rebre-ho, només calia que ho enrotllés de nou a la seva vara per tal de poder llegir el missatge correctament.

Qualsevol persona que hagués interceptat la tira contenint el missatge no hagués sigut capaç de llegir-ne el contingut, ja que es requereix obligatòriament una vara exacta a la que ha utilitzat l'emissor per tal de que les lletres encaixin bé.

L'*Escítala Espartana* és un dels mètodes més senzills de l'anomenada *Transposició o Permutació*, que consisteix en alterar l'ordre dels elements d'un missatge.

Hi ha una manera molt senzilla que ens permetrà entre el funcionament sense la necessitat de reproduir-ho. Posem per exemple que volem xifrar el missatge "INVESTIGANT LA CRIPTOGRAFIA" i suposem que la nostra escítala té 6 capes. Si escrivim aquest missatge en forma de taula de 6 columnes, obtindrem...

I	N	V	E	S	T
I	G	A	N	T	
L	A		C	R	I
P	T	O	G	R	A
F	I	A			

Si llegíssim el missatge per columnes i ignorant els espais, obtindríem el que apareixerà a la tira de papir, és a dir: IILPFNGATIVAOAENCGSTRRTIA
A la taula anterior, s'han respectat els espais per tal de veure el missatge més clar, però és important ignorar-los a l'hora d'escriure el missatge, ja que sinó el que obtindríem seria: IILPFNGATIVA OAENCG STRR T IA i si algun enemic interceptés el missatge, gràcies als espais en blanc, podria tenir més facilitats a l'hora de trobar el missatge.

CONCLUSIONS:

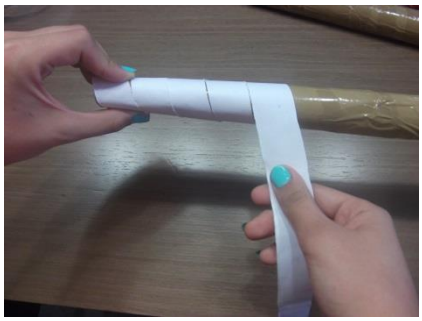
- El nombre de cares i el gruix de la cinta condicionen la longitud del missatge
- És una tècnica relativament fàcil de criptoanalitzar
- Es podria incrementar la seguretat afegint espais en blanc innecessaris

- PROVA PRÀCTICA:

  Realitzarem una prova pràctica per a demostrar els resultats d'aquesta antiga tècnica criptogràfica. Agafarem com a exemple de missatge el mateix que abans, és a dir: "INVESTIGANT LA CRIPTOGRAFIA".

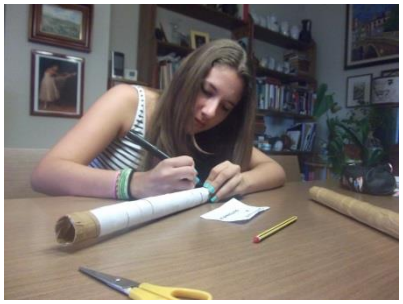
  MATERIALS:

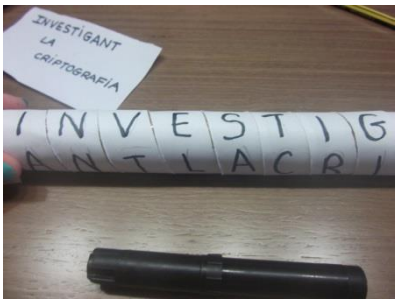
  - 2 vares de mateix gruix
  - una tira de paper
  - cinta adhesiva
  - un retolador
  - un paper per escriure el missatge



PRIMER PAS: enrotllar la tira de paper en un dels dos tubs, de manera que no deixem espai lliure però sense que les capes es superposin.

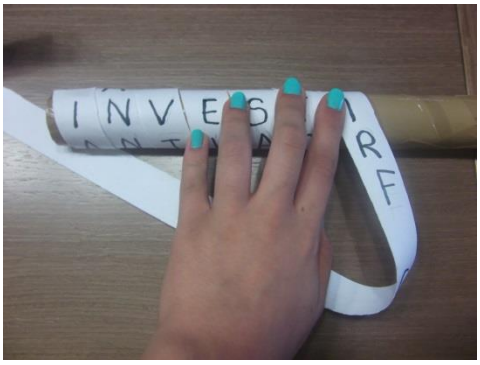
SEGON PAS: escriure el missatge que desitgem transmetre de la següent manera: una lletra per cada capa i de manera horitzontal.

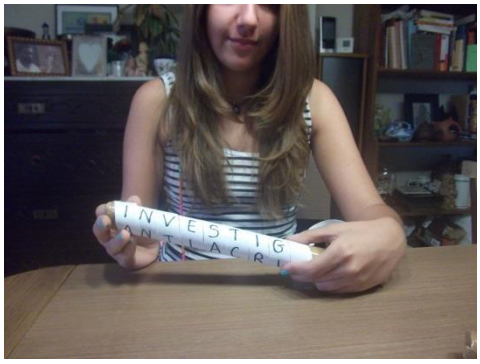




TERCER PAS: desenrotllar la tira de paper. Un cop la tinguem fora de la vara, veurem que el missatge ja està xifrat. En aquest cas, hem utilitzat 8 voltes i per això, la última filera de lletres (la quarta) només contenia una A. Aquest és el motiu pel qual les lletres ens queden separades de tres en tres cap al final. Això és un problema, ja que si algú intercepta el missatge, pot deduir el nombre de fileres que el formen i per tant, obtenir el missatge ocult.

QUART PAS: un cop el missatge arriba en mans del destinatari, aquest només haurà d'enrotllar-lo al voltant de la seva vara, i, com són iguals, coincidiran les lletres i podrà llegir-lo correctament.





5.2. EL DISC D'ALBERTI

El xifrat d'Alberti és el mètode descrit per Leon Battista Alberti al seu tractat *De Cifris* l'any 1466. Aquest tipus de mecanisme és conegut com el primer xifrat per substitució polialfabètic, i el seu ús es combina amb l'ajuda del *disc d'Alberti*, una eina per recolzar aquest mètode.

El disc d'Alberti consta de dues parts: un disc fix (més gran) i un de giratori (més petit). En un inici, en el disc fix hi constaven 24 cel·les, dins les quals hi havia una lletra de l'abecedari llatí en majúscules ordenat alfabèticament, i a les 4 últimes, les xifres 1 2 3 i 4.

En la part giratòria, s'escrivia l'abecedari llatí, incloent els símbols "&" "h" "k" i "y", de manera que també constava de 24 cel·les. En aquest cas no cal que les lletres estiguin ordenades alfabèticament; l'ordre pot ser aleatori o bé el pot escollir el propi usuari.

Aquests dos discs estan units pel centre, amb el disc giratori sobre el fix, de manera que el petit pot moure's respecte al gran. Per tal de poder xifrar un text, l'usuari només cal que emparelli els dos abecedaris en el punt que ell desitgi, per tant, determinarà la clau.

L'inconvenient que presenta aquest tipus de xifrat és que el nombre d'abecedaris creables és limitat: només poden ser 24.

Imatge d'un exemple de disc d'Alberti. El disc intern és el que l'usuari fa rotar per tal de fer coincidir les lletres amb l'altre abecedari tal i com ell vulgui.

PART 2

6. Novel·la 2

Núvols blancs que contrasten amb un cel molt blau. Realment, unes bones vistes. Vistes de llibertat, de joventut i de felicitat. I és que qui hagués pensat que jo, Elizabeth Schneider, tornaria 73 anys més tard a Anglaterra, a Bletchley Park? Qui hagués pensat que una dona, tant vella, de 92 anys, per molt impossible que sembli, estigui dalt d'un avió British Airways, amb una maleta, un bastó, i un necesser ple de pastilles diàries que són un bon indicador d'edat? Si m'ho haguessin preguntat anys enrere, hauria assegurat que això no era possible. Però sí, aquí estic, amb la mateixa valentia que em caracteritzava de jove; la mateixa que quan vaig creuar el mur vestida d'infermera; la mateixa que quan, als 19 anys, em vaig endinsar en el món dels secrets criptogràfics, sense saber les repercussions que això tindria a la meva vida. I és que, per un cop des de fa molt de temps, tot i les pastilles que duc a sobre i les arrugues marcades a la meva cara, em sento jove. I amb il·lusió de nou.

Em miro el meu fill, a costat meu. Dorm. Recordo el dia que va arribar la carta dient que podria tornar a Bletchley Park. Des de la mort del Klaus, fa 17 anys, jo visc amb el meu fill, la seva dona i la seva filla. Tot i que em va costar acceptar la proposta de viure amb ells, després de que el Max insistís molt, vaig acceptar: no era bo que una dona gran estigués sola a una casa gran les 24 hores. Un dia, fa aproximadament dos mesos, el meu fill va rebre una carta. Va arribar a casa, molt emocionat, amb un paper entre les mans i un gran somriure als llavis. Sense ni tan sols saludar, me la va llegir:

"Estimada Senyora Schneider,

em dic Richard Harrison, i sóc un membre de la societat Bletchley Park, treballant-hi actualment com a gerent. Aquest any, 2013, commemorem els 20 anys de funcionament del centre com a museu. El proper dia 7 de maig, aprofitant la diada anual al museu per celebrar la rendició alemanya de l'any 1945, es celebrarà una gran conferència, on hi seran presents les personalitats més destacades que han passat pel centre Bletchley. Així doncs, em complau convidar-la com a invitada d'honor als nostres actes. A les nostres bases de dades apareix el seu nom i tota la seva trajectòria, per tant, penso que seria una bona idea que vostè dediqués unes paraules al públic explicant la seva versió i experiències, així com encoratjant a futurs criptògrafs informàtics de l'actualitat. Si volgués venir, posi's en contacte amb nosaltres i l'avisaríem del funcionament de la quedada.

Esperant la seva resposta amb ànsia,

Richard Harrison

Bletchley Park"

No m'ho podia creure. No podia imaginar-me que m'haguessin escollit a mi com a convidada d'honor. Jo, que havia desitjat durant molt de temps tornar allí, i tornar a mantenir aquelles llargues converses amb intel·lectuals del món de l'espionatge... podria tornar a fer-ho, i a més, com a convidada especial. No hi va haver cap tipus de dubte en que acceptaria la invitació. El meu fill, abans de que tingués temps de demanar-li, va dir-me que m'hi acompanyaria: li havia parlat tants i tants cops sobre les meves experiències que ell i tot tenia molta il·lusió d'anar-hi.

Aquí estem els dos, a punt d'arribar a l'aeroport de Londres. Allí ens espera un cotxe que ens portarà a l'hotel per poder descansar, i demà al matí anar a Bletchley Park. El meu fill es desperta i em somriu. Estem a punt d'aterrar. Les hostesses van a seure a les seves respectives cadires i es corden els cinturons. M'agafo fort a la cadira: no estic acostumada als avions, i tot i tenir 92 anys, la gent gran també te pors. Es sent un soroll fort i uns cops bruscos: ja hem tocat terra. Agafem les nostres jaquetes i baixem. La meva rapidesa és molt diferent a la de l'últim cop que vaig viatjar a Anglaterra: en aquell temps caminava ràpidament i anava amb bicicleta als llocs. Ara, això ja no ho puc fer. És més, he d'agafar-me al meu fill i recolzar-me al bastó per poder caminar. Però bé, ha sigut una sort poder arribar a aquesta d'edat i d'aquesta manera, perquè dels meus antics amics, que tenien la mateixa edat que jo, ja quasi no me'n queden vius.

Baixem una rampa i el meu fill s'encarrega d'agafar la nostra maleta de la cinta transportadora. Fora, ens espera un home, ben vestit, amb un cartell amb el nostre nom. Ens hi acostem. Ens diu que és el taxista que han enviat per a que ens porti al nostre hotel.

Milton Keynes és bonic, tot i ser una New Town i no tenir una història. El paisatge és verd, ple d'arbres i un cel característic del Regne Unit. Des de la finestra del taxi, netejada curosament, veig gent passejant protegits de la pluja pels seus paraigües. Els contrastos de colors d'aquests objectes fan encara més variat i viu el paisatge. M'agrada molt aquest clima, em recorda als anys 40... em sento com a casa.

Arribem a l'hotel, i en Max m'acompanya a l'habitació. Descarreguem i aprofito que ell baixa a pactar els menús d'esmorzar i de sopar per asseure'm al sofà i treure una llibreta i un bolígraf. El bolígraf d'en Klaus, que sempre duc a la bossa. Començo a escriure sense aturar-me el que diré l'endemà a la conferència. Escric tot el que penso, i a l' anar-ho recordant se'm van posant llàgrimes als ulls.

Són dos quarts de vuit del matí. Ens aixequem per anar a esmorzar i tot seguit cap a Bletchley Park. Esmorzo ràpid: he esperat 73 anys per tornar i no vull perdre ni un segon més. M'he posat un vestit nou de seda, d'un color carmí. Va a conjunt amb els meus llavis, i contrasta amb els meus ulls blaus com el cel. Agafo la bossa i baixem fins arribar al cotxe.

Arribem a Bletchley. Començo a conèixer la ruta. No ha canviat tant des de l'últim cop. Però jo si que he canviat. Sóc molt més vella. I no tinc el Klaus amb mi. No puc evitar que se m'escapi una llàgrima i que rellisqui per la meva galta vermellosa. A mesura que ens anem acostant ho vaig recordant tot millor, com si ahir mateix hi hagués sigut. El camí, els arbres... inclús m'arriba l'olor de cigarret que feien els despatxos. I finalment, allí està. Davant meu. Torno a tenir aquell gran edifici davant els meus ulls. Amb les seves altes finestres, els arcs... tot està igual. Els meus ulls, submergits sota les llàgrimes, tornen a veure el que havien vist anys enrere. M'imagino els meus companys, passejant per aquella gespa. Alguns rient, d'altres engrescats discutint sobre algun full que tenen a les mans. I allí, al fons, veig en Klaus. Aquell home del que em vaig enamorar en aquell viatge. Em somriu des de la distància, i em convida a entrar. Així doncs, baixo del cotxe i entro al centre.

A la porta m'espera el gerent que em va enviar la carta, que em rep amb molta amabilitat. A dins, tots saben qui sóc i acudeixen a mi per saludar-me. Donem un tomb per dins de l'edifici, per les instal·lacions. Una jove ens fa una visita guiada a mi i al meu fill pel museu. Realment, està molt ben fet. Està tot ple de documents, i de maquetes. Acostant-me bé, començo a reconèixer gent a les fotografies exposades. Veig la Frida, aquella noia nascuda a Munich que es va casar amb un militar; també veig la Dietlinde, una noia d'ulleres i molt joveneta que dinava cada dia amb mi... i allí... a una fotografia del costat, em reconec a mi mateixa. No recordava el moment d'aquella imatge: em veig asseguda, aplicant-me amb uns documents, escrivint. Quins records. Se'm dibuixa un somriure als llavis al veure'm. Recordo en aquell moment també en Samuel, un bon home que vaig conèixer mentre jo tornava a residir a Berlin. Era jueu, i tenia

una història ben curiosa. Em va explicar que ell va rebre formació matemàtica, ja que el seu pare era un gran matemàtic i, tot i que els nazis no li van deixar acabar els estudis de secundària per les restriccions a l'accés a l'ensenyament que tenien els jueus als anys 30, ell li feia classes particulars i en gaudia molt... En una de les classes, li va fascinar una cosa que li va explicar el seu pare sobre el número pi: té infinites xifres decimals que no es repeteixen mai, i estan distribuïdes de manera tan aleatòria que qualsevol cadena finita de xifres que puguis imaginar-te, per exemple 31101918, que era la data del meu naixement, es troba en algun lloc del número pi!! Utilitzant unes tècniques de càlcul una mica avançades que el noi no vaig acabar d'entendre, el pare i ell van calcular els primers 1000 decimals de número pi. Són aquests:

3.14159265358979323846264338327950288419716939937510582097494459230781
64062862089986280348253421170679821480865132823066470938446095505822317
25359408128481117450284102701938521105559644622948954930381964428810
97566593344612847564823378678316527120190914564856692346034861045432
66482133936072602491412737245870066063155881748815209209628292540917536
43678925903600113305305488204665213841469519415116094330572703657595
91953092186117381932611793105118548074462379962749567351885752724891
22793818301194912983367336244065664308602139494639522473719070217986094
37027705392171762931767523846748184676694051320005681271452635608277
85771342757789609173637178721468440901224953430146549585371050792279
68925892354201995611212902196086403441815981362977477130996051870721134
99999983729780499510597317328160963185950244594553469083026425223082
53344685035261931188171010003137838752886587533208381420617177669147
30359825349042875546873115956286388235378759375195778185778053217122680
66130019278766111959092164201 99.

En Samuel sempre portava a sobre un full de paper amb aquestes mil xifres, escrites a mà pel seu pare. Durant la guerra, aquest paper li portava molts records, ja que al seu pare el van matar els nazis en un camp de concentració, i aquest full de paper era l'únic objecte que jo conservava d'ell.

Quan va entrar a col·laborar amb nosaltres, quan es trobava en una situació compromesa feia servir aquest mètode per xifrar un missatge. Per exemple, "perill" ho xifrava així: triava una posició entre 1 i 1000. Per exemple, 45. Aleshores, mirava les xifres del seu full de paper que es trobaven a partir de la posició 45: són

93751058209749... Llavors, a cada lletra del seu missatge li sumava el número corresponent a aquesta seqüència. Per exemple,

“p”	+	9	=	y
“e”	+	3	=	h
“r”	+	7	=	y
“i”	+	5	=	n
“l”	+	1	=	m

"l" + 0 = "l"

Així, el missatge quedava "yhynml". A més, després de xifrar el missatge posava "yhynml45". Aquest 45 indicava a la persona receptora del missatge la posició decimal del número pi a partir de la qual calia buscar la clau utilitzada. Evidentment, en aquella època poques persones a Europa eren capaces de generar els primers 1000 decimals del número pi, però els que sí que ho sabien fer eren els serveis d’intel·ligència de Bletchley Park.

Un cop la nostra visita s’ha acabat i ja ens hem acomiadat del gerent i els treballadors, marxem a l’hotel. Em sento molt cansada, i he d’estar bé per a aquesta nit.

Al voltant de les 7 del vespre, tornem a sortir de l’hotel direcció el teatre. Allí és on es farà l’homenatge central, i és on jo hauré de parlar. M’he tornat a canviar de roba. És una ocasió especial i cal estar presentable. Porto un vestit negre amb unes petites pedres brillants. Discret però sofisticat. M’he pintat els llavis d’un vermell marronós, i porto el cabell enlacat. Em miro l’anell de matrimoni, sobre les meves mans arrugades. “Això és pels dos, Klaus.” Surto per la porta.

A l’ arribar me n’adono de que realment hi ha molta gent. No em pensava que tant de públic s’interessés per temes com aquests. A la porta, un munt de flaixos immortalitzen l’entrada de diverses personalitats. Quan sortim del cotxe el meu fill i jo, tots els objectius es giren cap a nosaltres. La gent se’ns acosta, ens saluda: tothom ens coneix, i nosaltres no sabem qui és ningú. És una experiència realment estranya. Somriem a les càmeres i entrem a dins. Seguim les indicacions d’una organitzadora, que ens indica la porta per on hem d’entrar a la sala d’actes. Està tot ple de gent; em recorda l’estrena d’una obra de teatre que vaig anar amb el Klaus a Berlin l’any 1948. Aquella nit va ser un dels millors moments de la meva vida, un dels millors records que conservo amb el Klaus. Estàvem els dos somrient, feliços, amb els nostres amics al

FriedrichstadtPalast. L'obra, "Die Büchse der Pandora ", era la novetat de l'any i va aconseguir un gran èxit. Guardo amb molt d'afecte tots aquests records, i sovint torno a ells per gaudir-ne. Per tornar a estar amb tots aquells que avui ja no hi son.

Estem llestos per entrar. La gran porta que tenim al davant s'obre, i es descobreix l'interior d'aquella gran sala. El públic, a l'uníson, comença a aplaudir, tot aixecant-se. Agafo fort al meu fill i comencem a caminar. El teatre, mudat amb teles vermelles de vellut i decorats en color or, dona un aire de gran sofisticació a l'acte. Caminant pel passadís central d'entre els seients, observo els estranys que m'aplaudeixen, com si fos una estrella de cine. Com pot ser que tota aquesta gent em conegui, i jo no sàpiga qui és cap d'ells? Mai hauria pensat que m'esperaria això al tornar a Bletchley. És més, no m'esperava ni que tornaria. Jo fins fa uns mesos em pensava que tothom havia oblidat els que vam treballar al centre, i que desconeixien el treball que vam fer i la nostra funció. Però pel que veig, això no és així. Arribem al final del passadís central, i el meu fill m'ajuda a pujar les escales fins a l'escenari. A dalt, trobo en Richard Harrison i dos nois joves i ben vestits que m'entreguen un ram de roses vermelles. Els aplaudiments no s'aturen, el públic encara està dret i somrient. Harrison, sorprès pel gran entusiasme del públic, s'acosta al micròfon entre riures.

"Quina ovació més inesperada!! Bé, senyores i senyors, com ja saben avui commemorem com cada any, la rendició alemanya de l'any 1945. Però aquest any encara és més especial, ja que celebrem els 20 anys del museu de Bletchley Park. Per aquest motiu, durant aquesta setmana s'han organitzat diverses activitats, amb la finalitat de festejar aquest esdeveniment i alhora de promoure i donar a conèixer el museu. Avui, per concloure els actes i donar per acabada la celebració, ho fem de la manera més especial que ho podíem haver fet: tenim aquí, davant nostre, la única supervivent de l'equip que va actuar durant la Segona Guerra Mundial, i per tant, podem dir que gràcies a ella i a la seva feina, al igual que els seus altres companys, la guerra va acabar abans de l'esperat. Tenim la gran sort avui de que ella, estigui entre nosaltres, per parlar-nos i explicar-nos tot el que ella vulgui. Ella és una petita representació del gran nombre de persones atrevides i valentes que es van jugar les seves pròpies vides i les de la gent que estimaven per lluitar contra la injustícia. Si us plau, un altre cop, un gran aplaudiment per la Elizabeth Schneider."

De nou, el públic s'alça amb aplaudiments i xiulades. El meu fill m'acompanya fins al micròfon. Desplego el meu paper sobre el faristol i em miro el públic, tota emocionada. Els hi dirigeixo unes paraules de incredulitat i agraïment, i tot seguit, començo a llegir el que ahir vaig escriure a l'hotel.

“No tinc paraules. No tinc paraules per descriure com em sento en aquest moment. No pensava que hi hagués ni la meitat de la gent que hi ha aquí, i no esperava que ningú em conegués. Ni a mi, ni a la meva feina. I és que com acaba de dir en Richard Harrison, jo només sóc una petita representació de totes les persones que van actuar durant aquells anys, de totes les persones que no van tenir por d’enfrontar-se als nazis i de posar la seva vida en perill. La meva decisió d’anar de viatge l’any 1940 cap a Anglaterra, amb només 19 anys, i afegint-me a un grup de complets desconeguts, va ser una de les millors de la meva vida. El grup de resistència de Berlin vam arribar a aquest centre i vam ser acollits perfectament. Vam treballar conjuntament amb els desxifradors d’aquí, i ens vam ensenyar mútuament. Jo, que era una noia molt jove i desconeixia completament aquest món, vaig aprendre molt durant aquells mesos que vaig passar aquí. Conèixer tanta gent, aprendre tanta tècnica i viure tantes experiències noves va fer que jo madurés molt com a persona. Aquí vaig passar 8 mesos , i llavors, quan ja tenia la tècnica ben perfeccionada i ja havia aportat l’ajuda necessària, em van avisar des de Berlin dient-me que necessitaven la meva ajuda. Durant un parell d’anys vaig quedar-me a Berlin, com a membre d’un grup que xifrava missatges per als avions dels aliats. Llavors, em vaig haver d’ocupar d’un altre tipus d’afer, més perillós que aquest: vaig haver d’infiltrar-me dins dels edificis oficials nazis, fent-me passar per una jove atractiva de raça ària que va aconseguir enamorar a un dels generals. Amb aquesta tàctica, vaig accedir a informacions secretes i vaig ser testimoni d’escenes que ens van servir més tard per a l’espionatge d’un d’aquests generals. Sense dubte, aquesta va ser una de les missions més complicades que vaig dur a terme. Llavors, jo ja estava casada amb en Klaus Müller, un atractiu doctor membre de la Resistència que vaig conèixer al viatge al Regne Unit i del qual em vaig enamorar perdudament. Fins al final de la guerra vam seguir amb agrupaments de la Resistència. Sabíem que ens estàvem jugant la vida, que en qualsevol moment un tirador ens podria disparar amb una arma, però el nostre desig d’acabar amb el comandament de Hitler era molt superior a qualsevol por o temor. L’any 1957 va néixer el nostre primer i únic fill, el que ara mateix està a costat meu, el Max. El seu naixement va fer que el meu marit i jo ens replantegéssim tots aquells perills, ja que ara teníem un fill al nostre càrrec. Però bé, tampoc calia amoïnar-se gaire, ja que la guerra ja havia acabat, i no teníem cap objectiu ni missió. Això va canviar, però, l’any 1961, tot va tornar a canviar. La construcció del mur de Berlin va fer que antics companys es posessin en contacte amb mi: havíem de tornar a transmetre informació utilitzant la criptografia. El meu marit ja no va tornar a cap grup, ni tampoc va participar en cap més missió: havia trobat un motiu per voler mantenir-se viu, el Max i jo, i no volia exposar-se a la mort. Durant uns anys, vaig encarregar-me de passar missatges

d'una banda a l'altra del mur per tal de transportar famílies des de la banda comunista, però sempre ho feia amb prudència i exposant-me al mínim perill possible. Així va ser fins que el mur va ser tirat a terra. Llavors vaig viure la meva vida normal, sense relacionar-me amb la criptografia. Mantenia contacte amb alguns dels personatges que vaig conèixer aquí, a Bletchley Park, però poc a poc els vaig anar perdent. Avui, 73 anys després d'aquell viatge, torno a ser aquí. Ara ja sóc una senyora molt gran que quan pensa en tot el que va fer en el passat se li omplen els ulls de llàgrimes per no poder-ho tornar a fer mai més. No me'n penedeixo de res del que vaig fer, i és més, si ara m'ho tornessin a proposar, ho tornaria a fer. Perquè? Les guerres no són bones. No hi ha res pitjor que veure dos humans del mateix nivell lluitar entre ells. El que comença sent un conflicte entre dos, acaba sent una declaració de mort a qualsevol individu. Perquè a les guerres moren més innocents que culpables, i això és la injustícia més gran que es pot cometre. Moltes gràcies."

Acabo de parlar, amb els ulls blaus plens de llàgrimes. En Max, a costat meu, també està emocionat. Un silenci envaeix el teatre. De cop i volta, i per tercera vegada, el públic s'alça amb grans aplaudiments i cares d'admiració. En Richard Harrison se m'acosta i m'entrega una placa amb el meu nom i el logotip de Bletchley Park. M'agraeix la visita i després d'algunes fotografies, baixo per les escales i ens asseiem a unes butaques de primera fila.

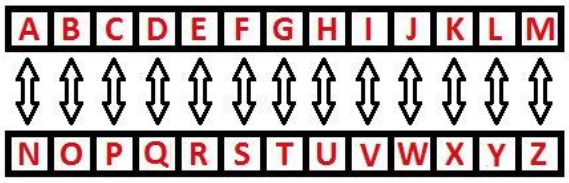
La vetllada continua, amb altres intervencions i pujades a l'escenari: hi ha música clàssica en directe, poesies, i inclús un recopilatori en imatges i vídeo de tota la història del centre, tant com a museu com quan estava en ús. Al final de l'acte, ens conviden a passar a una sala a l'entrada del teatre on hi ha un pica-pica i begudes. Un cop allí, molta gent s'acosta per felicitar-me per la meva tasca i la meva explicació. Alguns em fan preguntes, d'altres es limiten a observar-me sense atrevir-se a dir-me res, i d'altres es fotografien amb mi. Hi ha molt bon ambient. Un home d'aspecte agradable i interessant se m'acosta i es presenta. Es diu David Juher, i em diu que és un professor de matemàtiques molt interessat en la criptografia. Tant, que ha escrit llibres tractant aquest tema. Em sembla interessant conèixer més sobre els nous mètodes, per no quedar-me enrere i així també aprendre coses noves: m'encanta que m'ensenyin i m'expliquin. Així doncs, li dic d'anar a seure a uns sofàs que hi ha a l'altra banda de la sala per estar més còmodes. Un cop allí, comencem a parlar i parlar. Trobava a faltar parlar obertament d'aquests temes, i més amb algú que sàpiga de què parlo. Aquella situació em recorda als temps passats, quan entre tres o quatre membres d'un grup discutíem sobre els mètodes que havíem d'utilitzar, o com havíem de dur a terme alguna missió. En David m'explica que ell viu a Catalunya, i que va

arribar a la criptografia de manera casual, durant l'últim curs de la carrera. Els seus primers coneixements van néixer arrel de llegir un llibre força complex, *Introduction to Cryptography*. La meva curiositat em supera, tot i tenir 92 anys, i li demano que m'expliqui coses de les aplicacions de l'actualitat. Estava convençuda que una ciència com aquesta hauria desaparegut pràcticament, però ell em rectifica. Em diu que cada cop, amb les noves tecnologies, més i més persones s'interessen a aquesta ciència. Inclús hi ha empreses que s'hi dediquen plenament! La criptografia és la base de qualsevol tràmit que es faci per internet, com per exemple a l'hora de comprar, o bé de matricular-se a una Universitat no presencial. En David m'explica que la criptografia actual es basa en realitzar-la amb ordinadors, ja que tenen la capacitat de calcular xifres enormement grans que puguin fer servir per xifrar, i d'aquesta manera el missatge es converteix en gairebé impossible de descobrir sense la clau. Tot i això, m'assegura que entre la criptografia de la seva època i la meva no hi ha una diferència tan radical com pot semblar. Antigament, em diu, les lletres del missatge es barrejaven o bé es canviaven en altres símbols. En el fons, els mètodes que fan servir els ordinadors són els mateixos, però a nivell de bits, és a dir, dues xifres (0 i 1) enlloc de lletres, i amb una gran rapidesa. Noto que ja em perdo amb aquests nous tecnicismes, i que possiblement, jo ja no sabria xifrar amb la criptografia actual ni l'entendria. Ell, en canvi, m'afirma que tot i que és veritat que la criptografia moderna és més complexa que la clàssica, qualsevol persona pot entendre'n el funcionament bàsic sense entrar en gaires tecnicismes. La nostra conversa segueix, entre riures i preguntes, fins que gairebé no queda ningú més a la sala. Ja és molt tard, i hem de marxar cap a l'hotel. Demà mateix hem d'agafar un avió per tornar cap a casa, i hem d'estar descansats. M'acomiado d'en David Juher. M'ha encantat conèixer-lo. M'he tornat a sentir jove quan m'explicava i m'intentava ensenyar sobre la criptografia actual. Inclús jo li he ensenyat coses: li he pogut explicar detalladament algunes de les meves experiències i aventures, i pel que sembla li han agradat molt. En unes poques hores s'han pogut relacionar més de 60 anys d'història d'una ciència, contrastant l'actualitat del passat i ensenyant-nos l'un a l'altre. Agafo el meu abric i sortim en direcció a l'hotel. M'assec al taxi i contemplo per últim cop aquell edifici. Potser per molta gent aquell és un edifici com qualsevol altre, i no entenen els meus sentiments. Però jo si. I llançant lentament un petó des del vidre ben netejat d'aquell taxi número 216 m'acomiado, ara sí, per últim cop de Bletchley Park. M'ha encantat tornar-te a veure, vell amic.

7. Mètodes criptogràfics actuals

7.1. ROT13

ROT13 és un mètode criptogràfic clàssic basat en el xifrat per substitució. Del seu nom, deduïm que es tracta de "rotar 13 posicions". Això consisteix en el desplaçament de les lletres de l'alfabet llatí, substituint cada lletra per la que està a 13 posicions d'ella.



A l'esquema veiem el funcionament d'aquest mètode: la A es converteix en N; la B en O; la C en P... i així successivament, fins que arribem a la N, on aquesta seqüència s'inverteix, i llavors la N passa a ser una A, la O una B...

ROT13 és una variació de l'original Xifrat de Cèsar, i presenta una petita millora respecte al ROT-N, on el valor de N no està determinat: en el cas del ROT13, podem utilitzar el mateix algoritme tant per xifrar com per desxifrar, ja que l'alfabet conté 26 lletres i 13 ·2=26. Per això, aquest mètode és idoni per xifrar missatges d'un alfabet de 26 lletres.

<u>Interpretació matemàtica:</u>

Podem explicar el funcionament del mètode ROT13 amb funcions matemàtiques. Establim aquesta funció:

$$f(n) = \begin{cases} n+13 & \text{si } 1 \le n \le 13 \\ n-13 & \text{si } 14 \le n \le 26 \end{cases}$$

Numerem les lletres de l'abecedari de 1 a 26, prescindint per tant de la Ñ. Per exemple, si volem xifrar el text: CRIPTOGRAFIA tenim que C=3; R=18; I=9; P=16; T=20; O=15; G=7; R=18; A=1; F=6; I=9; A=1.

Aplicant la fórmula arribem a la conclusió que:

f(3)=3+13=16=P
f(18)=18-13=5=E
f(9)=9+13=22=V
f(16)=16-13=3=C
f(7)=7+13=20=T
f(18)=18-13=5=E
f(1)=1+13=14=N
f(6)=6+13=19=S

f(20)=20-13=7=G f(9)=9+13=12=L
f(15)=15-13=2=B f(1)=1+13=14=N

El missatge xifrat, per tant seria: PEVCGBTENSLN

Per obtenir un altre cop el missatge original, cal realitzar la mateixa tasca però a l'inrevés.

Actualment, el xifrat ROT13 no s'utilitza per tractar informació de comerç electrònic o de bancs perquè no ofereix seguretat real. És un xifrat dèbil que al utilitzar un desplaçament constant, no té clau, i per desxifrar-lo l'atacant només cal que sàpiga que està fet amb aquest mètode. Avui en dia, el mètode ROT13 té la mateixa utilitat que als anys 80: s'utilitza per ocultar respostes d'endevinalles i jocs de mots. A part d'això, aquest mètode sí que s'utilitza combinat dins d'alguns llenguatges de programació, com per exemple amb el Java.

7.2. RSA

L'RSA (Rivest, Shamir i Adleman) és un sistema criptogràfic de clau pública que va sortir a la llum l'any 1978. Actualment, és l'algoritme més comú i és vàlid, tant per xifrar com per firmar digitalment.

El funcionament de l'RSA es basa en la dificultat per factoritzar grans nombres enters. Tot i que aquests processos són realment, bastant complexos, es poden estudiar de manera prou senzilla, prenent com a exemple nombres petits. El procediment seria el següent.

Procediment:

Cada usuari té un codi públic que consisteix en un parell de nombres, molt grans, de 200 dígits o més (eA, nA), (eB,nB)... En el nostre exemple, com s'ha dit abans, seran petits.
A més d'aquests nombres, l'usuari A, B... té un altre nombre secret, el seu desxifrador, que l'ajuda a desxifrar el missatge dirigit a ell.

Suposem que A vol enviar a B un missatge, per exemple, 17. Per tal d'explicar-ho més clarament, establirem 4 passos:

1. A busca en el llistat públic el codi de B; suposem (47, 2173).
2. A encripta el missatge, 17, per a B. Per a fer-ho, forma el número 17^{47}, i tot seguit troba el residu de dividir aquest número per 2173, que resulta 587.

3. Aquest número, 587, és el missatge codificat per a B, de manera que únicament B és capaç de desxifrar-lo. L'usuari A envia el missatge 587 per xarxes públiques a B, per tant tothom sap que entre aquests dos individus hi ha la transmissió d'un missatge. Per molt que tothom ho sàpiga, només B podrà recuperar el missatge sense encriptar, 17.
4. Quan B rep el missatge 587, només cal que miri el seu desxifrador dB, que és el número 1903, formar la potència 587^{1903} i tot seguit fer la divisió d'aquest número per 2173 i troba el residu, que és precisament 17, el missatge sense xifrar que A ha volgut transmetre a B.

El càlcul d'aquestes claus es realitza en secret a la màquina a la que es guardarà la clau privada, i un cop generada aquesta, convé protegir-la mitjançant un algoritme criptogràfic simètric.

En quant a les longituds de claus, el sistema RSA permet longituds variables, sent aconsellable actualment l'ús de claus de més de 1024 bits (s'han arribat a trencar claus de fins a 512 bits, tot i que van ser necessaris més de 5 mesos i quasi 300 ordinadors treballant junts per a aconseguir-ho).

RSA és el més conegut i utilitzat dels sistemes de clau pública, i també el més ràpid d'ells. Presenta tots els avantatges dels sistemes asimètrics i això el fa realment útil.

7.3. ASCII

ASCII, American Standard Code for Information Interchange, és el que utilitza un ordinador per ordenar, interpretar i processar dades. Està basat íntegrament en l'alfabet llatí, ja que aquest és el codi de caràcters més utilitzat al món occidental i òbviament en l'anglès, idioma que s'usa normalment per a tots els llenguatges de programació.
L'ASCII va ser creat l'any 1963 per l'ASA (Comitè d'Estats Units d'Estàndards, en anglès) que actualment s'anomena ANSI i va tenir l'esperit d'agrupar i simplificar tots els codis que s'utilitzaven a les comunicacions d'aquells anys, sobretot en la telegrafia. Originalment, aquest codi només tractava els caràcters en majúscula de l'alfabet llatí, però posteriorment s'hi van integrar caràcters en minúscula, a més de poder establir alguns criteris de control per a que la informació sigui processada correctament i sense errors.
El seu funcionament està basat en la utilització d'una combinació de 7 bits per poder interpretar cadascun dels caràcters, als que s'afegeix un bit de paritat, arribant llavors

als 8 bits i garantint la detecció de fal·làcies en la transmissió o interpretació de les dades degudament processades.

Cal desmitificar alguns coneixements que s'han difós en forma errònia sobre ASCII, com per exemple:

- El codi ASCII no representa al conjunts de caràcters als que s'accedeix prement la tecla ALT juntament amb una combinació numèrica específica.
- Existeixen altres codis de caràcters que utilitzen la base de transmissió de dades mitjançant 8 bits, però no estan compresos per l'estàndard ASCII.

Així doncs, l'ASCII és un codi numèric que representa els caràcters, utilitzant una escala decimal del 0 al 217. Aquests nombres decimals són convertits per la computadora en nombres binaris, per ser posteriorment processats. Per tant, cadascuna de les lletres que s'escriuen corresponen a un d'aquests codis.

La organització de la taula de caràcters de l'ASCII és la següent:

Partint de que tots els demés valors corresponen a símbols, accents, i lletres accentuades, tenim que:
- Del 48 al 57 hi ha els nombres
- Del 65 al 90 hi ha les lletres amb Majúscula.
- Del 97 al 122 hi ha les lletres amb minúscula.

Taula de caràcters del codi ASCI

8. Màquines de xifrat actuals

8.1. La màquina Enigma

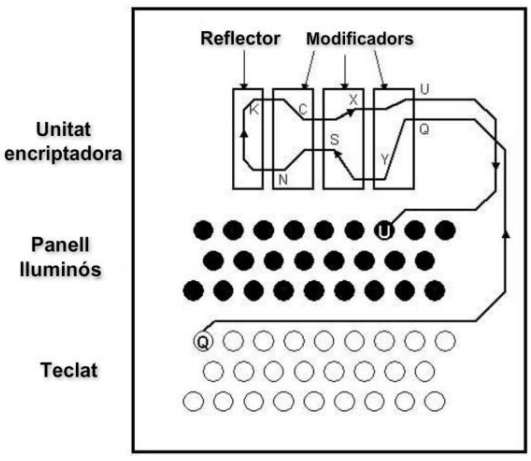
Després de la Primera Guerra Mundial, l'inventor alemany Arthur Scherbius i el seu amic Richard Ritter van fundar una empresa d'enginyeria i van crear la màquina Enigma amb la finalitat de vendre-la, no només a l'exèrcit sinó també a moltes empreses del país. La màquina es guardava dins una capsa de dimensions 34cm x 28cm x 15cm i pesava uns 12 kg.

Bàsicament, estava formada per tres components connectades per cables que, ben combinats constituïen una complexa màquina per xifrar: el primer component era un teclat per escriure cada lletra del text en clar; una unitat modificadora formada per tres rotors, un capçal i un reflector; i per acabar un tauler on quedava il·luminada la lletra xifrada.
Cada rotor era un disc amb dues cares i amb 26 contactes elèctrics, un per a cada lletra de l'alfabet. El capçal estava col·locat entre el teclat i el primer rotor, amb l'objectiu d'intercanviar 6 parells de lletres. Mentrestant, el reflector aconseguia que al codificar un missatge xifrat, utilitzant les mateixes posicions inicials dels rotors i els mateixos parells de lletres interconnectades al capçal, s'aconseguís el missatge en clar.

L'any 1925 Scherbius es va llançar a fabricar màquines Enigma en sèrie. L'exèrcit alemany, durant els següents anys, en va comprar més de 30 000 i van començar a enviar missatges xifrats. Cada mes, els operadors de Enigma rebien un nou *llibre de codis* amb les claus que havien d'utilitzar cada dia. En ella s'indicaven:

- Les posicions del capçal: A/D C/G M/P T/F L/U
- La disposició o ordre dels rotors: 2-1-3
- Les posicions inicials dels rotors: S M E

Esquema d'Enigma

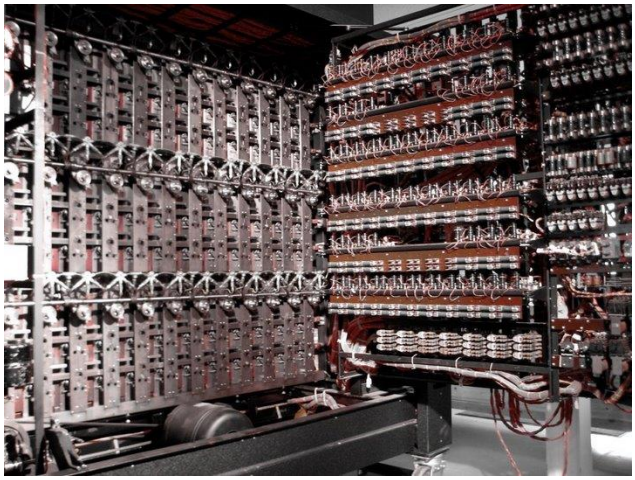


El fet que la màquina Enigma fos tan difícil de trencar era degut a l'enorme quantitat de maneres en què la màquina es podia configurar. En primer lloc, els tres rotors de la màquina es podien escollir d'un grup de cinc i podien ser intercanviats per a confondre als desxifradors. En segon lloc,

cada rotor podia estar ubicat en un dels vint-i-sis contactes elèctrics, això significa que la màquina podia estar configurada en més d'un milió de maneres diferents. A més, les connexions elèctriques de la part posterior de la màquina podien ser canviades manualment, donant lloc a més de 150 milions de milions de milions de possibles configuracions. Per a augmentar encara més la seguretat, l'orientació dels tres rotors canviava contínuament, així que cada cop que es transmetia una lletra, la configuració de la màquina, i per tant, l'orientació dels tres rotors, canviaven per a la següent lletra. D'aquesta manera, teclejar "MOMO" podria generar el missatge "FGTB": la "M" i la "O" s'envien dos cops però són codificades de manera diferent.

Paral·lelament a l'ús de les màquines Enigma, es va crear la primera computadora, que va rebre el nom de *Colossus*. La funció d'aquesta màquina va ser intentar trencar les claus de l'Enigma, i així desxifrar els missatges dels alemanys un cop interceptats.

Actualment, es conserven màquines Enigma en museus i centres històrics, com per exemple a Bletchley Park, o també al Quartell General de l'Exèrcit a Madrid.



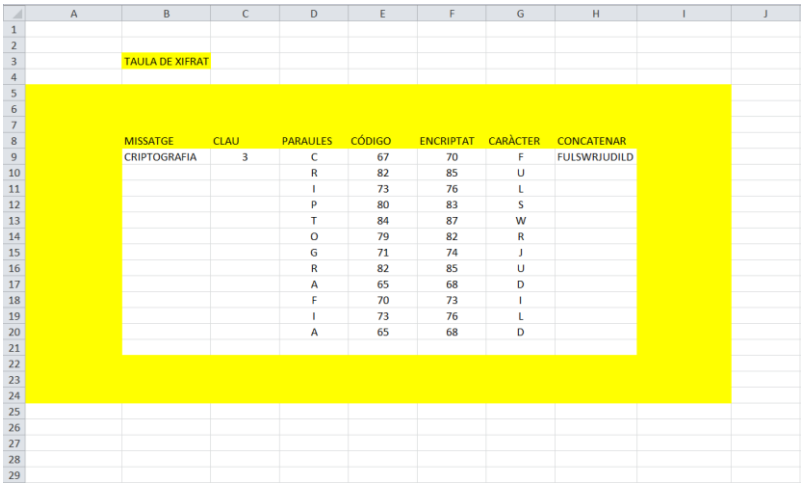
Màquina Colossus

9. Part Pràctica

La part pràctica principal del meu treball és l'elaboració de programaris informàtics mitjançant Excel amb els quals qualsevol usuari pugui codificar el missatge que ell desitgi, i alhora desxifrar un missatge ja codificat. Aquesta part pràctica està combinada també amb l'elaboració d'una novel·la de dues parts i la creació manual d'alguns estris per criptografiar.

9.1. PRÀCTICA 1 ~ ELABORACIÓ AMB EXCEL D'UN XIFRADOR / DESXIFRADOR DE CÈSAR

A) XIFRADOR DE MISSATGES



TAULA DE XIFRAT

MISSATGE	CLAU	PARAULES	CÓDIGO	ENCRIPTAT	CARÀCTER	CONCATENAR
CRIPTOGRAFIA	3	C	67	70	F	FULSWRJUDILD
		R	82	85	U	
		I	73	76	L	
		P	80	83	S	
		T	84	87	W	
		O	79	82	R	
		G	71	74	J	
		R	82	85	U	
		A	65	68	D	
		F	70	73	I	
		I	73	76	L	
		A	65	68	D	

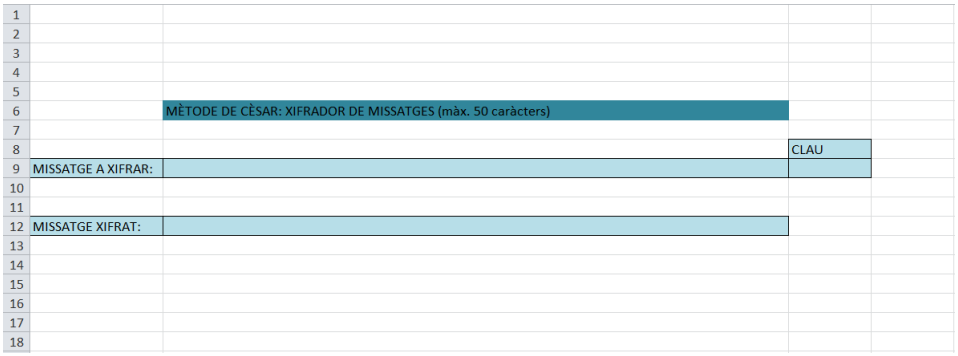
Per tal d'elaborar una taula de xifrat que em permetés fer el que jo buscava, vaig dissenyar aquesta primer. En ella, apareixen tots els apartats necessaris per a que funcioni i que es pugui obtenir un missatge xifrat.

- A la columna MISSATGE, escrivim el text que nosaltres vulguem xifrar. En aquest cas, l'usuari ha volgut xifrar CRIPTOGRAFIA.
- On hi apareix la paraula CLAU, determinem el nombre que volem que correspongui al desplaçament de l'alfabet. En aquest cas, és 3, tal com era originalment el Mètode de Cèsar.
- La única funció, però important, de la columna que porta el nom de PARAULES és separar les lletres de la paraula, o text originals. Això s'aconsegueix mitjançant la funció =EXTRAE, amb la que extraiem lletra per lletra al text fins

al final d'aquest. Això ho fem per tal de poder seguir després amb els càlculs corresponents.

- La transformació de CÓDIGO és sense dubte la més important, ja que és la que ens converteix la lletra en el seu codi de configuració a l'ordinador. La funció que ens permet fer-ho és la mateixa que el nom, =CODIGO.
- En la columna ENCRIPTAT, es realitza una funció també molt senzilla però important, perquè és on es suma la clau al codi de cada lletra. Això ho fem mitjançant la funció =SUMA.
- La següent columna consisteix en fer l'oposat de la del CÓDIGO, ja que busquem convertir el nou codi en lletres. Utilitzem la funció =CARACTER.
- Finalment, en la columna CONCATENAR apareix el missatge xifrat. Amb aquesta funció, oposada a la de EXTRAE, agrupem totes les lletres obtingudes i així formem el missatge final.

El programa definitiu no podia ser aquest, ja que no havien d'aparèixer visibles les columnes d'operacions, i tampoc podíem permetre que l'usuari les pogués modificar, ja que això acabaria amb el sistema d'obtenció del missatge xifrat. Per tal d'impedir-ho, havíem de bloquejar les cel·les amb contingut no-modificable, i només deixar lliures les de la clau, el missatge original i les del missatge xifrat. També calia arreglar l'aspecte de la taula. Al final, aquest va ser el resultat obtingut:



B) DESXIFRADOR DE MISSATGES

Per a crear el desxifrador de missatges, he utilitzat les mateixes funcions que en el xifrador, però a l'inrevés. El que tenim al principi és el text xifrat, per tant busquem arribar a l'original i comprensible.

TAULA DE DESXIFRAT

MISSATGE	CLAU	PARAULES	CÓDIGO	DESENCRIPTAT	CARÀCTER	CONCATENAR
FULSWRJUDILD	3	F	70	67	C	CRIPTOGRAFIA
		U	85	82	R	
		L	76	73	I	
		S	83	80	P	
		W	87	84	T	
		R	82	79	O	
		J	74	71	G	
		U	85	82	R	
		D	68	65	A	
		I	73	70	F	
		L	76	73	I	
		D	68	65	A	

En aquest cas, la única diferència respecte a la Taula de Xifrat, és que enlloc de sumar la clau a la cinquena columna, la restem. Així obtindrem el codi original i trobarem la lletra del missatge en clar.

Com en l'altre cas, calia millorar el mateix. Aquest és el resultat obtingut.

MÈTODE DE CÈSAR: DESXIFRADOR DE MISSATGES (màx. 50 caràcters)

CLAU

MISSATGE XIFRAT:

MISSATGE DESXIFRAT:

ALERTA! És important que la graella corresponent al MISSATGE XIFRAT/DESXIFRAT només s'utilitzi per copiar-lo, i en cap cas s'esborrin les fórmules que conté, ja que llavors s'anul·la la funció de la taula.

9.2. PRÀCTICA 2 ~ ELABORACIÓ AMB EXCEL D'UN XIFRADOR / DESXIFRADOR DE VIGENÈRE

A) XIFRADOR DE MISSATGES

CLAU	PARAULES	CÓDIGO	ENCRIPTAT	CARÀCTER	CONCATENAR
3	C	67	70	F	
4	R	82	86	V	
5	I	73	78	N	
7	P	80	87	W	
	T	84	87	W	
	O	79	83	S	
	G	71	76	L	
	R	82	89	Y	
	A	65	68	D	
	F	70	74	J	
	I	73	78	N	
	A	65	72	H	
		#¡VALOR!	#¡VALOR!		
		#¡VALOR!	#¡VALOR!		
		#¡VALOR!	#¡VALOR!		
		#¡VALOR!	#¡VALOR!		

En el cas de crear un programari per al Xifrat de Vigenère, el funcionament és una mica diferent al de Cèsar: es necessiten més i diferents funcions perquè fem més coses.

Una de les principals diferències és que en aquest mètode hi ha 4 claus. Per això, al dividir la

paraula amb la funció =EXTRAE com al Cèsar, a més de separar-la en lletres, també agruparem les lletres de 4 en 4. La continuació és la mateixa, amb la diferència que a cada grup, cada lletra es xifra amb una clau.

El resultat definitiu obtingut és el següent:

		MÈTODE DE VIGENÈRE: XIFRADOR DE MISSATGES (màx. 50 caràcters-4 claus)	
			CLAU
			3
	MISSATGE A XIFRAR:	CRIPTOGRAFIA	4
			5
			7
	MISSATGE XIFRAT:	FVNWWSLYDJNH	

B) DESXIFRADOR DE MISSATGES

Com abans, el desxifrador és igual però intercanviant l'ordre de les funcions.

CLAU		CÓDIGO	DESENCRIPTAR	CARÀCTER
2	e	101	99	c
3	u	117	114	r
4	m	109	105	i
5	u	117	112	p
	v	118	116	t
	r	114	111	o
	k	107	103	g
	w	119	114	r
	c	99	97	a
	i	105	102	f
	m	109	105	i
	f	102	97	a
		#¡VALOR!	#¡VALOR!	
		#¡VALOR!	#¡VALOR!	

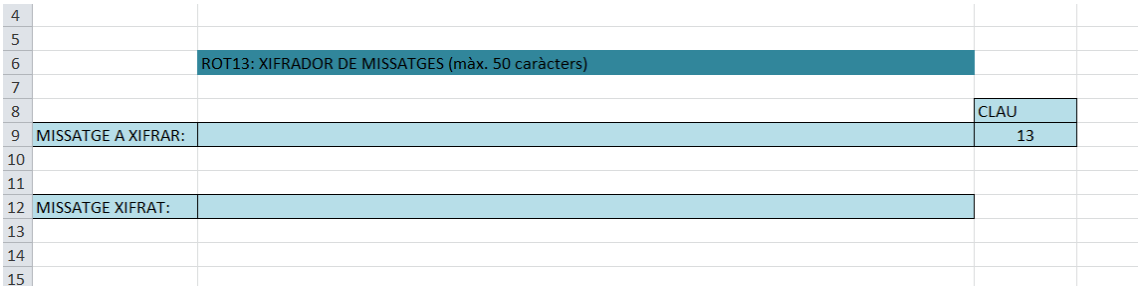
Enlloc de sumar la clau, com en el Mètode de Cèsar, la restem. Obtenim aquest resultat final.

		MÈTODE DE VIGENÈRE: DESXIFRADOR DE MISSATGES (màx. 50 caràcters)	
			CLAU
	MISSATGE XIFRAT:		
	MISSATGE DESXIFRAT:		

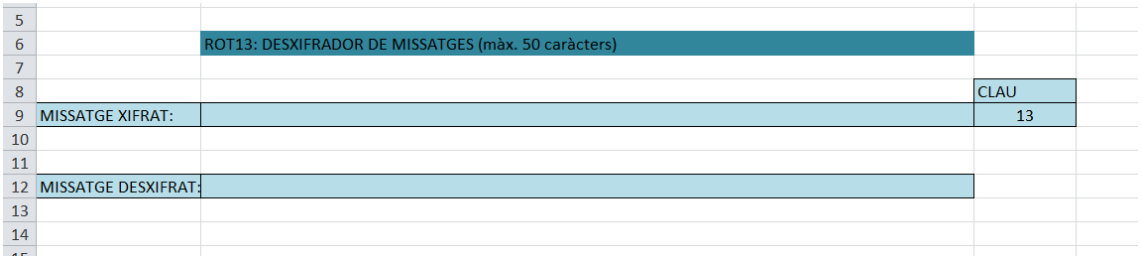
9.3. PRÀCTICA 3 ~ ELABORACIÓ AMB EXCEL D'UN XIFRADOR / DESXIFRADOR DE ROT13

En el cas del ROT13, crear un programa d'Excel que pugui xifrar i desxifrar un cop ja tenim fet el del Xifrat de Cèsar normal, és molt senzill. Només cal posar com a clau fixa 13, ja que és fonamental per a aquest mètode.

A) XIFRADOR DE MISSATGES



B) DESXIFRADOR DE MISSATGES



10. Curiositats de la Criptografia

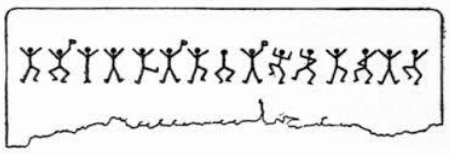
10.1. Criptografia en l'Art

La criptografia no només és una ciència relacionada amb les matemàtiques i la informàtica per a usos, sinó que també és un recurs molt utilitzat en altres àmbits més artístics, com per exemple la literatura, escultures o cinema. Vegem-ne uns exemples.

10.1.1. Criptografia en la Literatura

La presencia de la Criptografia en la literatura és bastant comuna. Molts escriptors utilitzen algun tipus de mètode per xifrar algun missatge en les seves novel·les, especialment si aquestes són d'acció, històriques, o tracten d'aventures. Aquest recurs, no és un mètode nou: ja fa temps que s'utilitza.

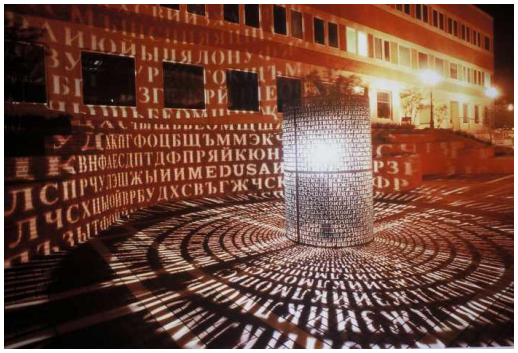
Utilitzar un recurs com aquest dona a l'obra un toc de misteri i incita al lector a voler desxifrar el missatge .Recalquem com a exemples de literatura que continguin aquest recurs "*El codi Da Vinci*" de Dan Brown; "*The adventure of the dancing men*", una aventura de Sherlock Holmes escrita per Arthur Conan Doyle; *"Lee a Julio Verne, El amor en tiempos de Criptografía*" de Susana Mataix; *"L'escarabat d'Or*" de Edgar Allan Poe...



10.1.2. Criptografia en el Cinema

També en gran nombre de pel·lícules apareixen de manera o altra la Criptografia, tot i que moltes d'aquestes pel·lícules estan basades en un llibre original, com és el cas de "El Codi Da Vinci". Moltes pel·lícules com "La Búsqueda" y "Ángeles y Demonios" tenen un rerefons en mètodes de xifrat.

10.1.3. Criptografia en l'Escultura



L'escultura també pot estar basada amb la Criptografia, com per exemple en el cas de l'americà James Sanborn, que combina escultures de missatges secrets amb llum per tal d'aconseguir un efecte visual molt interessant. La seva obra més coneguda, *Kryptos,* apareix a la novel·la de Dan Brown "*The Lost Symbol".* Aquesta escultura va ser presentada a la CIA l'any 1990 a Virginia. Aquesta escultura segueix sent alhora un trencaclosques i un misteri pels que esperen

trobar els missatges xifrats dins d'aquestes 2000 lletres que conté l'escultura. Durant aquests 20 anys de vida de l'escultura, s'ha confirmat que tres de les quatre seccions han sigut resoltes, però ningú ha sigut capaç de desxifrar els 97 caràcters restants. Sanborn ha afirmat que si mor abans de que es trenqui el codi complet de l'escultura, deixarà un document amb la informació *necessària* per verificar la resposta.

10.2. Un personatge molt especial: Mavis Batey

Fa tan sols uns dies, cercant a internet informacions diverses pel meu treball, vaig arribar a una notícia sobre una senyora, Mavis Batey. Segons els articles que vaig trobar, ella acabava de morir dies abans, el 12 de novembre de 2013. Curiosament, vaig voler llegir més sobre ella, perquè pel que deduïa tenia alguna cosa a veure amb la Criptografia però me'n volia documentar bé. Llavors, va ser quan vaig al·lucinar completament. Per pura casualitat, o potser no, el personatge que jo ja feia temps que havia creat a la meva novel·la i Mavis Batey, eren pràcticament el mateix. Les dues van néixer l'any 1921 i l'any 1940 van viatjar a Bletchley Park, on van aprendre les arts de la Criptografia. Totes dues van conèixer al seu futur marit en aquell lloc i van seguir dedicant-se als mètodes de xifratge. A més, la segona part de la meva novel·la passa l'any 2013, quan té 92 anys la meva protagonista, i curiosament Mavis Batey ha mort aquest mateix any.

Mavis Lever va néixer el 5 de maig de 1921 a Dulwich. Quan va estellar la Segona Guerra Mundial, ella estudiava alemany a l'Univeristy College de Londres. Enlloc d'evacuar-se a Gales, va presentar-se voluntària com a infermera per ajudar en l'esforç de la guerra. Però els seus entrevistadors van pensar que els seus coneixement de l'alemany serien més útils que la seva habilitat amb les gases. Per això, la van destinar al Ministeri de Guerra Econòmica, concretament a l'Escola de Codis i Xifres del Govern. Quan va arribar a Bletchley Park, es va posar a les ordres d'un criptoanalista llegendari, Dillwyn (Dilly) Knox.

Durant la seva estada a Bletchley Park, Mavis va encarregar-se de desxifrar missatges que arribaven a les seves mans. Un cop, va arribar a la conclusió que un missatge era un "dummy", emès per l'enemic per enganyar i desinformar. Això ho va descobrir ja que el missatge xifrat no contenia cap lletra L, i les màquines Enigma són de classe no-recíproca, és a dir, una lletra mai es transforma en ella mateixa al xifrar-la. Gràcies a això, ella va poder construir un altre rotor de la màquina Enigma. En una altra ocasió,

aquesta desxifradora va interpretar el que significava STGOCH, mentre que els seus companys estaven completament perduts. Per alguns significava Sant Goch, per altres era un error, però la solució correcta, i la que va trobar Mavis era Santiago De Chile. Mavis va contraure matrimoni amb Keith Batey, un matemàtic també de Bletchley. Quan va acabar la guerra, tots dos van viure sota l'anonimat i ella va passar a dedicar-se a la preservació de jardins d'Anglaterra, després d'escriure una biografia del seu conegut Dilly Knox.

Fins fa un temps, el personatge de Mavis Batey era desconegut, però a partir dels anys 70, molts dels noms de tots aquells espies van sortir a la llum.

10.3. Alan Turing

Alan Turing fou un matemàtic britànic, considerat el pare de la Informàtica Moderna. Des de ben petit va demostrar una alta capacitat per les matemàtiques, gràcies a la qual va poder accedir a la Universitat de Cambridge amb beca. El seu reconeixement comença a partir de la Segona Guerra Mundial, quan fou reclutat per l'exèrcit britànic per desxifrar els codis emesos per la màquina Enigma, utilitzada pels alemanys. Turing va participar en nombroses creacions i construccions de màquines o computadores paral·leles, com per exemple la *Colossus* o *The Bomb,* que van permetre trencar els codis de l'Enigma. Respecte a Bletchley Park, Turing va tenir-hi una estreta relació: va participar de forma decisiva en la feina duta a terme allí per trencar els codis alemanys i va col·laborar amb Dilly Knox, un veterà de la descodificació.

L'homosexualitat era il·legal al Regne Unit i es considerava una malaltia mental que comportava sancions criminals. L'any 1952 va reconèixer haver mantingut relacions amb un jove de 19 anys i va ser acusat d'indecència segons la secció 11 del Codi Penal. Va ser condemnat pel mateix crim que Oscar Wilde cinquanta anys abans. Per evitar la presó, Alan Turing va preferir ser sotmès a un tractament hormonal dissenyat per reduir la libido: es tractava d'una castració química via injeccions d'estrogen que van durar un any. Aquesta condemna va comportar que perdés el seu nivell de seguretat i per tant la feina de consultor criptogràfic per al govern.
El 8 de juny de 1954, la dona de fer feines el va trobar mort a casa: es va determinar que havia mort el dia abans per enverinament de cianur, aparentment per una poma coberta d'aquesta substància que va deixar a mig menjar al costat del llit. Es va

classificar aquesta mort com a suïcidi, tot i que gent propera a ell recolza que fos un assassinat degut als escàndols causats per la seva homosexualitat.

El primer logotip històric de la marca *Apple* era una poma mossegada que tenia els colors de l'arc de Sant Martí, i en un cert moment es va especular amb el fet que podia ser un homenatge a la seva mort. Això va ser finalment desmentit tant pel dissenyador com per la pròpia marca: la poma simbolitza la fruita de la saviesa, i podria fer referència a Newton, i els colors de l'arc de Sant Martí desendreçats farien referència a la no-jerarquització.

Alan Turing va ser indultat recentment per la Reina d'Anglaterra, i per tant, perdonat després de seixanta anys. Això és el que han aconseguit un grup de científics destacats, que van fer campanya durant anys demanant el perdó per "un dels matemàtics més brillants de l'era moderna".

10.4. Bletchley Park o Station X

Bletchley Park, una mansió situada al poble de Bletchley, va convertir-se en seu de GCCS (Global Command and Control System) al principi de la guerra l'any 1939. Va ser el principal lloc d'esforç destinat a la descodificació de missatges xifrats enemics. Els importants informes d'intel·ligència generats aquí a partir de la informació interceptada i desxifrada, classificats amb la paraula Ultra, van contribuir en gran manera amb l'esforç de guerra dels aliats i (possiblement) a escurçar-ne la seva durada.

L'any 1932, els polonesos van trencar la màquina Enigma, però en aquell any la màquina només s'alterava un cop cada pocs mesos. Amb l'arribada de la guerra, la màquina va passar a modificar-se cada dia, i al juliol del 1939, els polonesos van demanar ajudar a Anglaterra per poder vèncer aquests codis.

Al voltant del gener del 1940 es va realitzar el primer gran cop contra Enigma, quan l'equip liderat per Dilly Knox, va trobar la clau que utilitzava l'administració de l'armada alemanya, coneguda a Bletchley Park com "The Green". Encoratjats per aquest èxit, van tornar a intentar-ho amb "Red", una clau utilitzada per l'armada alemanya. El procés de trencar els codis d'Enigma va rebre l'ajuda d'un complex dissenyat per Alan Turing i Gordon Welchman. *The Bombe* era capaç de buscar totes les possibilitats de configuració d'Enigma, i així reduir les possibles opcions de codi.

Actualment, Bletchley Park és un dels museus més importants del món de Criptografia, ja que està ben adaptat per tal de comprendre el que és aquesta ciència i també per tal de reconèixer la gran tasca que van fer tots els que van col·laborar-hi (i per tant, jugar-se la vida), i que no van poder parlar-ne fins l'any 1970.

10.5. Entrevista a David Juher

David Juher és un professor de Informàtica i Matemàtica Aplicada a la Universitat de Girona. A més, també és Doctor en Matemàtiques per la UAB i membre de la Societat Catalana de Matemàtiques, filial de l'Institut d'Estudis Catalans. David Juher és l'autor del llibre "L'art de la comunicació secreta: el llenguatge de la criptografia". Aquest llibre és el que més he utilitzat per fer el meu treball, i vaig tenir el privilegi de poder contactar amb ell i parlar-hi.

1. **Com va arribar vostè a la criptografia?**

   Vaig arribar a la Criptografia de manera casual. A l'últim curs de la carrera de mates, a la UAB, et deixen escollir entre moltes assignatures optatives. Una d'elles era Teoria de Nombres, una cosa molt i molt abstracta que en principi sembla que no tingui cap relació amb el món real. La vaig agafar. El primer dia de classe el professor ens va dir que no faria examen, i que per aprovar el que havíem de fer és triar un tema d'una llista que ell proposava, llegir un llibre sobre el tema, fer-ne un treball i al final de curs explicar-ho a la classe. El tema que vaig triar (quasi sense saber què era) era "Criptografia". El vaig triar perquè em va cridar l'atenció que una cosa tan abstracta i estranya com la Teoria de Nombres tingués una aplicació tan important al món real. Així va ser com vaig llegir un llibre (molt avançat), que es diu "Introduction to Cryptography", d'en J. Buchmann, i vaig aprendre coses sobre el tema.

2. **Què pot empènyer a una persona de l'actualitat a interessar-se per la criptografia?**

   Actualment, cada cop que a Internet comprem alguna cosa (comerç electrònic), fem una transacció bancària, signem un contracte, ens matriculem a una universitat no presencial, etc etc (o sigui, cada cop que fem un tràmit important en el que donem el nostre número de compte corrent, número de DNI, o altres informacions delicades), els diversos ordinadors que intervenen en la gestió del tràmit es comuniquen de manera encriptada, per evitar que els hackers puguin llegir la comunicació. Per tant, una persona curiosa a qui li agradi la informàtica (per exemple) es pot preguntar com s'ho fan els ordinadors per comunicar-se

amb total seguretat. Aquest pot ser un motiu per entrar a estudiar les tècniques criptogràfiques. Pot haver-n'hi d'altres: observa que el motiu que em va empènyer a mi va ser que vaig trobar maco que una branca tan abstracta de les matemàtiques es pogués aplicar a situacions del tot reals.

3. **A què es pot aplicar actualment?**

   Es pot aplicar a tot el que t'he dit en l'apartat anterior, i també en moltes altres coses: Televisió de pagament (si pagues per tenir el Canal Plus a casa, el senyal que t'arriba encriptat es desencripta amb una maquineta que tens al teu televisor, i llavors pots veure les imatges; aquesta màquina conté la clau; si no estàs al corrent de pagament, no et renoven la clau, que es canvia cada mes, i llavors el senyal que t'arriba no els pots desxifrar: veus la tele "a ratlles"...), telefonia mòbil (és molt fàcil escoltar amb una antena la conversa que mantenen dues persones parlant per telèfon mòbil; llavors, abans que la teva veu surti del telèfon i viatgi per l'aire en forma d'ones per arribar al telèfon de destí, la conversa es distorsiona amb un mètode criptogràfic). Etc etc etc.

4. **Actualment existeix gent que viu exclusivament de la criptografia?**

   Suposo que sí, i tant que hi ha gent que viu de la Criptografia. Evidentment existeixen empreses que treballen en això.

5. **Creu que està a l'abast de tothom?**

   La Criptografia clàssica (la de tota la vida, abans de l'aparició dels ordinadors) sí que està a l'abast de tothom, perquè els mètodes eren molt artesanals i fàcils d'explicar. La Criptografia moderna (Internet, telèfons, tele, etc) és una mica més complicada, però si no entres en temes molt tècnics també es pot explicar i la gent ho pot entendre a grans trets, quedant-se amb les idees fonamentals (de fet és això el que intento fer a les xerrades, i el que vaig intentar fer en el meu llibre).

6. **No està tot inventat ja, parlant de la criptografia?**

   No, no està tot inventat!! Per exemple, darrerament s'estan fent molts esforços per desenvolupar la Criptografia quàntica, que serà la criptografia del futur. Ja s'han fet avenços molt importants.

7. **Quines diferències fonamentals veu entre la criptografia antiga i l'actual?**

   Les diferències entre la criptografia antiga i la moderna no són tan radicals com pot semblar. Antigament les lletres del missatge es barrejaven (mètodes de

permutació) segons alguna norma concreta, o bé es canviaven per altres símbols (mètodes de substitució). En el fons, els mètodes que fan servir ara els ordinadors són els mateixos, però a nivell de bits (zeros i uns) en lloc de "lletres", i a una gran velocitat, i amb molta més complexitat.

8. **Si vostè hagués sigut un personatge de la IIGM, un espia, com hauria actuat per tal de xifrar missatges i transmetre'ls?**

   Buffff... Aquí ho deixo a la teva imaginació. Hi ha molts llibres on s'explica com s'ho feien, els espies de la segona guerra mundial... Però si m'hagués d'inventar un mètode una mica original, em surt el següent: sóc un espia amb formació matemàtica, el meu pare era un gran matemàtic i, tot i que els nazis no em van deixar acabar els estudis de secundària per les restriccions a l'accés a l'ensenyament que tenien els jueus als anys 30, el meu pare em feia classes particulars i jo gaudia molt... En una de les classes, em va fascinar una cosa que em va explicar el meu pare sobre el número pi: té infinites xifres decimals que no es repeteixen mai, i estan distribuïdes de manera tan aleatòria que qualsevol cadena finita de xifres que puguis imaginar-te, per exemple 31101918, que era la data del meu naixement, es troba en algun lloc del número pi!! Utilitzant unes tècniques de càlcul una mica avançades que jo no vaig acabar d'entendre, el meu pare i jo vam calcular els primers 1000 decimals de número pi. Són aquests (això és real):

3.14159265358979323846264338327950288419716939937510582097494459
23078164062862089986280348253421170679821480865132823066470938 4
46095505822317253594081284811174502841027019385211055596446229 4
89549303819644288109756659334461284756482337867831652712019091 4
56485669234603486104543266482133936072602491412737245870066063 1
55881748815209209628292540917153643678925903600113305305488204 6
65213841469519415116094330572703657595919530921861173819326117 9
31051185480744623799627495673518857527248912279381830119491298 3
36733624406566430860213949463952247371907021798609437027705392 1
71762931767523846748184676694051320005681271452635608277857713 4
27577896091736371787214684409012249534301465495853710507922796 8
92589235420199561121290219608640344181598136297747713099605187 0
72113499999983729780499510597317328160963185950244594553469083 0
26425223082533446850352619311881710100031378387528865875332083 8
14206171776691473035982534904287554687311595628638823537875937 5

> 195778185778053217122680661300192787661119590921642019 9.
> Jo sempre portava a sobre un full de paper amb aquestes mil xifres, escrites a mà pel meu pare. Durant la guerra, aquest paper em portava molts records, ja que al meu pare el van matar els nazis en un camp de concentració, i aquest full de paper era l'únic objecte que jo conservava d'ell.

10.6. Entrevista a Richard Lewis, sènior archivist de Bletchley Park

Al juliol del 2013, vaig contactar amb Bletchley Park, antigament conegut com a Station X. Aquest és el nom d'una finca situada a uns 80 km de Londres que va ser la principal seu de l'esforç destinat a la descodificació de missatges xifrats enemics durant la Segona Guerra Mundial. Entre aquestes parets va ser dissenyada la primera computadora *Colossus*, que va permetre trencar els codis de la màquina alemanya Enigma. A més, va ser l'indret on va desenvolupar la seva activitat com a criptoanalista el matemàtic Alan Turing, l'arxiu del qual romà en aquesta mansió i ha sigut comprat per a conservar-lo.

Dear Carla
Thank you for your enquiry, received on Monday 30th July 2013, regarding Bletchley Park Trust.
Below I have briefly answered your questions:

Which is its origin?
The Trust was formed in 1992 to save the site which opened to the public in 1994.

Is this an interesting topic for visitors?
We feel that the work of Bletchley Park is hugely important and also fascinating and our visitor feedback is very good.

Are there a lot of visitors?
The visitor numbers are improving each year and last year there were 170,000 visitors.

Do you organize workshops?
We have a range of educational programs for children of all ages

Do you have cryptographers working in the museum?
There are no working cryptographers in the employment of the Trust.

I hope the above is of use to you.
Thanks again
Richard

Richard Lewis
Senior Archivist

11. Conclusió

La criptografia és una de les ciències més utilitzades i necessàries però alhora més desconegudes. El seu ús es remunta fins al segle V a.C, quan els espartans van començar a utilitzar-la sense ser-ne conscients contra els atenesos, i arriba fins a l'actualitat, sent la base de totes les operacions realitzades a la gran xarxa de dades anomenada Internet: des de la compra d'un bitllet d'avió fins a la contrasenya per entrar al compte personal de Facebook. La criptografia, com les altres ciències, ha tingut molts canvis, referents a l'ús i també a la tècnica. En primer lloc, cal fixar-se en que antigament, s'utilitzava únicament per a assumptes militars o d'Estat. Això contrasta amb l'actualitat, ja que ara tothom té accés a ella, i l'utilitza, inclús potser sense adonar-se'n. En segon lloc, les tècniques han millorat molt. Avui en dia, la criptografia és tota referent al camp de la informàtica, i per això, una clau és pràcticament irrompible.

Amb aquest treball he pogut fer un recorregut pels diferents mètodes criptogràfics de la història fins a arribar als actuals, i alhora també he pogut endinsar-me en la història mundial i veure en primera persona les utilitats d'aquestes tècniques. A més, la part pràctica m'ha servit per determinar com funcionen els sistemes com el Xifrat de Cèsar o bé el ROT13 i fer-ne una adaptació més manual i senzilla.

Un cop acabat el meu treball de recerca, me n'adono de que he complert tots els objectius que m'havia proposat en un inici: vaig partir d'un punt en què desconeixia completament tota la criptografia moderna; només tenia conceptes bàsics de l'Escítala, el Xifrat de Cèsar i el Xifrat de Vigenère; i no era conscient de la realment important funció de la criptografia en la guerra. Penso que he arribat a obtenir un treball molt complet: per una banda, conté explicada detalladament la història de la criptografia, i els canvis que ha patit, tot això realitzant exemples amb cada tècnica trobada. A més, la part pràctica relaciona la teoria explicada anteriorment amb la informàtica, i per tant, és un clar exemple del funcionament de la criptografia actual. Per altra banda, tot això està recolzat per una part novel·lada (inventada per mi mateixa). El personatge principal d'aquesta està basat en la meva àvia, i han estat utilitzades les seves pròpies fotografies per a realitzar els documents que apareixen en el treball. Tot això va acompanyat d'un apartat que recull les principals curiositats, personatges i elements d'interès que he anat descobrint al llarg de la realització de la meva investigació.

El resultat obtingut hagués variat lleugerament si no se m'haguessin presentat una sèrie d'imprevistos: per una part, hagués disposat de més entrevistes i documents semblants, si hagués rebut resposta de totes les persones i entitats a les quals vaig

demanar ajut; per altra part, he tingut una dificultat a l'hora de filtrar informació de la bibliografia que tenia al meu abast, deguda al seu alt nivell i als tecnicismes que una alumna de segon de batxillerat desconeix. També hi ha hagut factors personals que han dificultat el meu treball, com per exemple compaginar-lo amb els estudis de batxillerat, organitzar bé el temps per arribar a tot, o, com a últim entrebanc, ser diagnosticada d'Hepatitis dies abans de l'entrega del treball.

Com a treball de recerca, crec que ha arribat a tots els aspectes que havien de ser tractats, i per tant, no es pot ampliar. Referint-nos a la criptografia, la recerca no s'aturaria aquí: es podria fer recerca sobre mil temes més, i inclús investigar per intentar arribar a una nova màquina ideal de xifrat, és a dir, fàcil de desxifrar però impossible de trencar.

Amb aquest treball no només he après sobre Criptografia o Matemàtiques, sinó que també sobre Historia, Informàtica, i sobretot sobre com elaborar un treball d'investigació: com organitzar-se, com realitzar-lo, com arribar als resultats...

Jo quedo satisfeta de la meva investigació, ja que s'escapa dels cànons de treballs de Criptografia que he vist perquè considero que aporto un toc d'originalitat. A més, també estic satisfeta perquè he aconseguit l'objectiu bàsic d'un treball de recerca, que és aprendre sobre el tema i alhora aprendre a treballar. Gràcies a aquest treball de recerca he descobert aspectes i moments de la història, i he volgut rescatar personatges de l'oblit, com Mavis Batey que, com bé va dir Arturo Quirantes en un article dedicat a ella, "Queda pendiente que alguien escriba su historia, y aunque ella no quiso hacerlo, merece ser contada. Espero que alguien lo haga. Algún día".

12. Referències o fonts d'informació

Bibliografia

BROWN, Dan (2010) *El código Da Vinci.* Planeta. Barcelona.

CABALLERO, Pino (2002) *Introducción a la criptografia.* RA-MA.

CAMPÀS, Joan (2007) *Els Hackers*. Editorial UOC.

DURÁN, Raúl (2005) *El Criptosistema RSA.* RA-MA.

JUHER, David (2004) *L'art de la comunicació secreta: el llenguatge de la criptografia.* Llibres de l'Índex.

MARTOS, Ana (2010) *Word 2010*. ANAYA.

MATAIX, Susana (2002) *Lee a Julio Verne: El amor en tiempos de Criptografia*. Rubes.

NAVARRO, Luis (2010) *Word 2010. Fácil y rápido.* InforBooks Ediciones.

PALACIOS, Luis (1990) *Gran Historia Universal*. Editorial Nájera. V.XX

POE, Edgar Allan (1982) *Narraciones Extraordinarias. El escarabajo de oro.* Salvat.

STEPHENSON, Neal (2004) *Criptonomicon.* Ediciones B.

Webgrafia

Criptografía y Seguridad <http://www.kriptopolis.com>

Graffiti matemático <http://www.blogseitb.com/matematicas/tag/criptografia/>

Web dedicada a la historia de la Criptología espanyola <http://www.criptohistoria.es/>

Consultada a l'agost del 2013 (ja no apareix)
<http://www22.brinkster.com/nosolomates>

Technology News <http://news.cnet.com>

La historia escondida detrás del muro de Berlin
<http://ar.selecciones.com/contenido/a903_alas-de-libertad>

El Periódico <http://elperiodico.com>

Radio y Televisión Española <http://www.rtve.es>

Alan Turing
<http://www.dma.eui.upm.es/historia_informatica/Doc/Personajes/AlanTuring.htm>

Guerra Fría <http://www.todosobreguerrafria.blogspot.com>

Segunda Guerra Mundial <http://lasegundaguerra.com>

Bletchley Park Official Website <http://www.bletchleypark.org>

Red Temática de Criptografía y Seguridad de la Información
<http://www.criptored.upm.es>

Consultada al novembre de 2013 (ja no apareix) <http://www.cripto.es>

Pàgina web d'Història <http://www.historiasiglo20.org>

El País <http://www.elpais.com>

Ciencia, esceptismo y humor <http://www.naukas.com>

Filmografia

ENIGMA (2001) Michael Apted

CAÍDA DEL MURO DE BERLIN. HISTORY CHANNEL. (documental)

CRIPTOGRAFÍA: CÓDIGOS SECRETOS EN LA HISTORIA (documental)

INTRODUCCIÓN A LA CRIPTOGRAFÍA. UPV. (documental)

MATERIAL EUSKAMPUS PROYECTO "MÁS QUE NUM3ROS" VERANO 2012 (CD)

MANUAL COMPLETO MICROSOFT EXCEL 2010 (documental)

BREAKING THE CODE (1986) Hugh Whitemore

BBC: Code Breakers Bletchley Park Lost Heroes