LA CRIPTOGRAFIA AHIR, AVUI, I DEMÀ

ÍNDEX

1 CONCEPTE

La criptografia és la tècnica emprada per codificar un text i fer-lo incomprensible per a la persona que no en posseeix la clau. La paraula criptografia prové del grec *κρύπτος* (kryptós, que significa ocult), *γραφη* (grafein, que vol dir escrit) i el sufix –ia (usat per a formar substantius abstractes). El missatge codificat està a la vista, i qualsevol persona el pot veure, tot i que el seu significat es troba ocult. Per aconseguir entendre'l és necessari posseir la clau i l'algoritme de desxifratge. Tot i així, en la història, l'art d'ocultar el missatge també ha estat un mètode de compartir una informació en privat, sense que ningú, a més a més del destinatari, en conegués l'existència. Aquest art es coneix com esteganografia. El mot prové del grec *στεγανος* (steganos, ocult), *γραφη* (grafein, escrit) i el sufix -ia, per tant és el missatge ocult.

En la criptografia trobem diferents elements que el fan possible, i són necessaris i bàsics:

1. **Missatge en clar:** el missatge original que pot ser llegit i comprès per a qualssevol persones. També es coneix com a text en clar.
2. **Algoritme:** és el conjunt de regles per a resoldre un problema en un nombre finit de passos. Si l'algoritme es troba en una xarxa informàtica s'anomena algorisme.
3. **Criptosistema:** és el conjunt d'algoritmes criptogràfics per a implementar una solució criptogràfica.
4. **Clau:** necessària per a xifrar i desxifrar missatges. Hi ha dos tipus de claus: la clau simètrica (s'usa la mateixa clau per a codificar i descodificar un missatge) i la clau asimètrica (es fa servir una clau per a codificar un missatge, i una clau diferent per a descodificar-lo). A més a més, en el par de claus asimètriques es poden diferenciar una clau pública (la que es dóna a tothom) i una privada (només coneguda pel propietari). Això permet crear dues situacions: una que es fa servir la clau pública per a xifrar un text en clar, i per tant l'únic que podrà llegir el missatge desxifrat serà el propietari de la clau privada, i l'altre és la situació contrària. És a dir, es farà servir la clau privada per a xifrar un arxiu

adjunt al missatge (normalment amb la data i altres components), de manera que en ser desxifrat per a qualsevol, es demostrarà que l'arxiu és coherent amb el missatge. Per tant, serveix per a enviar un missatge o per a verificar-ne l'autoria.

5. **Xifrar:** és el procés pel qual es canvien els caràcters originals a símbols o diferents caràcters, per mitjà d'un algoritme, usant una o diverses claus.
6. **Missatge críptic o xifrat:** és el conjunt de símbols i/o caràcters que no poden ser compresos.
7. **Desxifrar:** és l'ús d'una clau i/o un algoritme per a convertir el missatge críptic en un missatge en clar.
8. **Criptnoanàlisi:** la branca de la criptografia dedicada a l'estudi dels criptosistemes per aconseguir-lo trencar.
9. **Ruptura o trencar:** trencar un criptosistema consisteix en la recerca de debilitats en l'algoritme per obtenir la clau, i amb aquesta el text en clar o de reduir la dificultat d'obtenir el missatge en clar en n-1, sent n el nombre de claus usades per a xifrar.
10. **Trencar per força bruta:** consisteix en provar cada una de les possibles claus d'un sistema criptogràfic fins a localitzar-ne l'adequada.

En criptografia cal aclarir la diferència entre encriptació i codificació:

L'encriptació és el procés de transformació de la informació (coneguda com a missatge en clar) utilitzant un algoritme (anomenat xifrat) perquè sigui il·legible per qualsevol, excepte per aquells que posseeixin uns coneixements especials, habitualment referents a una clau. El resultat del procés és la informació encriptada.

En canvi codificar consisteix a modificar cada caràcter en una seqüència de nombres naturals, octets o impulsos elèctrics, per tal de facilitar la transmissió de dades (generalment números i/o text a través de xarxes de telecomunicació) o l'emmagatzematge de text en els ordinadors.

Tot i les diferències usaré l'ús comú dels termes, com a sinònims, per a tal d'evitar contínues repeticions.

2 INTRODUCCIÓ

Des de fa segles reis, reines i generals han confiat en una eficient comunicació per tal de governar els seus països i comandar els exèrcits. Al mateix temps, han estat conscients del que implicava que aquesta informació caigués en mans equivocades. De manera que l'amenaça d'intercepció del missatge per part de l'enemic motivà al desenvolupament de codis i xifrats: mètodes per tal de modificar el missatge original i que només sigui comprès pel destinatari.

La creació de codis i xifrats ha resultat una lluita intel·lectual constant entre *codemackers* i *codebreakers*. Els primers busquen la fabricació de nous mètodes de codificar, mentre els altres treballen en l'ús d'altres mètodes genèrics basats en les debilitats dels codis per a tal d'obtenir el text en clar sense cap clau. Quan els *codebreakers* desenvolupen una nova "arma" que revela la debilitat del codi, aquest ja no és útil. I queda extingit, a no ser que evolucioni en un més fort. L'evolució dels codis, per tant, és el resultat d'aquesta lluita, i es pot comparar amb un bacteri infecciosa. El bacteri sobreviu fins que els doctors troben un antibiòtic que exposa la seva debilitat i el mata. L'única sortida que té per a sobreviure és evolucionar, i aquest procés es va repetint.

La història ha estat marcada pels codis. Han decidit el resultat de batalles i conflictes de mort de reis i reines. També és cert que cada vegada la criptografia és més important en les nostres vides. La informació és un producte molt valuós dins la nostra societat. Així que el procés de codificació de missatges, conegut com encriptació, jugarà un paper creixent en la vida quotidiana. Es pot veure exemplificat en l'ús de correus o missatges, que passen per diversos ordinadors, o les trucades que reboten en satèl·lits. Ambdues formes de comunicació poden esser interceptades amb facilitat, de manera que la nostra privacitat es posa en perill. De la mateixa manera, com més empreses estiguin a internet, en cal posar en marxa d'altres que protegeixin la informació de les empreses i els seus clients. L'encriptació és l'única eina coneguda per a tal de protegir la nostra privacitat i garantir la seguretat del mercat digital. La criptografia proporcionarà les claus de l'Era de la Informació.

No obstant això, la creixent demanda del públic per a la criptografia està en conflicte amb les necessitats policials i de seguretat nacional. Durant dècades, tant la policia com els serveis d'intel·ligència han usat les escoltes telefòniques per a reunir

proves en contra de terroristes i criminals. Les forces de la llei i ordre pressionen als governs per restringir l'ús de la criptografia, mentre els civils i empreses defensen l'ús de la criptografia per a tal de protegir la privacitat. Per tant, que és més important, la nostra privacitat o una efectiva policia?

Abans d'acabar aquesta introducció cal aclarir un problema al que s'enfronta qualsevol persona que tracta el tema de la criptografia. Al ser una ciència basada en el secret és en gran mesura una ciència secreta. Molts dels herois que apareixen en el treball no han obtingut mai cap reconeixement pel seu treball mentre eren vius. Això és degut a que el seu treball o invent tenia un gran valor militar o diplomàtic durant les seves vides. Aquest art secret segueix vigent i el més segur és que hi hagi altres mètodes d'encriptació no públics.

3 EL NAIXEMENT DE LA CRIPTOGRAFIA

Els primers registres d'ús de la criptografia són segurament dels egipcis. Aquests es troben en jeroglífics no estàndards tallats en monuments de l'Antic Egipte, de l'any 2500 aC. Tot i que no es consideren una comunicació secreta, sinó més aviat una forma de cridar l'atenció, i d'idolatrar els seus déus. Tot i que no ho podem saber en claredat, el cert és que la següent mostra de secretisme en els missatges, no apareix fins dos mil anys després.

El grec Heròdot, segle VaC, és considerat el pare de la història segons l'estadista Ciceró i la filosofia romana. En la seva obra "Historiae", descriu el conflicte entre Grècia i Pèrsia, i veia un conflicte entre la llibertat i l'esclavitud. Segons Heròdot, va ser l'art de l'escriptura secreta, l'esteganografia, que va salvar Grècia de ser conquerida per Xerxes, el líder dels perses.

El conflicte s'inicià a causa de l'absència d'homenatges i regals a la nova ciutat de Persèpolis, la nova capital del regnat de Xerxes, per part d'Atenes i Esparta. Decidit a venjar aquesta insolència, el líder persa passà cinc anys dissenyant un atac sorpresa, el més gran de la història. Tot i això, l'acumulació militar persa havia estat presenciada per l'espartà Demarat, un grec expulsat de la seva pàtria i que buscà refugi al territori persa. Tot i ser exiliat, sentia lleialtat a Grècia i decidí enviar un missatge per advertir el pla d'invasió de Xerxes. Diu Heròdot en el Llibre VII de la mateixa obra:

> "<< El caso es que no podía alertarlos así como así (Demacrato), por lo que se le ocurrió la siguiente idea: cogió una tablilla de doble hoja, le raspó la cera y, acto seguido, puso un escrito, en la superfície de madera de la tablilla, los planes del monarca; hecho lo cual, volvió a recubrirla con cera derretida, tapando el mensaje, a fin de que el transporte de la tablilla, al estar en blanco, no ocasionase el menor contratiempo ante los cuerpos de guardia apostados en el camino. Cuando la tablilla llegó definitivamente a Lacedemonia (Esparta), los lacedemonios no acertaron a dar con una explicación, hasta que, según tengo entendido, al fin Gogo (...) sugirió que raspasen la cera, porque encontrarían –les indicó– un mensaje grabado en la madera.>>"

Com a resultat d'aquest missatge, els grecs van començar a armar-se i es construïren vaixells de guerra. Xerxes havia perdut l'element sorpresa i acabà sent derrotat per la defensa grega a la badia de Salamina.

L'estratègia que feu servir Demarat d'Esparta es va basar en amagar el missatge. Heròdot va relatar un altre mètode esteganogràfic, en el qual Histeu animà a Aristàgores de Milet a rapar-se el cap. A continuació, va escriure al cuir cabellut el missatge que volia enviar. Esperà a que li creixés el cabell al missatger, de manera que podia viatjar sense que fós assetjat. En arribar al seu destí només calia rapar-lo i que el destinatari en llegís el contingut.

Tot i així el recurs esteganogràfic més conegut fins ara segurament és l'ús de tinta invisible. Normalment contenen materials orgànics, ja que aquesta tinta en ser assecada i escalfada es torna marró per la presència de carboni. Es feia servir suc de llimona i fins i tota orina humana, tot i que avui en dia es coneixen casos d'espies que usen aquest tipus de tinta.

L'inici de la pràctica de l'esteganografia ens mostra sens dubte un cert grau de seguretat, però és dèbil si el missatge és llarg o el missatger és buscat i el missatge descobert. Llavors el contingut és revelat i la seguretat és nul·la. De manera que un guàrdia podria cercar en qualsevol persona que creués la frontera, raspant qualsevol tauleta de cera, escalfant fulls de paper en blanc, afaitant els caps de la gent (tot i avui en dia no ser ètic) i així sempre hi hauria algun missatge que fos interceptat.

Per aquest motiu, juntament amb el desenvolupament de l'esteganografia trobem l'evolució de la criptografia. Per tant, en cas que el missatge sigués descobert, seria il·legible, donant així un grau major de seguretat.

3.1 La escítala espartana

La criptografia per ella mateixa es pot dividir en dues branques, conegudes com a transposició i substitució. En la transposició les lletres del missatge són reorganitzades formant un anagrama. Per a missatges molt curts, com una paraula, aquest mètode és relativament segur, ja que només hi ha un nombre limitat de maneres de reordenar un conjunt de lletres. Per exemple, tres lletres es poden organitzar de sis maneres, com és el cas de GOL, GLO, LOG, LGO, OLG i OGL. Tot i això, a mesura que el missatge és més llarg, el nombre de possibilitats augmenta ràpidament, de manera exponencial, fent impossible tornar al missatge, a no ser que es conegui el procés de barreja de les lletres.

Per exemple, AQUEST MISSATGE ÉS ÚTIL, conté vint lletres, i es poden organitzar en més de 1.000.000.000.000.000 = 1x10 a la 15= 100 bilions de maneres diferents. (Tenint en compte que hi ha vint lletres, amb algunes repeticions, 20!/(3!*3!*3!*2!*2!*2!)= 1.407.929.403.000.000, i traient possibles repeticions). En el cas que una persona comprovés una possibilitat cada segon, treballant nit i dia, necessitaria (60*60*24=86.400 en un dia, 500.000.000.000.000/86.400= =5.787.037.037,037037037 dies, ANS/365=15.854.895,99188229325215626573 anys) més de 15.000.000 anys de vida. La transposició aleatòria sembla oferir un alt nivell de seguretat, ja que l'interceptor, com he demostrat anteriorment, necessitaria un temps del que no disposaria, i un anagrama enormement difícil.

Per a dur a terme la transposició es feia servir, en la guerra entre atenesos i espartans, l'escítala, un sistema de codificació usat per espartans format per dues vares de gruixor variable i una tira de cuir o papir. Per enviar un missatge, s'enrotllava en espiral una cinta a una de les vares i s'escrivia el missatge longitudinalment, de manera que a cada volta apareixés una lletra. Un cop escrit es desenrotllava la cinta i ja es podia enviar, i només l'havia d'enrotllar amb la mateixa vara o una de dimensions idèntiques a la que s'havia emprat per escriure el missatge.

Per exemple, amb una escítala de sis cares, si volguéssim enviar el missatge: <<LA HISTORIA DE LA CRIPTOGRAFIA>>, en fem una taula amb sis columnes i les files que fessin falta, en aquest cas cinc, i s'escriu el missatge en files:

L	**A**		**H**	**I**	**S**
T	**O**	**R**	**I**	**A**	
D	**E**		**L**	**A**	
C	**R**	**I**	**P**	**T**	**O**
G	**R**	**A**	**F**	**I**	**A**

Taula 1*:* Escítala de 6 cares.

En xifrar el missatge, ara es llegirà en columnes, de manera que el text ara serà: <<LTDCGAOERR R IAHILPFIAATIS OA>>. Per desxifrar aquest text cal enrotllar-lo a una escítala de sis cares i el mateix gruix, però invertint-ne la llargada per l'amplada, obtenint el text en vertical:

L	**T**	**D**	**C**	**G**
A	**O**	**E**	**R**	**R**
	R		**I**	**A**
H	**I**	**L**	**P**	**F**
I	**A**	**A**	**T**	**I**
S			**O**	**A**

Taula 2*:* Escítala invertida.

L'algoritme de transposició aleatòria ofereix un alt nivell de seguretat per a missatges relativament llargs. Tot i així, les claus que es feien servir per aquest mètode podien arribar a ser enormement complicades. Per tant, es necessitava un altre mètode, que amb claus més senzilles donés la mateixa seguretat.

3.2 La substitució

L'alternativa al mètode de transposició va ser la substitució. Una de les primeres descripcions del funcionament del xifrat per substitució apareix en el *Kama-sutra*, un text del segle IV aC. escrit pel braman Vatsiaiana. En aquest s'indiquen seixanta-quatre arts que les dones haurien d'estudiar, com la cuina, servei de massatges o escacs. La número quaranta-cinc de la llista es basa en el coneixement de l'escriptura secreta. Una de les tècniques que recomana és emparellar dues lletres de l'alfabet a l'atzar i substituir cada lletra per la seva parella. En català podríem fer l'emparellament següent:

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

Taula 3*:* Exemple d'emparellament.

Llavors en lloc del missatge: "EL XIFRAT PER SUBSTITUCIO", l'emissor escriuria "MU STCWHI YMW XLGXIITILFTK". El mètode s'anomena xifratge per substitució ja que cada lletra del text en clar (abans d'encriptar) és substituïda per una altra lletra diferent. De manera que no hi ha una conservació de la identitat del missatge com en la transposició, sinó que cada lletra manté la seva posició. El primer ús documentat d'un xifratge per substitució amb ús militar es remunta al segle I aC., i apareix a les Gàl·lies, pel militar i polític Juli Cèsar. Cèsar va substituir cada lletra de

l'abecedari per la tercera lletra que la seguia, desplaçant l'alfabet tres posicions a la dreta. Va ser tan usat per Juli, que tot mètode de substitució basat en el desplaçament de tres llocs en l'abecedari es coneix com a xifratge de Cèsar. En podem veure un exemple a continuació:

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**
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**

Taula 4*:* Xifratge de Cèsar.

Les minúscules indiquen les lletres del text en clar mentre les majúscules el missatge que enviarà l'emissor. D'aquesta manera la substitució del missatge "*vaig arribar, vaig veure, vaig vèncer*", sense tenir en compte els accents, s'enviaria com a: "YDLJ DUULEU, YDLJ YHXUH, YDLJ YHQFHU". Per a desxifrar caldria fer el pas contrari, substituir les lletres que apareixen en el text xifrat per les de sobre de la taula.

Tot i que Juli només fa un canvi de tres posicions, és evident que podem fer canvis entre un i vint-i-cinc llocs, per tant, és possible generar vint-i-cinc xifrats diferents. De fet, si no tenim en compte l'abecedari, i en fem una reordenació aleatòria, llavors podem generar un nombre major de codis diferents. N'hi hauria més de 400.000.000.000.000.000.000.000.000 = 4x10 a la 26 = 4 * 10^{26} (26! = =403.291.461.126.605.635.584.000.000), i per tant el mateix nombre de xifrats diferents.

Cada xifrat es pot considerar en termes generals un mètode d'encriptació, conegut com a algoritme i clau, els quals especifiquen els detalls d'una encriptació particular. En aquest cas, l'algoritme consisteix a substituir cada lletra de l'alfabet original (del missatge en clar) en una lletra de l'abecedari de xifratge, caracteritzat per poder reorganitzar de tota manera possible l'alfabet original. La clau defineix l'abecedari de xifratge que es fa servir per a una encriptació particular.

Podria una persona que no fos el destinatari interceptar un missatge i desxifrar-lo? Tot i que tingués una forta sospita de quin és l'algoritme, no sabria la clau exacte. Per exemple, si creu que cada lletra del text clar ha estat substituïda per una lletra diferent segons l'alfabet, és poc probable que sàpiga quin alfabet de xifratge s'ha usat. Si l'abecedari de xifratge, la clau, es guarda com un secret entre emissor i receptor, l'enemic no podrà desxifrar el missatge que hagi interceptat. La importància de la clau, el coneixement de la qual ha d'estar únicament en mans d'emissor i receptor, és el

secret per a que la criptografia sigui segura. Segons el *Principi de Kerckhoffs*, la seguretat no depèn de mantenir en secret l'algoritme, sinó que només depèn de mantenir secreta la clau.

Però mantenir en secret la clau no és l'únic essencial per a un mètode eficaç. També cal que el sistema de xifratge tingui una àmplia gamma de claus possibles. Per exemple, si l'emissor usa el xifratge Cèsar per a xifrar el missatge, l'encriptació és relativament feble, ja que només hi ha vint-i-sis claus possibles. D'aquesta manera, des del punt de vista d'un enemic, si intercepta el missatge i sospita que l'algoritme fet servir ha estat el canvi de Cèsar, simplement haurà de comprovar vint-i-cinc claus. No obstant, si l'emissor fa servir l'algoritme general de substitució, en el qual l'alfabet de xifratge pot ser qualsevol reorganització de l'abecedari simple, llavors hi ha 400.000.000.000.000.000.000.000.000 = 4x10 a la 26 claus possibles. Des del punt de vista de l'enemic, tot i conèixer l'algoritme, el nombre de claus possibles és immens. En el cas que aquest comprovés una clau cada segon, trigaria aproximadament un bilió de vegades la vida de l'univers comprovar totes les claus i desxifrar el missatge. A continuació se'n veu un exemple:

[60 * 60 * 24 = 86.400 en un dia, 400.000.000.000.000.000.000.000.000 / 86.400 =
= 4.629.629.629.629.629.629.629,629629 dies, ANS / 365 =
= 12.683.916.793.505.834.601,725012 anys, ANS/ 13.830.000.000 (edat univers) =
= 917.130.643,058990 (vegades l'edat de l'univers, aproximadament 1 bilió)]

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

Taula 5*:* Equivalència del xifratge per substitució.

Un possible text en clar podria ser: "algoritme de substitució general".
El text ja xifrat resultaria ser el següent: "FOPYATLWQ JQ KIEKLTLINTY".

Aquest tipus de xifrat és fàcil d'implementar i a més a més proporciona un alt nivell de seguretat. L'emissor pot definir la clau d'una manera senzilla, indicant solament l'ordre de les vint-i-sis lletres de l'alfabet de xifratge. I tot i que sigui impossible, teòricament, que l'enemic comprovi totes les claus possibles per mitjà de l'atac per força bruta, la senzillesa de la clau és important. Emissor i receptor han de

compartir el coneixement de la clau, i si aquesta és complicada, hi ha més possibilitats de que hi hagi un malentès.

De fet, és més senzill que l'emissor es prepari una clau més senzilla encara que el nombre de possibles claus es redueixi. En lloc de reordenar l'abecedari per aconseguir l'alfabet de xifratge, l'emissor tria una paraula o frase. Per exemple, es pot usar "LA CRIPTOGRAFIA CLÀSSICA" com a frase clau, i traient els espais i lletres repetides (LACRIPTOGFS), i fer servir aquest com a inici de l'alfabet de xifratge. La resta de l'abecedari és merament la resta de lletres de l'alfabet, en el seu ordre correcte a partir d'on acaba la frase clau. Per tant quedaria el següent:

0.	**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**
1.	**L**	**A**	**C**	**R**	**I**	**P**	**T**	**O**	**G**	**F**	**S**	**U**	**V**	**W**	**X**	**Y**	**Z**	**B**	**D**	**E**	**H**	**J**	**K**	**M**	**N**	**Q**

Taula 6*:* Xifratge per substitució amb paraula clau.
0.==> Alfabet original
1.==> Alfabet de xifratge

L'avantatge de construir una clau d'aquesta manera és que la paraula o frase clau és fàcilment memoritzable. És important, ja que si la clau no és senzilla és normal que la recordem escrivint-la en un paper, de manera que si l'enemic roba o aconsegueix el paper, podria llegir tot missatge encriptat en aquella clau. Tot i així, si és memoritzat la possibilitat que la clau caigui en mans enemigues és menor.

La simplicitat i la força del xifrat per substitució va fer que dominés l'art de l'escriptura secreta durant el primer mil·lenni dC. Els *codemakers* havien creat un sistema que garantia la seguretat de les comunicacions, i per això no es necessitava evolucionar o crear nous algoritmes. La balança havia caigut en contra dels *codebreakers*, els quals no aconseguien resoldre el xifratge de substitució d'una manera més simple, i no per força bruta. Molts en aquella època consideraven que aquest algoritme de substitució aleatòria era com un mur impenetrable, gràcies al gran nombre de possibles claus, i durant segles semblava que tenien raó. Però no és cert que l'algoritme perfecta encara no existeix? La resposta a aquesta pregunta la trobem anys després.

4 LA CRIPTOGRAFIA DE CLAU SIMÈTRICA

4.1 L'anàlisi de freqüència

Muhammad, a l'edat d'uns quaranta anys, començà a anar a una cova del mont de Hira, a les afores de la Meca. Allà meditava i pregava, durant llargs períodes de reflexió. Al voltant del 610 dC, va ser visitat per l'arcàngel Gabriel, i així començaren les revelacions del profeta. Les revelacions van ser enregistrades per diversos escribes durant la seva vida, però només com a fragments. Totes les revelacions van ser recopilades en un sol text gràcies als tres primers califes: Abu Bakr, Umar i Uthhman. L'Alcorà està compost per 114 capítols, cada un explica una revelació del Profeta.

Un segle més tard, el segle VIII dC, l'islam s'havia estès fins arribar al seu auge. A més a més, la civilització islàmica deixà els teixits més elaborats de la història, i en camps científics, es mostra el seu poder pel nombre de paraules d'origen àrab en la ciència moderna, com n'és exemple l'àlgebra.

La riquesa de la cultura islàmica prové en gran part com a resultat d'una societat de benestar i tranquil·la. Els Califes estaven més interessats en l'organització que no pas en la conquesta, de manera que les taxes s'abaratien per a les empreses, potenciant així el seu creixement. Mentre les lleis reduïen la corrupció i protegien els ciutadans. Tot això es basava en un sistema eficaç de l'administració, que gràcies al xifratge aconseguia una comunicació segura. Es xifraven tant registres d'impostos com afers d'estat, fet que demostra l'ús generalitzat de la criptografia.

Els àrabs, només s'havien familiaritzat amb l'ús del xifratge monoalfabètic. Tot i això, també eren capaços de destruir els xifrats. De fet, van ser els estudiosos àrabs, experts en matemàtiques, lingüística i estadística entre d'altres, qui varen inventar la criptoanàlisi. I varen ser els criptoanalistes àrabs qui van aconseguir trobar un mètode per trencar el xifratge de substitució monoalfabètic, que s'havia mantingut irrompible durant varis segles.

Aquest fet és degut a la recerca del màxim coneixement possible per part de l'islam. Volgueren traduir textos de civilitzacions anteriors com la babilònica o egípcia. A més a més, la criptoanàlisi també impulsava el creixement de l'educació religiosa. Per aquest motiu els teòlegs començaren a estudiar les revelacions del Profeta Mahoma que contenia l'Alcorà. Els teòlegs pretenien ordenar cronològicament les revelacions,

basant-se en l'evolució recent de certes paraules, per tant, si una revelació contenia nombroses paraules noves, indicava que es trobava més tard en la cronologia. Els teòlegs també intentaren demostrar que cada revelació fos atribuïble a Mahoma. Això ho aconseguien fent un estudi etimològic de les paraules i les oracions, comprovant que els texts particulars contenien patrons lingüístics del Profeta.

Gràcies a aquest estudi de les paraules, els teòlegs s'adonaren que hi havia lletres que es repetien més que d'altres. En el cas de l'àrab les més freqüents són la *a* i la *l*, en part per l'ús de l'article *al-*. Aquesta observació tan simple i evident portaria el primer gran avenç en criptoanàlisi.

El mètode usat per trencar el xifratge de substitució monoalfabètic és l'anàlisi de freqüències. El primer en escriure'n els detalls de la tècnica va ser el científic Abū Yūsuf Ya´qūb ibn Isḥāq al-Kindī. Estudià nombroses branques científiques, com la matemàtica, l'astronomia, la cosmologia, la medicina, la física... però s'especialitzà en filosofia. Tot i que el seu tractat més important va ser descobert el 1987a Estambul, titulat com: "*Un manuscrit sobre desxifrar missatges criptogràfics*". En aquest trobem un petit fragment:

"*Una manera de resoldre un missatge xifrat, si sabem en quina llengua esta escrit, és localitzar un text pla escrit en la mateixa llengua, suficientment llarg, i després comptar quantes vegades apareix cada lletra. A la lletra que aparegui amb més freqüència l'anomenàrem "primera", a la següent en freqüència l'anomenarem "segona"... i així fins a cobrir totes les lletres que apareguin en el nostre text. A continuació observem el text xifrat que volem resoldre i classifiquem els símbols de la mateixa manera trobem el símbol que apareix en major freqüència i el substituïm per la "primera" del nostre text. Fem el mateix amb la "segona" i així successivament, fins a que haguem cobert tots els símbols del criptograma que volem resoldre."*

Aquesta explicació d'al-Kindi és més fàcil d'explicar en català. En primer lloc cal estudiar un text llarg en català, o uns quants, i analitzant-ne la freqüència de cada lletra en l'alfabet. En català la lletra més comuna és la *e*, seguida de la *a*, així successivament com s'indica a la taula posterior. Després examinem el text xifrat i en treballem igual la freqüència d'aparició dels caràcters. De manera que és probable que el caràcter més repetit en el text sigui la lletra *e*, i el segon en freqüència possiblement sigui la *a*, i així successivament. La tècnica d'al-Kindi és coneguda com l'anàlisi de

freqüències, o freqüencial. Aquest ens mostra la innecessària tasca de comprovar els bilions de possibles claus, i permet trencar el missatge en una sèrie de senzills passos.

A 14,47%	**H 0,65%**	**O 6,58%**	**V 1,25%**
B 1,15%	**I 8,08%**	**P 2,39%**	**W 0,01%**
C 3,19%	**J 0,25%**	**Q 1,20%**	**X 0,45%**
D 3,47%	**K 0,02%**	**R 5,99%**	**Y 0,35%**
E 16,01%	**L 5,94%**	**S 7,43%**	**Z 0,01%**
F 0,90%	**M 2,79%**	**T 5,44%**	**Ç 0,01%**
G 1,15%	**N 5,84%**	**U 4,84%**	

Taula 7*:* Taula de freqüències dels percentatges amb que localitzem cada lletra en texts escrits en català.

Segons l'INE, i l'Institut d'Estudis Catalans les lletres segueixen aquestes probabilitats: E (13,89%), A (12,55%), S (8,43%), R (7,74%), I (6,99%), L (6,76%), N (6,40%), T (6,11%), O (5,71%), U (4,18%), D (3,94%), C (3,60%), M (3,16%), P (2,72%), V (1,40%), Q (1,35%), B (1,32%), G (1,28%), Ç (1,06%), F (1%), H (0,72%), X (0,52%), J (0,30%), Y (0,18%), Z (0,006%), K (0,004%), W (0,001%).

També cal tenir en compte quines són les paraules més comunes en el català. Les vint que apareixen més, ordenades de més a menys, són les següents:

de, la, i, el, a, l', en, que, d', va, del, per, les, els, un, amb, es, al, una i *és*.

4.2 A Europa

Mentre els àrabs en aquest període assoliren un alt nivell intel·lectual, els europeus encara lluitaven amb els fonaments de la criptografia. Les úniques institucions que estudiaven l'escriptura secreta van ser els monestirs, on els monjos volien entendre els significats ocults de la Bíblia.

El creixement de la indústria de la criptografia europea no arribà fins el segle XV. Això és degut a l'entrada en el Renaixement, caracteritzat per una intriga política que implicava la motivació suficient per a la comunicació secreta. Itàlia, al ser el centre d'aquest corrent, és l'ideal per a la criptografia. A més de ser el centre, estava formada per ciutats-estat independents, i per tant, calia burlar els altres. A més a més, cada estat

tenia ambaixadors a les Corts dels altres, i aquests, rebien missatges dels respectius caps d'estat per a tal de descriure en detall la política exterior implementada. En resposta, cada ambaixador enviaria qualsevol informació recollida fins ençà. Clarament, el xifratge del missatge era una part clau de les comunicacions. Per aquest motiu cada estat establia una oficina de xifrat i cada ambaixador tenia un secretari de xifratge.

Probablement el primer gran criptoanalista europeu va ser Giovanni Soro, secretari de xifratge venecià. El 1506 fou contractat, i conegut per tot Itàlia per trencar la majoria de missatges de les ciutats-estat italianes. Soro treballà uns quaranta anys com a criptoanalista, i fins i tot el Vaticà li enviava missatges xifrats per a que ell els desxifrés.

Els criptògrafs de l'època seguien confiant en el xifratge per substitució monoalfabètic, mentre els criptoanalistes van començar a usar l'anàlisi freqüencial per a trencar-lo. I aquells que desconeixien l'anàlisi de freqüències seguien confiant en el mètode, ignorant que criptoanalistes com Soro podien arribar a llegir els seus missatges.

Mentrestant, països amb el coneixement de la feblesa del xifratge per substitució per mitjà d'un alfabet de xifratge, van començar a investigar com desenvolupar un algoritme o una clau millor, capaç de protegir amb més seguretat els missatges. Una de les millores més simples del xifratge per substitució monoalfabètic va ser la incorporació de valors nuls, lletres o símbols que no es substituirien per res, és a dir, que el destinatari els ignoraria ja que només tenen la finalitat de confondre l'enemic que intercepta el missatge. En seria un exemple aplicar un valor a cada lletra entre el 00 i el 99, assignant a cada una de les vint-i-set lletres un valor, i deixant setanta-tres números amb valor nul.

Una altra millora consistia en introduir paraules codi. Fins ara ens hem concentrat en la idea del xifratge per substitució monoalfabètic, per la qual cosa cada lletra es substituïa per una lletra diferent, número o símbol. Tot i això, també és possible tenir una substitució a nivells més elevats, canviant una paraula del text en clar per un símbol o una altra paraula. Per exemple:

Segrestar = L	**Avui = 10**
Assassinar = N	**Ministre = ***
Demà = H	**Rei = ª**

Usant aquestes paraules codi podem encriptar un missatge simple:

Text en clar: **Assassina al ministre demà**

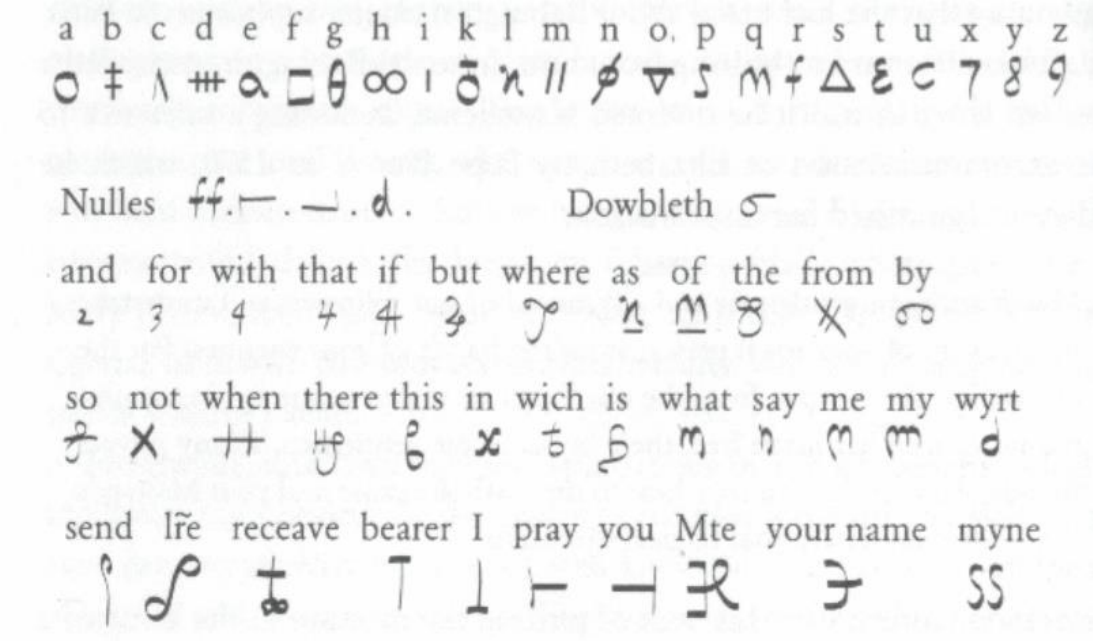
Text encriptat: **N-*-H**

A simple vista, l'ús de paraules codi sembla oferir més seguretat que els xifrats. Això és degut al fet que cal identificar el veritable significat de centenars o fins i tot milers de paraules codi. Tot i així, a l'hora de la pràctica no és tant eficaç, ja que entre emissor i receptor, a més d'acordar l'ordre de les vint-i-set lletres de l'abecedari de xifratge, necessitarien un llistat de centenars de pàgines especificant cada paraula codi per a cada paraula del text en clar. En definitiva, recopilar un llistat així seria una tasca complicada, i portar-lo a terme seria un inconvenient, tant per la possibilitat de que l'enemic pugui aconseguir el llistat, com per la complexitat d'elaborar-ne un des de zero.

Era tal la debilitat, que fins i tot, en el segle XVI, els criptògrafs apreciaven les debilitats dels codis, i es van basar en els xifrats, o a vegades en *nomenclàtors*. Un *nomenclàtor* és un sistema d'encriptació basat en un xifratge alfabètic i un seguit de paraules codi. Aquest sistemes eren usats per ambaixades, espionatge i conspiracions polítiques. Fins el segle XVIII els nomenclàtors van perdurar, tot i que segles abans ja es poguessin trencar. Això es deu al fet que la major part del missatge es pot desxifrar utilitzant un anàlisi freqüencial, i la resta de paraules es poden endevinar a partir del context. El motiu d'ús fins aquesta data és producte de la incorporació de paraules claus, un màxim de 50.000 que s'hagi enregistrat, en el nomenclàtor.

L'exemple on s'il·lustra millor la criptoanàlisi és en el cas de la reina Maria d'Escòcia. El resultat del seu judici depenia de la batalla entre els criptògrafs i els criptoanalistes de la reina Elisabet. Maria tenia els títols de reina d'Escòcia i Reina de França, i pretendent al tron anglès, tot i que el seu destí depengués de si un missatge en un tros de paper pogués ser desxifrat, o no.

Maria intercanviava missatges amb els seus co-conspiradors, particularment amb Anthony Babington, qui pretenia assassinar Elisabet d'Anglaterra per a tal que Maria tingués el poder escocès i anglès. Per a dur a terme una comunicació segura usaren un xifratge feble pel segle XVI. Aquest era un nomenclàtor, el qual il·lustraré a continuació:



Il·lustració 1: Nomenclàtor de la reina Maria.

Tal i com podem observar el xifratge de Maria es basava en un alfabet de xifratge i un seguit de paraules codi.

Aquests nomenclàtor va ser desxifrat pel cap dels descodificadors d'Elisabet, Thomas Phelippes, gràcies a que els seus espies, liderats pel Lord Walsingham, varen interceptar els missatges. Com a conseqüència, el dia 8 de febrer de 1587 Maria fou decapitada a Londres, i oficialment es demostrà que l'algoritme per substitució no era útil.

4.3 Vigenère

Després de l'execució de Maria reina dels escocesos, la lluita entre criptografs i criptoanalistes s'havia inclinat cap als segons. Ja no es podia confiar en la seguretat absoluta en enviar un missatge encriptat, per això s'havia d'inventar un xifrat nou més fort. Tot i que no sorgís fins a finals del segle XVI, els seus orígens es remunten al segle XV, amb el geni renaixentista Leon Battista Alberti. Nascut el 1404, fou un artista polifacètic –pintor, compositor, poeta i filòsof, així com l'autor en fer la primera anàlisi científica de perspectiva, un tractat sobre una mosca i la tomba per al seu gos. Conegut també per dissenyar la primera Fontana di Trevi a Roma, i per escriure el primer llibre imprès sobre arquitectura.

Tot i així Alberti, predí el futur exposant la seva idea sobre la criptografia. La nova forma de xifratge que el feu ser tan important, és l'ús de dos o més alfabets de

xifratge i combinar-se al llarg de l'encriptació del missatge, tal i com es mostra a continuació:

0.	**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**	**ç**
1.	p	a	E	h	k	ç	j	g	x	i	y	t	w	o	q	z	b	d	c	r	f	n	m	l	u	s	**v**
2.	l	e	O	n	b	a	t	i	s	r	h	j	q	g	x	z	w	u	m	y	ç	d	f	k	c	v	p

Taula 8: Combinació d'alfabets de de xifratge.
o.==> Alfabet pla
1.==> Primer alfabet de xifratge o clau 1
2.==> Segon alfabet de xifratge o clau 2

Per exmple, aquí trobem dos xifrats possibles, i podem encriptar un missatge alternant les dues claus. Per encriptar la paraula **battista** usaríem el primer alfabet de xifratge subtituint així la **b** per una **a**, la segona lletra, la **a** per la **l**, ja que les claus es van alternant. Per tant, les lletres en una posició senar es subtituiran per la primera clau, mentre les que es troben en posicions parella ho faran per la segona clau, de manera que quedaria un missatge encriptat com a **alryxmrl**. Com podem observar, la lletra **t** de la paraula del text clar es substitueix dues vegades per la **r** i una per la **y**. Així que aplicant un nombre més elevat d'alfabets de xifratge s'aconseguiria burlar l'anàlisi de freqüències.

Anys més tard, cap al 1562, el diplomàtic francès Blaise de Vigenère, nascut el 1523, amb l'edat de 39 anys, incrementà el seu interès cap a la criptografia a nivell pràctic gràcies als escrits d'Alberti. Anys abans ja havia llegits texts seus, però no tenia prous diners per deixar la feina i concentrar-se a l'estudi. Va ser llavors que examinà la idea de Leon Battista Alberti i la va convertir en un nou xifrat, coherent i potent, conegut com a <<quadrat de Vigenère>>. Aquest consistia en un alfabet clar d'*n* caràcters, i *n* claus o alfabets de xifratge, cada un trobat per desplaçar una posició cada lletra cap a l'esquerra, tal i com es mostra en la següent taula. Per tant, la fila 1 representa un alfabet de xifartge amb un canvi Cèsar d'1 posició. De la mateixa manera, la 2a fila representa un alfabet de xifratge amb un canvi Cèsar de 2 posicions i així successivament. La primera fila representa les lletres de l'abecedari en clar. Per exemple, si la clau usa el nombre 3, llavors el missatge és encriptat D, mentre si es fa servir la clau amb nombre 20, serà encriptat U.

La importància del mètode polialfabètic recau a la combinació de 27 claus. Així les lletres en posició 1+*n*, sent n múltiples de 4, es podrien substituir per la fila 2, les

lletres en posició 2+*n* per la fila 11, les que es troben en posicions 3+n per la 27 i les de posició n per la 20. Si féssim servir aquesta combinació de claus obtindríem que la paraula clau és **clau**. Per a mostrar el funcionament d'aquest en mostrarem un exemple.

0	**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**	**Ç**
1	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	ç	a
2	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	ç	a	b
3	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	ç	a	b	c
4	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	ç	a	b	c	d
5	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	ç	a	b	c	d	e
6	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	ç	a	b	c	d	e	f
7	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	ç	a	b	c	d	e	f	g
8	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	ç	a	b	c	d	e	f	g	h
9	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	ç	a	b	c	d	e	f	g	h	i
10	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	ç	a	b	c	d	e	f	g	h	i	j
11	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	ç	a	b	c	d	e	f	g	h	i	J	k
12	m	n	o	p	q	r	s	t	u	v	w	x	y	z	ç	a	b	c	d	e	f	g	h	i	j	k	l
13	n	o	p	q	r	s	t	u	v	w	x	y	z	ç	a	b	c	d	e	f	g	h	i	j	k	l	m
14	o	p	q	r	s	t	u	v	w	x	y	z	ç	a	b	c	d	e	f	g	h	i	j	k	l	m	n
15	p	q	r	s	t	u	v	w	x	y	z	ç	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
16	q	r	s	t	u	v	w	x	y	z	ç	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
17	r	s	t	u	v	w	x	y	z	ç	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
18	s	t	u	v	w	x	y	z	ç	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
19	t	u	v	w	x	y	z	ç	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
20	u	v	w	x	y	z	ç	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
21	v	w	x	y	z	ç	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
22	w	x	y	z	ç	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
23	x	y	z	ç	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
24	y	z	ç	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
25	z	ç	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
26	ç	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
27	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	ç

Taula 9: Taula Vigenère, el 0 indica l'alfabet clar, mentre la resta de nombres són les claus.

Si volem xifrar amb la paraula clau **clau** el missatge **BLAISE DE VIGENERE** s'encriptaria seguint l'estructura següent:

La primera lletra, la **B**, s'encripta amb la clau **c** (fila 2), obtenint la **d**.

La segona lletra, la **L**, s'encripta amb la clau **l** (fila 11), obtenint la **w**.

La tercera lletra, la **A**, s'encripta amb la clau **a** (fila 27), obtenint la **a**.

La quarta lletra, la **I**, s'encripta amb la clau **u** (fila 20), obtenint la **b**.

La cinquena lletra, la **S**, s'encripta amb la clau **c** (fila 2), obtenint la **u**.

La **E** (fila 11) per la **p**.

La **D** (fila 27) per la **d**.

La **E** (fila 20) per la **y**.

La **V** (fila 2) per la **x**.

La **I** (fila 11) per la **t**.

La **G** (fila 27) per la **g**.

La **E** (fila 20) per la **y**.

La **N** (fila 2) per la **o**.

La **E** (fila 11) per la **p**.

La **R** (fila 27) per la **r**.

La **E** (fila 20) per la **y**.

La taula que fem servir en aquest exemple és la següent:

0	**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**	**Ç**
2	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	ç	a	b
11	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	ç	a	b	c	d	e	f	g	h	i	j	k
27	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	ç
20	u	v	w	x	y	z	ç	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t

Taula 10: Taula de Vigenère per a la paraula clau *clau*

La frase original quedaria encriptada com <<**dwabup dy xtgyopry**>>. Com es pot comprovar, la freqüencia d'aparició de lletres respecte el missatge en clar desapareix. Passem de tenir 5 **e** a tenir 3 **y** com a modes de cada text. Per tant l'anàlisi freqüencial es veia afectat i amb aquest no es podia arribar a obtenir el text en clar. A més una lletra com pot ser la **e** en aquest exemple es canvia per les lletres **p** i **y**, però també ho podria haver fet per les lletres **g** i la mateixa **e** si haguessin estat en posicions diferents. També es pot comprovar que la **d** del text xifrat té els valors **b** i **d**. Així es demostra que de moment l'ús de xifratge polialfabètic, anomenat d'aquest mode per l'ús de més d'un alfabet de xifratge, era segur.

En el 1586 Vigenère publicà el seu treball "*Un tractat sobre l'escriptura secreta*". Durant més de tres segles els criptoanalistes no van poder descobrir els missatges en clar sense tenir coneixement sobre la clau, i trencar aquest algoritme polialfabètic era quasi impossible per la quantitat enorme de possibles claus. Fins al segle XIX no va ser molt popular entre les empreses, però l'arribada del telègraf en

aquest segle va fer que les comunicacions secretes es fessin usant el quadre de Vigenère. Va durar tant que era més conegut com el xifrat indesxifrable, *le chiffre indéchiffrable*, en francès.

4.3.1 Programa d'encriptació i desxifratge de Vigenère

Del mètode Vigenère n`he fet un programa informàtic que permet realitzar de manera senzilla tots els seus xifratges per substitució. Per iniciar la descripció d'aquest, primerament s'ha d'esmentar el llengutage informàtic emprat per a dur-lo a terme, aquest és el Python, exactament la versió 3.4.3. Cal aclarir uns conceptes abans d'iniciar la programació en si.

Aquest es basa en dos tipus de caràcters: els *str*, els quals són inmutables i es marquen entre cometes (com per exemple: 'Hola' o "Hola"), i els *int*, els quals són valors enters (com 35).

També cal aclarir que per a nombrar una cadena llarga de valors en podem fer una equivalència, com es mostra posteriorment. Un altre factor que es necessita tenir en consideració, és que per definir una funció es fa servir l'abreviació *def* seguida del nom de la funció, un igual, dos parèntesis i dos punts (per exemple: *def xifrar():*), dins els parèntesis podem posar les variables de la funció.

Un cop hem creat una funció, hem de definir com actuarà la funció. Per fer-ho hem de tenir coneixements bàsics sobre com escriure cada cosa, a mesura que s'expliqui l'exemple del xifratge de Vigenère es mostraren en anotacions precedides pel símbol #, per tal de no confondre amb el contingut del programa (escrit amb negreta, també per identificar-lo). Procedim a mostrar com s'ha creat el programa:

abcd = " .,'abcdefghijklmnopqrstuvwxyzç" # Primer de tot hem de definir el nostre alfabet, al qual podem afegir símbols, caràcters, les vocals amb accent... *abcd* és la manera curta d'anomenar la nostra cadena, l'alfabet que feia servir Vigenère només contenia les lletres de l'alfabet.

def xifrar(cadena, clau): # Ara creem la funció xifrar segons les variables de la cadena i de la clau (*cadena, clau*). Tot el que es troba i modifica la funció s'ha de trobar en una posició més a la dreta que l'inici de la definició de la funció, és a dir, amb una sagnia major.

text_xifrat ='' **#** Per a crear una variable que anomenarem text_xifrat, fem servir l'igual seguit de dues cometes.

i = 0 # És la variable que fa iniciar en 0, ja que el primer caràcter de la cadena *abcd* no és l'1, sinó el 0.

for lletra in cadena: # Per a xifrar necessitem crear un bucle en la cadena, i ho fem amb la nomenclatura *for lletra in cadena*, que significa: "per cada lletra de la cadena:". A continuació definim els paràmetres que actuaran com a bucle.

suma = abcd.find(lletra) + abcd.find(clau[i % len(clau)]) # El que estem buscant és la suma de la posició que ocupa la lletra en la cadena (*abcd.fin(lletra)*), i de la posició que ocupa la clau en la cadena. Per això localitzem la clau dins la cadena (*abcd.find(clau[])*), però si la suma és més gran que la longitud de la cadena no podríem obtenir cap resultat. Per aquest motiu posem la condició [*i % len(clau)*], la *i* ens mostra la posició de cada caràcter dins la cadena, mentre el *%* és el mòdul de la longitud de la clau (*len(clau)*). Serveix simplement en el cas que el missatge a xifrar sigui més llarg que la clau. Llavors, necessitem fer el mòdul, és a dir, *i* entre la longitud de la clau, i agafant com a resultat el residu. El que indica és que el valor obtingut de [*i % len(clau)*] no superarà mai la longitud de la clau, per tant, quan arribem a la lletra final de la clau, torna al principi. Per exemple, si la clau és **pol**, la quarta lletra del misatge s'encriptarà com a **p**, igual que la primera.

mòdul = int(suma) % len(abcd) **#** Fem el mòdul igual però amb la cadena. Per què l'operació sigui vàlida passem la *suma*, o resultat de l'apartat anterior, a valors enters, amb *int(suma)*. Aquest en el mòdul de la longitud de la cadena [*len(abcd)*].

text_xifrat = text_xifrat + str(abcd[mòdul]) # Només fa falta xifrar. Per a això indiquem que el text xifrat final (*text_xifrat*) suigui el mateix text que volem xifrar, anomenat també *text_xifrat*, més la suma de la posició de la cadena especificada pel mòdul que hem obtingut en el pas anterior(*str(abcd[mòdul])*).

i = i + 1 # Per a que la *i* vagi en increment es defineix com a *i + 1*.

return text_xifrat **#** Retornem el text xifrat

def main(): **#** Definim la funció *main*.

a = str(input('cadena a xifrar: ')).lower() # Per a localitzar la cadena que hem de xifrar, representada com *a*, hem de posseir la informació en *str*, i obrim parèntesi per indicar tot el que afectarà. *Input* és allò que volem que el programa

imprimeixi en obrir-lo, en aquest cas *cadena a xifrar:*. Si hi ha alguna majúscula, la funció *.lower()* la converteix en minúscules. Si el nostre alfabet fos en majúscula usaríem *.uper()*, i si aparaguessin les dues no s'afegiria res.

clau = str(input('clau alfabètica: ')).lower() # Llegeix i emmagatzema la clau que ha introduit l'usuari. Igual que anteriorment, en executar el programa ens apareixarà la demanda d'una *clau alfabètica:*.

print (xifrar(a,clau)) # Tot el que hem escrit a la funció *main* té l'objectiu de retornar-nos la cadena ja xifrada, per això indiquem que imprimeixi (*print*) la cadena xifrada (*xifrar*) segons la cadena (*a*) i la clau (*clau*).

if __name__ == '__main__': **#** Especifiquem la funció *main* per a que el

main() programa pugui funcionar.

Per a desxifrar fem servir la mateixa metodologia que hem fet servir per xifrar, modificant caràcter a caràcter per obtenir el text en clar.

def desxifrar(cadena, clau): # Enlloc de definir la funció xifrar definim la de *desxifrar*.

text_xifrat =''

i = 0

for lletra in cadena:

suma = abcd.find(lletra) - abcd.find(clau[i % len(clau)]) # Com que en el procés de desxifrar enlloc de sumar la posició de la lletra amb la de la clau, es resten per obtenir el valor original.

mòdul = int(suma) % len(abcd)

text_xifrat = text_xifrat + str(abcd[mòdul])

i = i + 1

return text_xifrat

def main(): # La funció *main* la definim igual ja que és el que volem que aparegui en executar el programa.

a = str(input('cadena a desxifrar: ')).lower() # Ara la cadena que haurem d'introduir és la de *desxifrar*, per això es modifica.

clau = str(input('clau alfabètica: ')).lower()

print (desxifrar(a,clau)) # El programa ens dóna el missatge desxifrat segons la cadena i la clau (*desxifrar(a,clau)*).

if __name__ == '__main__':

main()

4.4 El criptoanalista anònim

La figura més reconeguda en criptoanàlisi del segle XIX és Charles Babbage, un geni britànic que dissenyà el primer projecte d'un ordinador modern. Nascut el 1791, i fill de Benjamin Babbage, un ric banquer de Londres, inventà el velocímetre. També va elaborar un conjunt de taules de mortalitat, una eina bàsica en la indústria d'assegurances de vida, i deduí que es podia estudiar el clima del passat estudiant arbres centenaris.

Com s'ha demostrat era un veritable geni, i era molt perfeccionista. Tant que el 1821, mentre feia taules matemàtiques junt amb John Herschel, útils en astronomia navegació i enginyeria, va voler dissenyar una màquina capaç de fer tots els càlculs sense errors. El portà a fer el projecte, i va acabar de dissenyar-lo el 1823, conegut com a la màquina diferencial No.1 . Tot i que era un brillant innovador no va portar mai a terme el seu disseny i deu anys més tard abandonà el desenvolupament de la màquina per començar-ne un de nou amb el mateix objectiu, la màquina diferencial No.2. Però un cop abandonat el primer, el govern anglès no finançà més el seu projecte i mai l'acabà, tot i així la seva aportació seria vital en la segona guerra mundial, ja que aconseguí un disseny de màquina amb memòria i processador.

Babbage, fascinat per la criptoanàlisi des de ben petit, va fer un gran treball en la criptoanàlisi. A arrel d'un intercanvi epistolar amb un amic, Charles va treballar en desxifrar l'algoritme polialfabètic. Mentre la majoria de criptoanalistes donaven al quadre de Vigenère una seguretat perfecta, Babbage va aconseguir determinar un mètode senzill per a resoldre qualsevol algoritme polialfabètic. Per a fer-ho es va basar en el nombre d'alfabets de xifratge usats per a encriptar el missatge, és a dir, la longitud de la clau. Per exemple la clau **MONKEY** presenta sis alfabets de xifratge. Aquesta característica que el defensava de l'anàlisi freqüencial seria el pany en que Charles trobaria la clau per dexifrar-lo. Es basava en la repetició de certs caràcters al llarg d'un text xifrat, a partir dels quals en deduia la longitud de la clau. I un cop conegut el nombre d'alfabets de xifratge només calia fer un anàlisi de freqüencies per a cada lletra trobada en la posició n x y, sen n la longitud de la clau i y els nombres naturals, després en (n+1) x y, a continuació (n+2) x y... successivament fins que el nombre sigui igual

a n, en aquest cas fins a (n+5) x y. En veiem un exemple definit en detall a continuació:

En el cas que interceptem el missatge:

"**vesshyowikuroijpepovçyqpygikmdxsokrçsebwjynizspjorqaiikvyyijqyfk**", hem de buscar repeticions en la cadena. Podem veure remarcades totes les repeticions que trobem. La seqüència **ik** aparèix tres vagades, separada per 18 espais i 27, mentre les lletres **ij** es troben a 45 espais. És lògic que la longitud de la clau sigui un nombre que els seus múltiples siguin 18, 27 i 45 entre d'altres. Per tant les úniques longituds vàlides són 1, 3 i 9, tot i que una clau amb 1'alfabet de xifratge és il·lògic ja que amb un anàlisi freqüencial en trobaríem el text en clar. Per tant la longitud de la clau és 3 o 9. Al ser un text tant curt no en tenim una longitud exacta, però si féssim un exemple més extens segurament aconseguiriem trobar la longitud de la clau.

Suposarem que hem fet servir 3 alfabets de xifratge i analitzarem en detall. Podem dir que la clau és **A1, A2** i **A3**. Trobats en aquest punt només cal fer un anàlisi freqüencial per a cada lletra. En el cas de **A1** les lletres que observerem seran les que es troben en la primera, quarta, setena... (1+ múltiples de 3) posició. Les lletres més repetides són la **k-o-y-s**. Tal i com podem veure, entre la **k** i la **o** hi ha quatre espais, pel que es pot deduir amb facilitat que la **k** equival a la **a** del text en clar i la **o** a la **e**. Sent així la **s** la **i**, i la **y** la **o**. Ja coneixem que **A1** és igual a **K**.

"v s o k o p o y y k x k s w n s o a k y q k "

Per a **A2** seguirem el mateix procediment però agafant les lletres en segona, cinquena, vuitena... (2+ múltiples de 3) posició. Les més repetides són la **i-e-v-r**. Entre la **i** i la **e** hi ha quatre espais, que equivalen a la **a** i la **e**. De manera que la **e** correspon a la **a** i la **i** a la **e**, mentre la **v** substitueix a la **r** i la **r** a la **n**. També podria ser que la **r** fós la **a**, sen així la **v** la **e**, però en aquest cas la **i** equivaldria a la **r** i la **e** a la **n**. Casualment hi ha la mateixa probabilitat. Per tant **A2** pot ser igual a **E** o a **R**. Ho comprovarem al final, tot i que l'absència de lletres abans de la e, com són la ç-a-c-d, fan creure que l'alfabet correcte és el **E** ja que correspondrien a la x-y-z-ç de l'alfabet clar. Mentre que apareix una **m,** que en el cas que fós **R,** substituiria a la **x**, poc comuna en català.

"e h w u i e v q g m s r e j i p r i v i y"

Per a **A3** és exactament el mateix, i obtindrem que equival a **Y**.

“s y i r j p ç p i d o ç b y z j q i y j f”

El resultat obtingut amb la clau **KEY** és: “lavidaeslaqueemfasercomsoclaignoranciaemfadebilmentrelaraoemguia”, si el separem i puntuem com toca queda: “la vida és la que em fa ser com sóc, la ignorancia em fa dèbil, mentre la raó em guia”. Per tant queda demostrat que l’alfabet polialfabètic no és tant segur com es creia, i es pot acabar desxifrant sense tenir coneixement de la clau. En el cas que el missatge obtingut no tingués cap sentit canviariem la **E** per la **R**, la segona opció més probable, i sino agafar la clau de longitud de nou llocs, però aquí ja hem aconseguit el nostre objectiu.

Aquest senzill tot i que llarg mètode fou completat als vols del 1854, encara que mai en publicà res. Tal i com va fer amb la màquina diferencial N.1, Babbage no acabà del tot la seva feina tot i ser un geni. Va ser anys després, pel segle XX, que estudiant les seves notes es va descobrir que el primer en desxifrar l’algoritme polialfabètic va ser Charles. Babbage va ser durant nou anys l’únic que coneixia el punt dèbil de l’algoritme, fins que el 1863, l’oficial prussià Friederich Wilhelm Kasiski va fer públic un mètode similar. Per això Babbage no ha tingut el reconeixement fins anys posteriors, i es coneix com a mètode kasiski el conjunt de passos per resoldre una clau polialfabètica.

També hi ha hipòtesis que expliquen el fet de la no publicació dels seus descobriments. Podria ser que per a tal de beneficiar el seu país, no divulgués aquesta informació, pràctica que es repetiria durant el segle XX. A més, la seva innovació fou després de l’esclat de la guerra de Crimea, i Babbage proporcionava una clara avantatge als britànics sobre els russos.

Sigui un cas de protecció nacional, o un costum de no acabar els seus projectes, el que és evident és que el xifrat polialfabètic ja no era segur. La dificultat era trobar claus tan llargues que l’anàlisi de freqüencies i el mètode Kasiski, no funcionessin. Per altra banda els criptoanalistes volien agilitzar el procés d’obtenir la informació sense la clau. Ambdós processos passaven per un mateix punt: la mecanització.

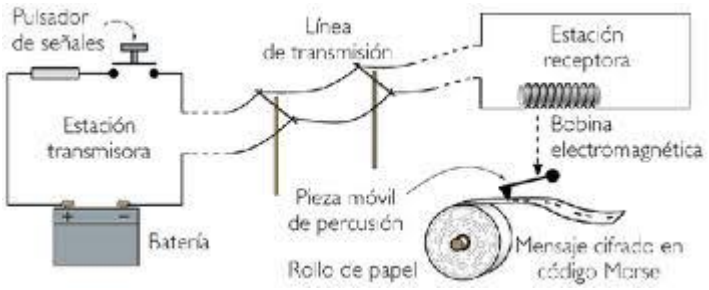
4.5 La mecanització

A finals del segle XIX la criptografia es trobava en desordre, i la comunicació segura no existia. A més, amb el descobriment del telègraf es buscava que la informació

no pogués ser interceptada i desxifrada. Però com funcionava el telègraf? Com es podien convertir els corrents elèctrics en missatges?

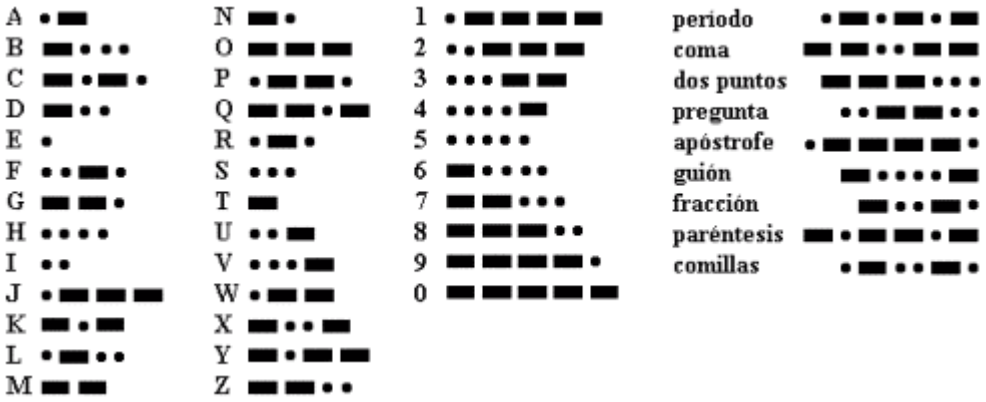
La solució a aquest problema la trobà Samuel F. B. Morse. El físic i pintor estatunidenc, que dissenya un sistema de barres i punts. El codi Morse representa l'abecedari, els números i els altres signes per mitja de la combinació de punts, barres i espais. Aquest fet feia possible la comunicació senzilla per via lluminosa, sonora o elèctrica. Es posà en pràctica l'ús del codi Morse en línies telegràfiques el 1843, amb financiació governamental. El 1844 ja hi havia més de 300.000 kilòmetres de cablejat per l'ús del telègraf. Un aparell relativament senzill format per una clau telegràfica de transmissió que tenia la funció d'interruptor de la corrent elèctrica, i d'un electroimant que rebia la senyal. Formava corrents elèctriques en oprimir la clau telegràfica, enviant així al cablejat elèctric els impulsos intermitents.

L'aparell receptor dels impulsos elèctrics estava format per un electroimant amb una bobina de filaments de coure enrotllats al nucli de ferro. Quan la bobina rebia els impulsos elèctrics el nucli de ferro es magnetitzava i atreia una peça de ferro mòbil que colpejaba un paper i emitia un so sec i peculiar, més curt o llarg depenent de si equivalia a un punt o una ralla. El funcionament es veu exposat en la imatge següent:



Il·lustració 2: Funcionament del telegrama.

I el missatge era entès gràcies a taules com la següent:



Il·lustració 3: Possibles signes rebuts per un telegrama.

Tot i que l'invent en comunicació més important del segle XIX el va fer l'italià Guglielmo Marconi, que intensificava la necessitat de poder encriptar de forma segura un missatge.

Al 1894, Marconi, mentre estudiava algunes propietats dels circuits elèctrics descobrí que sota certes condicions era possible passar un corrent elèctric d'un circuit aïllat a un altre. Amb poc temps, usant amplificadors, va poder rebre informació i enviar-la a uns dos kilòmetres i mig de distància. Havia inventat la ràdio, és a dir la comunicació per ones electromagnètiques. Al contrari que amb el telègraf ja no eren necessaris llargs cablejats per poder comunicar-se, ja que es feia a través de l'aire. Per tant, les línies telegràfiques van passar de tenir una gran importància en la comunicació, a ser un element innecesari.

Tot i que l'invent de Marconi proporcionà als criptoanalistes grans cantitats de texts xifrats amb algoritmes ja coneguts, degut a que és més fàcil interceptar una ona electromagnètica, que viatge en totes direccions, que un corrent elèctric, que ho fa per un cablejat, també aportà un enorme avantatge en el camp militar. Com és evident els generals abans de l'invent de la ràdio no es podien comunicar amb els seus soldats quan eren en una expedició o batalla, ja que no hi havia cablejat telegràfic per tot arreu, i menys al mar. També es podia avisar dels moviments de l'enemic durant una batalla o canvis de tàctica a última hora. Per aquests motius l'ús d'ones i receptors d'ones va ser un important invent en el camp militar, entre altres.

Tant la força que proporcionava militarment, com la debilitat d'interceptar fàcilment un missatge, impulsà l'ús d'un mètode criptogràfic per a què el missatge enviat per ràdio sigués intel·ligible. L'invent de Marconi també va ser el punt clau del

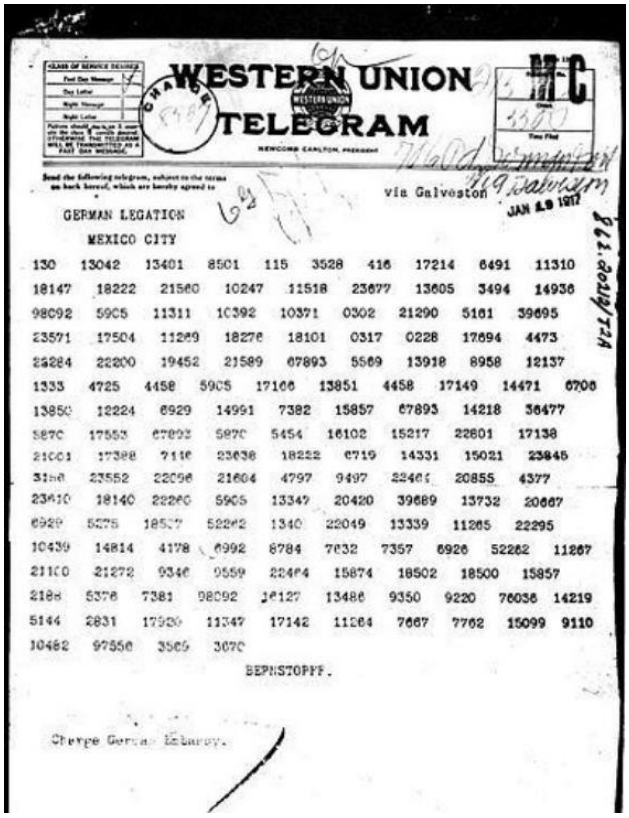
desenvolupament de la Primera Guerra Mundial. Entre el 1914 i el 1918 no hi va haver grans descobriments, és cert que es van inventar nous mètodes, però els criptoanalistes els trencaven un rere l'altre. El bàndol Aliat tenia un gran poder en el camp de la criptoanàlisi, i Alemanya en pagà les conseqüències el 17 de gener del 1917, quan els britànics van interceptar un telegrama alemany. Estaven planejant formar una aliança amb Mèxic, i que aquest ajudés a la guerra a canvi que després les dues forces militars recuperessin territori als americans, els quals es mentenien neutrals. Tot i que després que un vaixell estatunidenc fós enfonsat s'uniren amb els aliats. A més, l'incorporació de Mèxic als alemanys implicava que l'exèrcit americà es mantingués als Estats Units i no a Europa. El telegrama escrit per Zimmermann va ser enviat a l'ambaixada alemanya de Mèxic, amb la intenció que aquest arribés en mans del president, i formulava el següent propòsit:

«Ens proposem començar el primer de febrer la guerra submarina sense restricció. Malgrat això, ens esforçarem per a mantenir als Estats Units d'Amèrica neutrals. En cas de no tenir èxit, proposem una aliança amb Mèxic sobre les següents bases: fer la guerra junts, fer la pau junts, ajuda financera abundant i l'enteniment per la nostra part que Mèxic reconquerirà el territori perdut a Nou Mèxic, Texas i Arizona.

Cal informar de tot això al president (de Mèxic) el més secretament possible tan aviat com la guerra amb els Estats Units d'Amèrica estigui a punt d'esclatar. Suggereixo també que el President de Mèxic consideri la possibilitat de convidar el Japó, a iniciativa pròpia, a adherir-se immediatament a aquest pla i, al mateix temps, oferir la seva mediació entre Japó i nosaltres.

Li prego que també faci notar al President que la utilització despietada dels nostres submarins, ofereix la perspectiva d'obligar Anglaterra a fer les paus en pocs mesos.»

El telegrama de Zimmermann es veu en la següent imatge:



WESTERN UNION

TELEGRAM

via Galveston

JAN 19 1917

GERMAN LEGATION

MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7110 23638 18222 6719 14331 15021 23845
3180 23552 22290 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13349 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3070

BERNSTORFF.

Charge German Embassy.

Il·lustració 4: Telegrama de Zimmermann.

Aquest missatge va ser dut a la sala 40, on es trobaven els criptoanalistes més importants de l'època, allà Montgomery i Nigel de Grey van treballar per desxifrar el missatge urgentment, ja que per l'encriptació del text suposaven que era diplomàtic. En pocs dies ja havia estat desxifrat totalment i es van veure els plans del ministre d'exteriors alemany. Tot i que es deia en el telegrama que els Estats Units d'Amèrica ja no es mantindrien en una posició neutral, el 3 de febrer de 1917 anunciaren els propis estatunidencs que es mantindrien com a pacificadors. Per això els anglesos no van tenir més remei que mostrar el telegrama Zimmermann. A finals de febrer el president americà llegí el missatge, i observà una greu i directa agressió contra Amèrica, i el feu canviar d'idea pel crim contra la població dels Estats Units d'Amèrica. Passà d'estar a favor de la pau, a voler entrar en guerra amb els Aliats.

4.6 El desenvolupament de les màquines d'encriptació

La Primera Guerra Mundial mostrà un seguit de victòries dels criptoanalistes culminades pel telegrama Zimmermann, i els anys posteriors s'intentà trobar un mètode basat en les màquines i no en la taula de Vigenère i altres, que es feien amb paper i llapis. Per tant hi va haver un esforç per part dels criptògrafs en la mecanització de l'encriptació.

El primer aparell criptogràfic conegut va ser el disc d'Alberti, inventat el segle XV per l'italià Leon Alberti, un dels pares del xifrat polialfabètic. Agafà dos discs, un més llarg que l'altre, i en va escriure un alfabet en cada un dels dos. Els uní amb una agulla o alguna cosa semblant, formant un disc semblant al de la següent imatge, usat a la guerra civil nord-americana:

Il·lustració 5: Disc de Lion Alberti.

Cada un dels discs rotava independentment, formant així diferents posicions, podent fer servir el disc com a eina per encriptar un missatge per l'algoritme de Cèsar. Amb antelació ja hem exposat com es fa un xifrat usant el mètode Cèsar, i és el mateix sistema, l'únic que usem un disc per facilitar la tasca.

Al mateix temps el disc es pot usar per encriptar un text en l'algoritme polialfabètic si es va rotant la posició de l'alfabet extern. Si la clau és **LEON** per xifrar la primera lletra els discs estaran alineats amb la **A** i la **L**, la segona la **A** amb la **E,** la tercera la **A** amb la **O** i com és evident la quarta la **A** amb la **N**... les següents anirien repetint la clau, **LEON**. Per tant el disc d'Alberti era útil per qualsevol rotació de l'alfabet, tant monoalfabètic com polialfabètic. A més, n'evita els possibles errors, ja que el quadre de Vigenère has de mirar bé les files i columnes, i hi ha moltes lletres al voltant, en canvi amb el disc, la possibilitat d'equivocar-se és mínima. Tot i que l'invent

d'Alberti no proporcionava un mètode infal·lible, ja que Babbage i kasiski van trencar aquests algoritmes de rotació. Tot i així, cinc segles més tard una nova màquina més complexa que el disc portaria a una nova era dels xifrats, més difícils de trencar que cap dels vists fins ara.

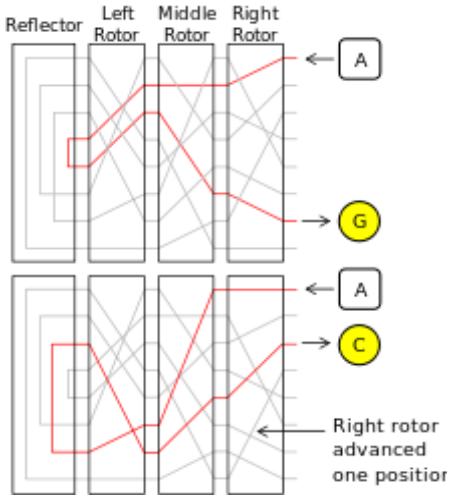
4.7 Enigma

En el any 1923 l'enginyer alemany Arthur Scherbius patentà una màquina derivada del disc d'Alberti, molt més complexa per a encriptar de manera més segura. Arthur treballava en la seva pròpia empresa Scherbius, fundada juntament amb Richard Ritter. Es dedicaven a la recerca i desenvolupament de mètodes combinats per xifrar un text, els usats a la Primera Guerra Mundial amb altres que caracteritzarien el segle XX. Al final aconseguí el seu objectiu, gràcies a tenir grans coneixements d'enginyeria elèctrica. El seu invent era una versió del disc d'Alberti però amb circuits elèctrics, anomenada Enigma, que revolucionà el món de l'encriptació. El nom d'Enigma, ha passat a significar el secret militar, per això es relaciona amb laboratoris subterranis i màquines de gran complexitat.

La màquina Enigma era portàtil, i era una màquina electromecànica de rotor. Estava formada per un conjunt de subsistemes mecànics i elèctrics. El mecànic era el teclat alfanumèric, i un seguit de discs giratoris que s'anomenen rotors, que s'unien a un eix. Al tocar una tecla els mecanismes fan avançar més o menys els rotors. El mecanisme per avançar depenia del model, tot i que en la majoria, el rotor dret feia una passa cada vegada que es premia una lletra, mentre els altres ho feien ocasionalment. Això implicava que al teclejar dues vegades seguides la mateixa lletra en clar, el resultat xifrat fos dues lletres diferents, ja que el circuit elèctric canviava. Per tant en el teclat s'il·luminaven dues lletres diferents.

Al prémer una tecla, es tanca el circuit, el corrent passa per diferents components i al final encén la bombeta de la lletra ja xifrada, i només cal apuntar la lletra. Per això cada vegada que una lletra era teclejada, els rotors canviaven de posició, fent així una encriptació polialfabètica molt segura.

En la següent imatge es descriu com funcionen els rotors:



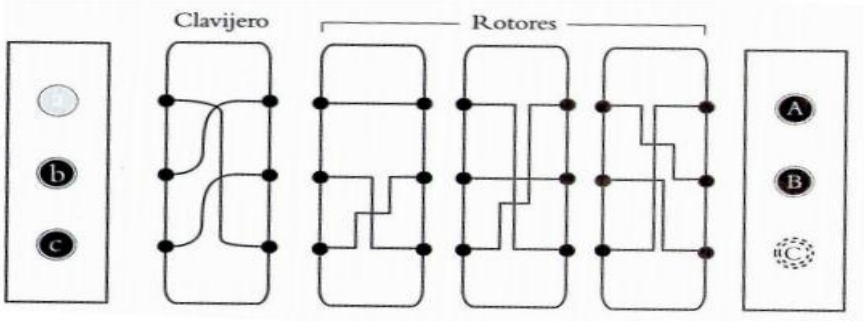
Il·lustració 6: Funcionament dels rotors d'Enigma.

Com es pot veure hi ha tres rotors. Cada un té un cablejat elèctric que acaba tancant el circuit il·luminant una lletra. A més, trobem un reflectant que té la funció de poder desencriptar un missatge, ja que com podem observar en la primera imatge al clicar la **A** el circuit fa il·luminar la lletra **G**, però si cliquéssim la **G**, el resultat seria la **A**. En canvi el segon cop que cliquem la **A**, el rotor de la dreta ha girat una posició, i tot el circuit canvia completament. En aquest segon cas la lletra resultant serà la **C**. Per tant la funció del reflectant, es mostra alhora de desencriptar un missatge.

En aquest exemple només apareixen 8 lletres, però la màquina Enigma hi havia 26 lletres, és a dir 26 posicions possibles. Per tant només amb el gir del primer rotor es formaven 26 alfabets diferents, però per complicar-ho més, cada cop que el primer rotor avançava 26 llocs, el segon rotor n'avançava un, és a dir un vint-i-sisè de volta. I quan el segon rotor completava un gir de 360 graus, el tercer rotor girava un vint-i-sisè de volta. Això suposa que hi ha un total de 26 * 26 * 26 = 17.576 de diferents alfabets només tenint en compte les posicions dels rotors. Aquest nombre de possibles alfabets és també el nombre de possibles inicis per desencriptar un missatge. Per tant, per trencar un text xifrat amb Enigma necessitaríem provar les 17.576 opcions, col·locant els rotors en una posició determinada i teclejar un tros del missatge interceptat per veure si té sentit. Suposant que cada minut es pot provar una disposició dels rotors, i treballant dia i nit, necessitaríem poc més d'un parell de setmanes en trencar-lo. (17.576/60/24 = 12,2055556 dies). Si treballessin en un mateix xifratge 12 persones, es trigaria poc més d'un dia en trencar el xifratge i obtenir el missatge en clar a partir de la força bruta.

Va ser per aquest motiu que Scherbius va incorporar altres factors que augmentaven el nombre de possibles alfabets. Un factor va ser poder intercanviar els rotors de posició, és a dir, poder moure el rotor de la dreta al mig, i el del mig a la dreta, això implicava 6 possibles posicions: 1-2-3, 1-3-2, 2-1-3, 2-3-1, 3-1-2 i 3-2-1.

L'altre factor va ser la incorporació d'un claviller que permetia canviar parells de lletres, en els primers models es podien canviar 6 lletres. No es va incorporar un altre rotor ja que ocuparia un gran espai addicional. La incorporació del claviller suposava un gran augment en el nombre de possibilitats, com es veu en la imatge següent:



Il·lustració 7: Funcionament del claviller i rotors d'Enigma.

Aquí es mostra un exemple simplificat, però en el cas de poder combinar N = 26 lletres i n = 6 claus o pars de lletres, ve donat per la fórmula següent:

$$\frac{N!}{(N-2n)! \cdot n! \cdot 2n} = 100.391.791.500 \text{ combinaciones.}$$

Tenint en compte tots els factors que influencien en el nombre de possibles claus, obtenim que pels rotors hi ha 17.576 possibles claus, per la posició dels rotors 6 i gràcies al claviller 100.391.791.500 combinacions. El producte de la multiplicació dels tres ens mostrarà el nombre de possibles alfabets que té Enigma: 17.576 * 6 * * 100.391.791.500 = 10.586.916.764.424 combinacions. Per tant, aconseguir trencar un missatge encriptat per Enigma, era quasi impossible pels més de deu bilions de possibles inicis.

Tot i ser una màquina complexa, el seu ús era relativament senzill, i la complexitat del missatge encriptat va fer que el govern alemany usés l'invent d'Arthur

per encriptar tot missatge militar durant la Segona Guerra Mundial. Aquest va ser el principal motiu pel qual els governs enemics a la Alemanya nazi prioritzaren el desxifrat d'Enigma. Al final s'aconseguí desxifrar els missatges, i aquest va ser el detall que inclinà la balança a favor dels Aliats. La història que envolta Enigma és fascinant, en la que intervingueren majoritàriament els criptoanalistes de Polònia i del Regne Unit, i el matemàtic Alan Turing, el pare de la computació moderna. Va ser ell qui intentant desxifrar Enigma creà el primer ordinador de la història, un gran pas per a la criptoanàlisi militar, i pel desenvolupament del món tal i com el coneixem avui en dia.

El resultat de l'invent de Scherbius és la màquina Enigma, on en trobem imatges a continuació:

Il·lustració 8: Màquina Enigma.

4.8 Desxifrar el codi Enigma

Per a poder encriptar un missatge amb Enigma i anar canviant dia rere dia la clau utilitzada es necessitava especificar les lletres intercanviades en el claviller, i la posició dels rotors, tant l'ordre com la orientació. Aquesta informació anava donada per llibres de claus, que alhora eren encriptats.

També és cert que per evitar enviar durant tot un dia sencer missatges amb la mateixa clau, els alemanys codificaven amb la clau del dia tres lletres que indicaven una nova posició dels rotors. Per més seguretat repetien les tres lletres, per exemple **D-H-S-D-H-S**, mantenint el claviller i l'ordre dels rotors igual. D'aquesta manera s'evitava que tots els missatges xifrats en un dia fossin interceptats i compresos, segurament trencats per atzar.

Les primeres informacions sobre Enigma que van obtenir els Aliats van ser gràcies a Hans-Thilo Schmidt, un alemany que va ser soldat i va fracassar en els seus negocis després de la Primera Guerra Mundial. Aconseguí feina al centre d'encriptació alemany gràcies a l'alt rang del seu germà, el qual organitzava tot allò relacionat amb Enigma. Hans-Thilo, envejós del seu germà, i davant la pàtria que el va rebutjar, es va voler venjar per aconseguir diners. Així el dia 8 de novembre de 1931 es va reunir a l'hotel Verviers a Bèlgica amb un agent secret francès amb el nom en clau Rex. Schmidt deixà fotografiar documents on s'explicava el funcionament d'Enigma, o alguna de les seves parts.

Aquesta informació proporcionà als Aliats aconseguir tindre el coneixement per a fabricar una màquina Enigma idèntica a la dels alemanys. Era un gran pas per aconseguir desxifrar els missatges nazis interceptats, però les possibles combinacions encara eren de més de deu trilions, pel qual, molts francesos consideraven impossible aconseguir trencar un codi. Gràcies a un acord de feia deu anys entre polonesos i francesos, el qual especificava l'intercanvi de qualsevol informació d'Enigma, entrà en acció Byuro Szyfrów, el departament de criptoanàlisi polonès. Aquests estaven convençuts de que hi havia una manera més curta per aconseguir trencar un missatge encriptat per Enigma. Tot i això, les fotografies només revelaven una part inicial de la màquina, com el cablejat dels rotors, per la qual cosa dedicaren esforç i enginy a la tasca.

En els documents obtinguts de Schmidt també s'exposava l'ús dels llibres de codis, en els quals es deia quin codi es feia servir cada dia, i es renovaven cada mes. Per exemple els codis d'un dia podien ser:

1. *Claviller:* ***S/E-F/M-H/L-R/N-W/U-A/Y***
2. *Ordre dels rotors:* ***3-1-2***
3. *Orientació dels rotors:* ***P-F-G***

Per a poder encriptar un missatge en aquest dia necessitaríem preparar la màquina de la següent manera:

1. *Claviller:* hauríem d'intercanviar els par de lletres **S** per la **E**, la **F** per la **M**, la **H** per la **L**, la **R** per la **N**, la W per la **U** i finalment la **A** per la **Y**, tots aquests es canviarien mitjançant el cablejat del claviller.
2. *Ordre dels rotors:* disposaríem el tercer rotor a la primera ranura, el primer rotor a la segona ranura i el segon rotor a la última.
3. *Orientació dels rotors:* disposaríem en el rotor de la primera ranura la lletra **P** en el lloc més elevat, ja que en cada rotor hi ha un abecedari escrit, permetent l'orientació a l'operador. En el rotor en la ranura intermèdia la **F** ocuparia el lloc més elevat, i en la tercera ranura la **G**.

Així es xifrava la informació durant un dia, tot i que depenent de la informació que contenia el missatge es feien servir codis alternatius a l'establert. També és cert que per no encriptar centenars de missatges en un dia amb el mateix codi, codificaven segons la posició del rotors tres lletres, que indicaven la nova orientació dels rotors, i les repetien per assegurar-se de no cometre cap error, d'aquí les sis lletres. Per exemple, la nova combinació d'orientació dels rotors podia ser **L-S-D**, que podia encriptar-se com a **W-S-A-F-T-B**. Com es pot veure es codifica de diferent manera, ja que els rotors es mouen. De manera que els receptors només tenien que canviar la orientació dels rotors després de les sis lletres i ja podia desencriptar el missatge sense problemes.

El motiu pel qual els alemanys duen a terme aquest sistema de canvi d'encriptació era degut al gran nombre de missatges que s'enviaven cada dia, ja que per un criptoanalista, com més texts escrits amb una mateixa encriptació hi hagi, més fàcil

ho tindrà. Això es deu a l'anàlisi freqüencial monoalfabètic, ja que com es pot deduir, en cada missatge la clau es repetiria, podent fent un anàlisi de freqüències per obtenir la clau. Per tant, canviant la clau tal i com s'ha exposat anteriorment, enviant codificada amb la clau del dia la nova orientació de rotors per a cada missatge, l'interceptor del missatge no tenia per on començar l'anàlisi freqüencial. Per aquest motiu Enigma semblava ser invulnerable.

Tot i així, els polonesos no van descansar intentant trobar un punt dèbil en la clau diària o del missatge. Byuro va fundar un curs de criptografia per a vint matemàtics, que juraren total lleialtat. Tots eren de la Universitat de Poznan, que tot i no ser la institució acadèmica més respectada, tenia l'avantatge d'estar situada a l'oest del país, territori que pertanyia a Alemanya fins el 1918. Per tant aquests matemàtics tenien influències alemanyes.

Tres dels vint seleccionats demostraren una bona actitud per a resoldre missatges xifrats, i s'incorporaren a Byuro. El més destacat va ser Marian Rejewski, un noi tímid de vint-i-tres anys que estudià estadística.

La estratègia de Rejewski per atacar Enigma es va centrar en l'estudi de les repeticions de les claus dels missatges. Aquest detall que servia per evitar qualsevol error, va ser el que va aprofitar per trencar els missatges d'Enigma. La única repetició que es podia estudiar eren les primeres sis lletres dels missatges, que eren codificades totes amb la clau del dia. Per tant, si l'emissor tria la clau del missatge **E-D-F**, i després encripta **E-D-F-E-D-F,** que pot ser encriptat com **C-Q-H-I-F-R**, i envia aquest seguit de lletres. De manera que interceptant una gran quantitat de missatges en un dia, tots tindrien en comú que les sis primeres lletres dels missatges s'encriptarien amb la mateixa clau. Per exemple, podia rebre cinc missatges que comencessin amb la següent seqüència de lletres:

	1a	**2a**	**3a**	**4a**	**5a**	**6a**
1r missatge	F	V	E	X	T	H
2n missatge	Q	G	K	D	W	A
3r missatge	X	D	K	C	J	A
4t missatge	R	S	X	L	Ç	Q
5è missatge	Q	V	C	D	S	F

Taula 11: Possibles combinacions de lletres de cinc missatges.

En cada missatge la primera i la quarta lletra són la mateixa lletra encriptada, el mateix passa entre la segona i la cinquena i la tercera i la sisena. Això implicava que en primer missatge, entre la **F** i la **X**, amb tres passos els rotors han canviat totalment. El fet que **F** i **X** siguin encriptacions de la mateixa lletra va permetre a Rejewski deduir alguna lleu limitació de la configuració inicial de la màquina. La posició inicial dels rotors, encara desconeguda, encripta la primera lletra de la clau del dia, també desconeguda, en **F**, i amb tres passos de la posició del rotor cap endavant, xifra la mateixa lletra de la clau del dia en **X**. De moment seguim desconeixent la clau, és a dir la posició i orientació dels rotors.

Pot semblar que no treiem res en clar, ja que desconeixem el més important, però demostra que **F** i **X** estan relacionades per la posició i orientació dels rotors. A l'interceptar tots els missatges, és possible identificar altres relacions entre la primera i la quarta lletra. Totes aquestes relacions es deuen a la posició inicial de la màquina Enigma. Per exemple, el segon i cinquè missatge s'indica que la **Q** i la **D** estan relacionades, en el tercer que la **X** i la **C** estan relacionades, i en el quart, la **R** i la **L**. Rejewski començà a tabular aquestes relacions, per cada par de lletres, obtenint una taula similar a la següent:

1a lletra	**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 Ç**
4a lletra	**X D L C**

Si el jove Rejewski tenia accés a suficients missatges en un dia, podia completar aquesta taula, i obtindria totes les relacions entre els alfabets, com pot ser exemple la següent taula:

1a lletra	**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 Ç**
4a lletra	**WE S F I X H T J ZM Q N P U B D L GR K Ç A C O V Y**

Tot i així la clau seguia sent una incògnita, però sabia que la relació entre la primera i quarta lletra era aquesta. Necessitava trobar un camí que el portés a descobrir la clau empleada en els missatges del dia. Rejewski començà a observar la taula en busca de patrons. I trobà un patró, que formava cadenes de lletres. Per exemple, en la

taula, **A** de la primera fila està lligada a **W**, i **W** de la primera línia es relacionava amb la **A**, tancant la cadena, així ho feu amb totes:

A→W→A 2 unions
B→E→I→J→Z→V→Ç→Y→O→U→K→M→N→P→B 14 unions
C→S→G→H→T→R→L→Q→D→F→X→C 11 unions

Només hem tingut en consideració la relació que hi ha entre la primera i la quarta lletra, però Rejewski ho va fer amb les tres relacions, repetint el procés entre la segona i la cinquena i la tercera i la sisena. També n'identificà les cadenes respectives.

Gràcies a aquest mètode s'adonà que depenent del dia les cadenes variaven amb consideració. De vegades n´hi havia moltes de curtes, d'altres unes poques llargues, com és el cas de l'exemple exposat. Com es pot comprendre, les lletres de les cadenes canviaven dia rere dia. La característica de les cadenes era clarament un resultat a la clau del dia, com a conseqüència del claviller, la posició del rotors i la seva orientació. Tot i així, el nombre de claus possibles no es veia reduït, i n'hi havia masses, tal i com s'ha exposat amb anterioritat, més de deu bilions; 10.586.916.764.424 opcions.

En aquest punt, on tot sembla que hagi estat en va, es descobreix un patró que tenen les cadenes, en concret, el nombre d'unions. Aquest no es veia alterat pel claviller. Es veu clarament en l'exemple de les cadenes que si la lletra **J** i la **R** han d'intercanviar el seu rol, i de la mateixa manera, si en el claviller també s'intercanvien la **G** i la **O** i com a última parella la **U** i la **T**, la cadena resultaria la següent:

A→W→A 2 unions
B→E→I→R→Z→V→Ç→Y→G→T→K→M→N→P→B 14 unions
C→S→O→H→U→J→L→Q→D→F→X→C 11 unions

Com es pot veure les cadenes segueixen tenint el mateix nombre d'unions, per tant el nombre de possibles claus es veu reduït en gran nombre. Ara només es pot considerar la posició dels rotors (6), i l'orientació d'aquests (17.576), que originen un total de 105.456 possibles claus. Per tant es simplifica en més de cent miliards de vegades.

Tot el treball de Rejewski es deu a l'espionatge de Hans-Thilo Schmidt, sense el qual no s'hagués aconseguit fer una rèplica d'Enigma. Va ser amb aquestes rèpliques que es va fer un manual, estudiant la longitud d'unions per a cada una de les 105.456 possibles claus. Van necessitar un any en acabar el manual, però un cop Byuro va tenir tota la informació, Rejewski va poder començar la desencriptació del xifrat d'Enigma.

A partir d'ençà ja podia fer taules de relacions amb les sis primeres lletres dels missatges. Això permetia poder comparar les cadenes resultants amb les del manual. Per exemple, les relacions entre la primera i la quarta lletra s'aconseguien tres cadenes de dues, onze i quinze unions. Analitzant també les relacions entre les altres lletres podríem obtenir entre d'altres opcions:

3 cadenes respecte la 1a i 4a lletra, amb 2, 11 i 14 unions
5 cadenes respecte la 2a i 5a lletra, amb 3, 4, 6, 7 i 7 unions
4 cadenes respecte la 3a i 6a lletra, amb 5, 6, 7 i 9 unions

Observant les relacions ja es podia comparar amb el manual, que contenia totes les possibilitats. De manera que ja s'havia trobat la posició i orientació dels rotors per a la clau del dia. Usant aquest mètode s'aconseguí desxifrar Enigma d'una manera força senzilla i ràpida. Tot i que encara quedaven milions de possibles combinacions dels claviller, aquesta tasca va ser més senzilla de resoldre.

Per a tal d'obtenir els parells de lletres que havien intercanviat el seu valor només feia falta traduir el missatge amb la clau del dia sense tenir en consideració el claviller, és a dir, només tenint en consideració la posició i orientació dels rotors. D'aquesta manera el missatge podia ser comprès, tot i que amb petits canvis. Per tant, al traduir un text podríem llegir **ataqulu ple onrd**, es podria entendre per "ataqueu pel nord". Si és correcte, la **E** i la **L** haurien intercanviat la seva funció, igual que la **N** amb la **O**. Analitzant un text, o més d'un, és relativament senzill trobar les parelles de lletres. De manera que ja es podia desxifrar qualsevol missatge d'Enigma amb un xic de paciència. Obtenint així la clau del dia, es podia desxifrar qualsevol missatge interceptat el mateix dia.

Tal i com hem vist amb anterioritat, amb un any calculant les cadenes de lletres i recopilant-ne la informació en un manual, Rejewski fou capaç de desxifrar un missatge amb menys d'un dia, quan en un principi era quasi impossible desxifrar una sola clau.

Les comunicacions alemanyes ja eren transparents per quelcom que interceptés un gran nombre de missatges en un dia, i tot i que Polònia no estava en guerra, Alemanya pretenia envair-la, però els polonesos podien descansar més tranquils després d'aconseguir que Enigma fos vulnerable. Ara podien preparar-se abans que els nazis ataquessin Polònia, tot gràcies a Rejewski, que va fer un dels grans èxits de la criptoanàlisis. Aquí no hi ha tots els camins que seguí el polonès, sinó que arriba a molts punts morts on va haver de tornar a començar amb la investigació. Enigma és una màquina complexa, i aconseguir desxifrar-ne un missatge sense la clau requereix una gran força intel·lectual i esforç.

L'èxit en trencar el xifrat de la màquina Enigma es deu a tres factors: la por, les matemàtiques i l'espionatge. La por dels polonesos en ser envaïts pels alemanys, sense la qual haguessin donat per impossible la tasca de desxifrar qualsevol missatge. Sense les matemàtiques i l'estadística, Rejewski no hagués sigut capaç d'analitzar les cadenes. I sense l'espionatge realitzat per Hans-Thilo Schmidt, anomenat Asche per no ésser identificat, i als seus documents, sobre el cablejat dels rotors, no hagués estat descobert.

Aquest mètode es va fer servir durant anys pels polonesos, fins i tot quan els alemanys dissenyaren una petita modificació de la manera d'enviar un missatge. Ja que Rejewski modificà el seu llibre de longitud de cadenes. A més a més, ideà una versió mecanitzada d'enigma que buscava la posició correcta dels rotors, la qual, amb dues hores provava cada una de les 17.576 possibles posicions. Entre les quals trobava una combinació amb sentit. La màquina de Rejewski funcionava només si treballaven 6 màquines en paral·lel, això es deu al fet que els rotors es poden disposar en 6 posicions diferents, per tant cada màquina n'interpretava una. Així es creà una unitat capaç de trobar la clau del dia amb menys de dues hores. Cada unitat s'anomenava *bombes*, el nom del qual prové del soroll que feien mentre es provaven totes les possibles orientacions dels rotors.

Durant la majoria dels anys 30, la vida de Rejewski i el seu equip consistia en trobar la clau del dia i desxifrar missatges interceptats. Tota aquesta feina era innecessària, degut que el cap de Byuro, Major Gwido Langer, tot i tenir les claus del dia, les mantenia amagades al seu despatx. Langer rebia per part d'espies els manuals amb les claus del dia que posseïen els alemanys, tot i així decidí no comunicar-ho a Rejewski. Per això la seva feina era innecessària i una pèrdua de temps, ja que treballava per descobrir la clau del dia quan el cap ja la tenia.

Les habilitats del polonès Rejewski arribaren a la cúspide quan al desembre del 38 els alemanys van augmentar la seguretat d'Enigma. Totes les màquines emprades pels alemanys van incorporar dos rotors nous, van passar de poder-ne triar 3 a poder-ne triar 5, incrementant així de 6 possibles combinacions dels rotors a 60, tal i com es veu a la següent taula:

Combinacions amb tres rotors	Combinacions extra amb dos rotors més								
123	124	125	134	135	142	143	145	152	153
132	154	214	215	234	235	241	243	245	251
213	253	254	314	315	324	325	341	342	345
231	351	352	354	412	413	415	421	423	425
312	431	432	435	451	452	453	512	513	514
321	521	523	524	531	532	534	541	542	543

Taula 12: Possibles combinacions amb cinc rotors.

El primer repte va ser trobar el cablejat interior dels dos nous rotors, sense els quals era quasi impossible desxifrar un missatge. El més preocupant, tot i això, era que la combinació de sis màquines Enigmes treballant al mateix temps s'havia de multiplicar per 10 per l'augment de les combinacions dels rotors. Això implicava construir 50 bombes noves, el preu del qual superava 15 vegades el capital emprat per Biuro d'un any. El mes següent la situació es complica encara més, amb la incorporació de quatre cables més d'intercanvi de lletres, en lloc de sis ara n'hi havia deu. Per tant, en lloc d'intercanviar dotze lletres ara n'eren, o en podien ser vint. El nombre de claus possibles augmentava a 159.000.000.000.000.000.000.

En el 1938, els missatges encriptats i el seu desxiframent per part dels polonesos es trobava en un moment de gran èxit, però a principis del 1939, els nous rotors i cables d'intercanvi de lletres fan canviar el flux d'intel·ligència. Rejewski, que havia demostrat que Enigma no era una màquina indesxifrable, no tenia els suficients recursos per provar cada possible combinació, no podia trobar la clau del dia, i el desxifrat era impossible. Sota aquestes circumstàncies, Langer podria haver lliurat el llibre de claus, però amb la incorporació dels dos nous rotors, Shmidt va acabar amb el contacte de l'agent Rex. Justament quan es necessitaven les claus, no les tenien.

La nova invulnerabilitat d'Enigma va ser un cop devastador per Polònia, ja que no només era una mera màquina de comunicació, sinó que era la base de l'estratègia del *blitzkrieg* de Hitler. El mot *blitzkrieg* (significa "guerra llamp") implicava atacs ràpids, intensos, coordinats, que significava la comunicació entre tancs, artilleria i infanteria. També era imprescindible la comunicació del front de batalla amb els avions de combat Stukas, que eren bombarders alemanys. Per tant, el *blitzkrieg* es basava en atacs ràpids i una ràpida comunicació. Si els polonesos eren incapaços de trencar Enigma, era impossible aturar els alemanys, que amb qüestió de mesos haurien ocupat Polònia. Alemanya ocupà els territoris del sud polonesos, i el 27 d'abril del 39 es va retirar el tracte de pau entre les dues potències. Amb tot això, si Polònia era envaïda, els mètodes criptoanalístics de Rejewski no beneficiarien més el país, i per aquest motiu, hauria de servir com a mínim per ajudar els Aliats.

El 30 de juny, Langer telegrafià a França i Anglaterra, invitant-los a Varsòvia per discutir alguns afers urgents sobre Enigma. El 24 de juliol els criptoanalistes francesos i anglesos es trobaven a la seu de Byuro, sense poder imaginar el que els esperava. Aquests nous vinguts estaven sorpresos en escoltar i veure el treball de Rejewski, aconseguit gràcies a anys de dura feina. Els polonesos es trobaven una dècada més avançats que ningú més al món. Els francesos estaven especialment sorpresos ja que el treball de Rejewski es basava en informació rebuda dels francesos, a la qual no donaven cap mena d'importància.

Com a sorpresa final, Langer oferí a França i a Anglaterra dos màquines Enigmes i les pistes per a dissenyar les bombes, que havien de ser embarcades en maletes diplomàtiques cap a París. Des d'allà, una de les màquines va ser enviada a Londres el 16 d'agost. La maleta amb la màquina va ser part de l'equipatge del dramaturg Sasha Guitry i la seva dona, l'actriu Ivonne Printemps, per no aixecar

sospites als espies alemanys. Dues setmanes després, l'1 de setembre Alemanya va envair Polònia i començà la guerra.

Els polonesos havien demostrat que Enigma no era un xifrat perfecte, i van demostrar als Aliats la importància de les matemàtiques com a criptoanàlisi. A Anglaterra, a la sala 40 només hi havia lingüistes i classicistes, en canvi a partir de llavors van aparèixer matemàtics i científics. Els nous contractats per a l'estudi del desxifrat també anaren a Bletchley Park, la seu del *Government Code and Cypher School* (GC&CS), una nova organització de criptoanalistes format a partir de la sala 40. Bletchley Park podia rebre més personal, el qual era important ja que la intercepció de missatges encriptats començà amb l'inici de la guerra. Durant la I Guerra Mundial, Alemanya transmetia 2 milions de paraules al mes, però l'ús de la radio en la II Guerra Mundial feu poder arribar a 2 milions de paraules al dia.

Bletchley Park era una gran mansió, on s'instal·laren barraques al voltant per a set mil homes i dones. Durant l'agost del 1939, els científics i matemàtics, varen estudiar les complexitats i els estudis i tècniques poloneses. Tenien molt més personal que Byuro, per tant, podien provar una quantitat enorme de possibles disposicions dels rotors, tot i que llavors desxifrar Enigma era una tasca molt més difícil. Per aquest motiu els criptoanalistes anglesos treballaven provant possibles combinacions fins a trobar-ne la clau del dia. Un cop arribava mitja nit la clau del dia canviava, i s'havia de buscar altre cop la clau, sense desxifrar tots els missatges interceptats. De manera que tenien 24 hores per trobar la clau del dia, i un cop aconseguida es disposaven a desxifrar tota la informació acumulada.

La sorpresa era i és una poderosa arma per a un general, però si Bletchley podia entrar dins Enigma, els plans alemanys serien transparents a ulls dels britànics, els quals podrien anticipar-se. De manera que podrien enviar reforços a un punt o fer atacs a les bases més dèbils. En el cas que poguessin desxifrar les comunicacions els Aliats podrien centrar els seus atacs. Per això els desxifrats de Bletchley eren de gran importància. Per exemple, quan Alemanya es disposa a envair Dinamarca i Noruega a l'abril del 1940, els criptoanalistes de Bletchley van poder informar de possibles bombardeigs, incloent-hi situacions exactes i la hora.

Un cop van ser uns experts en les tècniques poloneses, els criptoanalistes britànics començaren a dissenyar mètodes per a trobar la clau del dia amb més rapidesa, però no tanta com feu Rejewski. Per exemple, s'adonaren que a vegades les claus d'Enigma eren obvies. Ja que per a cada missatge, s'elegien tres lletres a l'atzar, per

això podien acabar posant tres lletres consecutives del teclat d'Enigma, com pot ésser **RTY** o **SDF**. Altres possibilitats eren les repeticions de la mateixa clau per un missatge, potser perquè eren les inicials del seu nom o de la mare de l'operador que les posava, com pot ser **CAR** (cal recordar que la clau de la que s'està parlant ara no és la del dia, sinó les tres lletres repetides que mostren la nova disposició dels rotors).

Alhora que Enigma anava evolucionant al llarg de la guerra, els criptoanalistes es veien obligats a innovar, redissenyar i modificar les bombes, a més d'investigar noves estratègies. Part de l'èxit aconseguit es devia a l'estranya combinació de les matemàtiques, la ciència, els lingüistes, els classicistes, grans jugadors d'escacs i addictes als puzles, cadascuns a unes cabanes. Un problema passava per totes les cabanes fins que algú n'aconseguia una solució. Tot i que, si s'ha de nomenar una persona pels seus mèrits, ha de ser, sens dubte, el matemàtic Alan Turing, qui identificà la major debilitat d'Enigma, i el va aprofitar. Gràcies a Turing va ser possible desxifrar la màquina fins i tot en el pitjor dels casos.

A l'inici de la guerra, Turing va deixar la seva posició a la universitat de Cambridge i es va unir a Bletchley Park. Passava la major part del seu temps a la sala del tanc dedicat a reflexionar. En aquest els criptoanalistes feien pluges d'idees per a intentar resoldre un problema, i anticipar-se a d'altres de possibles en el futur. Turing es va centrar en quines serien les conseqüències que tindria el fet que els alemanys canviessin el mètode de canvi de claus. Tots els èxits dels britànics giraven al voltant del treball de Rejewski, que s'aprofitava de la repetició de la clau del missatge, que repetia les tres lletres que informaven de la nova disposició dels rotors (per exemple: si la clau era **GHW**, l'operador encriptava **GHWGHW**). Aquesta repetició assegurava que el receptor no cometia un error, però provocava una obertura a la seguretat d'Enigma. Es creia que els alemanys no trigarien a notar que aquesta repetició era el motiu pel qual els seus missatges eren entesos, de manera que els operadors d'Enigma abandonarien la repetició, fent inútils les tècniques emprades a Bletchley. Trobar una alternativa a la manera d'atacar Enigma era la feina de Turing, ja que no confiava en la repetició de la clau dels missatges.

Passades unes setmanes, Turing es recordà que a la mansió de Bletchley hi havia una gran biblioteca de missatges desxifrats, i s'adonà que la majoria d'aquests seguien un patró estricte. Estudiant aquests missatges, va creure que a vegades podia predir part del contingut del missatge encriptat sense saber-ne la clau, es basava en la hora en que s'havia enviat un missatge i la seva font. Per exemple, els estudis mostraven que els

alemanys enviaven cada dia poc després de les 6 A.M. un informe sobre el temps, per tant si s'interceptava un missatge a les 6:03 A.M. es podia quasi assegurar que contenia la paraula **wetter**, la paraula "temps" en alemany. El protocol emprat pels militars a l'hora d'enviar una comunicació era estricte pel que fa a l'estil. Per això, Turing podia localitzar la paraula **wetter** sense el missatge desxifrat. Per exemple, l'experiència li deia que les sis primeres lletres del text en clar corresponien a la paraula temps. Quan una part del missatge en clar es pot relacionar amb una altra del missatge codificat, aquesta combinació es coneix com a *crib*, en anglès (la traducció literal seria bressol, però no em sembla adient en el context a no ser que fos l'inici de la tècnica de desxifrat d'Enigma).

Turing va demostrar que la posició del *crib* suposava una gran limitació en l'organització de la màquina emprada per xifrar el missatge. En altres paraules, era possible trobar la clau del missatge, i a partir d'aquesta la clau del dia, i usar-la per a llegir altres comunicats enviats aquell mateix dia. Tot i que encara calia comprovar milers de combinacions dels rotors per veure quin era l'adequat, per això Turing dissenyà una màquina per a fer la labor. Es va anomenar "bomba", després de la màquina de descodificació polonesa que ajudà a Bletchley Park a començar el desxifratge contra Enigma.

Mentre esperava la fabricació i lliuració de la primera "bomba", Turing seguia el seu treball diari. Les notícies de les seves investigacions no trigaren a arribar a oïdes d'altres criptoanalistes, que reconeixien que era un geni. Malgrat tot, tot el que envoltava el *Government Code and Cypher School* era un secret, per això fora de Bletchley Park ningú sabia res dels seus èxits. Per exemple, els seus pares no tenien ni la més remota idea de que Alan era un criptoanalista. És cert que un cop li digué a la seva mare que estava involucrat en una mena d'investigacions militars, però res més. Simplement perquè ella estava decebuda pel tallat de cabell del seu fill. Ja que treballava sota el control militar havia d'anar rapat. Però a Turing no li molestava aquest fet.

Pel final del 1941, hi havia quinze "bombes" en funcionament, aprofitant els *cribs*, provant combinacions dels rotors i revelant claus. Cada una retrunyint com un milió d'agulles de teixir. Si tot anava bé, la "bomba" hauria de trobar la clau del dia en una hora. Un cop la posició dels rotors i l'emparellament del claviller (la clau del missatge) es localitzaven per a un text, era fàcil deduir la clau del dia. Per tant ja es podia desxifrar tota la informació interceptada en l'interval de vint-i-quatre hores.

Tot i que les "bombes" suposaren un veritable avançament en la criptoanàlisi, hi havia molts obstacles per superar, com podia ser la recerca de la clau per part de la mateixa "bomba". Ja que per fer-la funcionar abans s'havia de localitzar un *crib*. El criptoanalista es podia equivocar a l'hora de donar un *crib* a l'operador de la "bomba", ja que havia d'interpretar el significat correcte d'una petita part d'un text xifrat. Per tant, havia d'endevinar el *crib* i la seva localització en el text. No obstant això, hi havia un truc per comprovar si el *crib* es trobava en la posició correcte.

En el següent *crib*, el criptoanalista està segur que el text en clar és correcte, però no pot assegurar si l'ha combinat amb les lletres correctes del text xifrat.

Possible text en clar	w e t t e r n u l l s e c h s
Text xifrat conegut	G L T O L E Z W T J S X C P L E R I S

Una de les característiques d'Enigma era la incapacitat de xifrar una lletra com ella mateixa, una conseqüència del reflector. La lletra **a** mai era encriptada com a **A**, la lletra **b** mai com a **B**, i així amb totes. El *crib* exposat anteriorment està clarament mal alineat, ja que la segona **e** de **wetter** està enllaçada amb una **E** del text xifrat. Per trobar la posició correcte del possible text en clar només hem de desplaçar el text fins que cap lletra estigui intercanviada per ella mateixa. Si la desplacem cap a l'esquerra l'alineació falla per les dues **t** de **wetter**, tot i que si la desplacem, cap a la dreta, no hi ha cap coincidència. Aquest *crib* pot ésser correcte, i pot ser la base pel desxiframent de la "bomba":

Possible text en clar	w e t t e r n u l l s e c h s
Text xifrat conegut	G L T O L E Z W T J S X C P L E R I S

La intel·ligència militar provenia dels desxifrats d'Enigma, nombrant l'operació relacionada amb Enigma amb el nom d'Ultra. Els arxius d'Ultra, que també contenien missatges desxifrats d'italians i japonesos, donà als Aliats un avantatge clar en els principals àmbits de la guerra. Al Nord d'Àfrica, Ultra va ajudar a destruir els subministraments alemanys, i informar de l'estat de les tropes al general Rommel i avançar-se als moviments alemanys. Ultra també alertà de la invasió alemanya de Grècia, permetent la retirada de l'exèrcit britànic sense patir gaires baixes. De fet, proporciona informes necessaris sobre l'enemic al llarg de tota la mediterrània. Aquesta

informació va ser particularment vital quan els aliats van desembarcar a Itàlia i Sicília el 1943. un any després, Ultra juga un paper important en la invasió aliada d'Europa.

El més important de tot, era sens dubte, usar aquesta informació de tal manera que no aixequessin sospites als militars alemanys. Per a mantenir Ultra en secret, els comandants de Churchill van prendre un seguit de precaucions. Per exemple, els desxifrats d'Enigma donaven als aliats les posicions exactes del vaixells alemanys, però hagués cridat l'atenció un atac a cada un d'ells, fent un seguit de victòries britàniques que només podien ésser explicades si les comunicacions no eren segures. Per això, un conjunt de vaixells es deixaven escapar. Altres d'aquestes embarcacions eren atacades només després que un avió britànic passes per damunt, fent així una explicació lògica de com ha estat localitzat. També es solien enviar missatges fals en els quals s'enviaven la vista de certs vaixells, que eren la conseqüència d'un atac imminent a aquell.

Tot i els numerables intents exitosos de minimitzar les sospites dels alemanys, alguns fets aixecaven sospites als experts en seguretat. En una ocasió Bletchley desxifrà un missatge d'Enigma informant de la posició exacte de tancs i vaixells de subministrament alemanys, nou en total. Els responsables d'utilitzar la informació d'Ultra van decidir enfonsar set dels vaixells, i deixar-ne escapar a dos, el *Gedania* i el *Gonzenhein*. Els set vaixells van ser enfonsats, però vaixells de l'armada anglesa es trobaren accidentalment les dues embarcacions amb subministracions, i els enfonsaren. Els de l'armada no coneixien ni l'existència d'Enigma o la política de no aixecar sospites. L'almirall Kurt Fricke investigà sobre aquest atac i d'altres de similars. Tingué en compte la possibilitat que els Aliats haguessin aconseguit trencar Enigma. Per sort, en el seu informe argumentà que era impossible trencar Enigma, i que aquests fets eren causa d'un conjunt de mala sort o d'un espia britànic que s'havia infiltrat a l'armada alemanya.

Ha estat argumentat que els èxits de Bletchley Park van ser un factor decisiu per la victòria dels Aliats. El que és indiscutible, es que els criptoanalistes britànics van fer més curta la guerra. Això es demostra visualitzant la batalla de l'Atlàntic i especulant què hagués passat sense la informació d'Ultra. Per començar, molts U-boots, vaixells de subministraments alemanys, havien estat enfonsats gràcies a l'operació aliada basada en el desxifrat d'Enigma. Aquests U-boots haguessin posat en perill la principal comunicació entre Amèrica i els Aliats, el mar. Segons historiadors aquest fet hagés retardat els plans aliats varis mesos, el que hauria posposat el desembarcament de

Normandia com a mínim fins el següent any. Això hauria costat moltes vides en ambdós costats.

Tot i així, la criptoanàlisi és una activitat clandestina, i va ser un secret fins passat el 1945. Desxifrant exitosament els missatges interceptats durant la guerra, els britànics volien continuar amb les operacions d'intel·ligència i no publicaren les seves habilitats, sinó que després de capturar milers de màquines Enigma les distribuiren per les seves colònies, les quals creien que el xifratge era segur. Els britànics no els van corregir, i els deixaren creure que les seves comunicacions eren segures, i de tant en tant desxifraven les seves comunicacions secretes.

Com a conseqüència, els milers d'homes i dones que contribuïren a la creació d'Ultra no reberen el reconeixement pels seus èxits. La majoria dels criptoanalistes tornaren a les seves vides quotidianes, amagant per obligació, el seu rol en la segona guerra mundial. Una altra conseqüència fou que mentre els soldats explicaven els fets heroics i les batalletes que visqueren, els que havien lluitat intel·lectualment havien de mantenir-ho en secret.

Després de tres dècades de silenci, pels principis dels anys 70, el capità F.W. Winterbotham, qui distribuí el secret d'Ultra, argumentà a les colònies angleses que l'ús d'Enigma no era una via de comunicació segura, i per tant que els britànics havien aconseguit trencar el seu xifrat. Els serveis d'intel·ligència el deixaren escriure un llibre sobre Bletchley Park, publicat l'estiu de 1974, titulat *The Ultra Secret*, el qual donava el mèrit que els criptoanalistes britànics mereixien.

Tot i el mèrit que reberen, alguns, com Alan Turing no van viure suficient per a presenciar aquests fets, i rebre un reconeixement públic. Abans de la guerra Turing havia mostrat ser un geni en el camp matemàtic, publicant treballs que serien la base per a la fabricació d'ordinadors. Per aquest motiu se'l coneix com un dels pares de la ciència de la computació i precursor de la informàtica moderna.

4.9 La barrera de les llengües

Mentre els criptògrafs britànics destruïen el xifrat d'Enigma i alteraven el curs de la guerra a Europa, els criptògrafs americans aconseguien una importància similar als anglesos en els afers al Pacífic, desxifrant els varis mètodes japonesos com "Purple". Per exemple, al juny del 1942 els americans desxifraren un missatge on s'informava que enviarien un missatge fals, per a que la flota americana deixés sense defensa Midway, i

a continuació l'atacarien. De manera que la flota va sortir de Midway, però mai s'allunyà massa, per això quan els japonesos enviaren el missatge per atacar Midway, la flota dels Estats Units d'Amèrica va tenir temps a defensar i derrotar-los. Aquesta batalla és una de les més importants del Pacífic, i es considera una victòria gràcies a la intel·ligència.

Les forces americanes, per protegir les seves comunicacions, usaven màquines mecàniques, com el xifrat d'Enigma, amb la diferència que aquests no es van desxifrar, tot i que durant la campanya del Pacífic, els comandants americans s'adonaren que aquests xifrats tenien una gran desavantatge. Encara que l'encriptació electromecànica oferia un nivell de seguretat major, era un procés massa lent. Els missatges s'havien de teclejar lletra per lletra, i s'havien de copiar les lletres xifrades una per una. I el missatge codificat havia de ser transmès via ràdio. L'operador que el rebia passava la informació a un expert en xifratges que seleccionava la clau i teclejava el text xifrat lletra per lletra i n'anotava el text en clar mica en mica.

El temps que es necessitava per aquesta delicada operació era possible en les seus o en els vaixells, però no en el camp de batalla, on es necessitava tenir informació precisa i ràpida. A més a més, molts dels soldats japonesos sabien anglès i havien assistit a universitats nord-americanes, fet que els proporcionava entendre estratègies i tàctiques americanes, les quals estaven caient a mans enemigues i eren emprades en contra d'ells.

Un dels primers en afrontar el problema fou Philip Johnston, un enginyer de Los Angeles, qui era massa gran per a lluitar, però que volia contribuir en la guerra. A principis de 1942 començà a formular un sistema d'encriptació inspirat en experiències d'infantesa. Johnston va créixer a Navajo, reserves d'Arizona, i com a resultat, estava completament informat sobre la cultura navaja. Ell era una de les poques persones fora la tribu que podien parlar el seu idioma amb fluïdesa, que li permeté fer de traductor entre els navajos i els agents del govern. Amb l'edat de nou anys va fer de traductor entre dos navajos que es queixaven al president Roosevelt de la por que tenia la seva tribu per culpa de la comunitat nord-americana. Aquest fet feu veure a Johnston com era d'impenetrable aquest idioma per aquells que no eren de la tribu, o aquells que havien viscut amb la seva cultura. Per tant el navajo era com un codi indesxifrable. Si cada batalló del Pacífic disposava d'un parell d'americans natius com a operadors de ràdio, la comunicació segura seria garantida. Aquesta comunicació seria molt més simple que una encriptació mecànica, i més difícil de desxifrar.

Aportà aquesta idea al tinent coronel James E. Jones, l'oficial de comunicacions al Camp Elliott, a les afores de San Diego. La idea no va trigar en ser provada amb dos natius, els quals estaven aïllats, i van fer proves amb missatges típics. Els navajos traduïen el missatge i el comunicaven via ràdio, l'altre el traduïa a l'anglès i després es comparaven els missatges originals amb els obtinguts. El projecte va ser un èxit, tant per l'eficàcia, com per la rapidesa i com per la invulnerabilitat de ser desxifrats per quelcom que no conegués l'idioma.

En el moment en que els nord-americans entraren a la Segona Guerra Mundial, el navajo convivia en condicions difícils i eren tractats com a gent inferior. Però ben aviat van recolzar l'esforç de la guerra i declararen la seva lleialtat. No va ser difícil trobar numerables candidats per servir com a codificadors. Amb quatre mesos, després de Pearl Harbor, vint-i-nou navajos, alguns de quinze anys, començaren un curs de comunicació de vuit setmanes al cos de Marines.

Abans que l'entrenament pogués començar, els Marines havien de superar un problema amb la llengua nativa. Tal i com passà durant la Primera Guerra Mundial, el capità E. W. Horner de la Companyia D, Infanteria 141, ordenà que vuit natius del nord-est de França, de la tribu de Choctaw, foren operadors de ràdio. Naturalment, cap enemic entenia l'idioma, per això asseguraven una comunicació segura. Tot i això, l'encriptació era feble pel fet que no tenien el vocabulari per a l'argot militar. Un terme específic, per tant, s'havia de traduir en una vulgar expressió inventada, amb el risc de poder ser mal interpretada pel receptor.

El mateix problema hagués afectat a l'idioma navajo, però els Marines ho tingueren en consideració, i crearen una equivalència en els termes de l'idioma, per a tal de no patir malentesos. Usaven paraules natives per a referir-se a termes militars. En són exemples les paraules: ocell, emprat per significar avió; o peix, per a referir-se a vaixells. De manera que la paraula mussol (**Da-he-tih-hi**) era un avió de combat; granota (**Chal**), significava un vehicle amfibi, capaç d'anar per terra i aigua; o la paraula peix de metall (**Besh-lo**) representava un submarí. Per a altres termes militars s'inventaven les paraules, per exemple els morters eren coneguts com a " *guns that squat* ", traduït en català com a " pistoles que ocupen, envaeixen ", com es veu no té massa sentit lògic.

Aquesta petita mostra és només un petit exemple de les 274 paraules, per això s'intentà reduir el nombre de mots equivalents, que s'unien a l'aprenentatge dels noms de gent i de llocs. La solució la van trobar separant l'alfabet fonèticament per a paraules

difícils, no comuns en navajo. Per exemple, la paraula Pacífic es lletreja, en anglès, com a "pig, ant, cat, ice, fox, ice, cat", que al navajo es traduïa com a **bi-sodih, wol·la-chee, moasi, tkin, moasi**. Tot l'alfabet navajo s'exposa a continuació:

A	Ant	**Wol-la-chee**	**N**	Nut	**Nesh-chee**
B	Bear	**Shush**	**O**	Owl	**Ne-as-jah**
C	Cat	**Moasi**	**P**	Pig	**Bi-sodih**
D	Deer	**Be**	**Q**	Quiver	**Ca-yeilth**
E	Elk	**Dzeh**	**R**	Rabbit	**Gah**
F	Fox	**Ma-e**	**S**	Sheep	**Dibeh**
G	Goat	**Klizzie**	**T**	Turkey	**Than-zie**
H	Horse	**Lin**	**U**	Ute	**No-da-ih**
I	Ice	**Tkin**	**V**	Victor	**A-keh-di-glini**
J	Jackass	**Tkele-cho-gi**	**W**	Weasel	**Gloe-ih**
K	Kid	**Klizzie-yazzi**	**X**	Cross	**Al-an-as-dzoh**
L	Lamb	**Dibeh-yazzi**	**Y**	Yucca	**Tsah-as-zih**
M	Mouse	**Na-as-tso-si**	**Z**	Zinc	**Besh-do-gliz**

Taula 13: Alfabet navajo.

Amb vuit setmanes els navajo aprenien els mots equivalents i tot aquest lèxic, això prevenia l'ús de manuals de xifratge, que podrien caure en mans enemigues. El navajo originalment era una llengua oral que no s'escrivia, per tant no tenien símbol per a cap so. Per això, tot es trobava en la ment, ja que no en podien deixar registre escrit.

Al final del seu entrenament s'examinaven. Aquests consistien en missatges en anglès que havien de traduir al seu idioma, després havien de fer el procés contrari amb altres missatges, és clar, que els missatges es transmetien via oral. Els resultats finals eren perfectes. Per comprovar la seguretat de la transmissió, facilitaren a la intel·ligència militar, la qual havia trencat Purple, el sistema criptogràfic més segur emprat pels japonesos. Després de tres setmanes de dur treball, no havien aconseguit avançar res de res. Van nombrar a l'idioma navajo com a " weird succession of guttural, nasal, tongue-twisting sounds... we couldn't even transcribe it, much less crack it." El que van dir els criptògrafs va ser una descripció del navajo, entès com una successió de sons estranys, guturals, nasals, un embarbussament... no el van poder ni transcriure, encara menys el van poder desxifrar. Per tant, va ser un èxit teòric, ara calia posar-lo a

la pràctica. Dos soldats navajos, John Benally i Johny Manuelito, es quedaren a la base per a ensenyar a la futura remesa de soldats, mentre als altres vint-i-set navajos els assignaren a quatre regiments i foren enviats al Pacífic.

Les forces japoneses van atacar Pearl Harbor el 7 de desembre del 1941, i dominaven grans parts d'est a oest del Pacífic. Les tropes japoneses van envair Guam, una de les cadenes de Solomon, Hong Kong i les Filipines, totes aquestes victòries van tenir lloc en menys d'un mes. Per a consolidar el seu control al Pacífic construïren un aeròdrom a Guadalcanal, des d'on els bombarders podrien enlairar per a destruir les línies de subministrament americà, de manera que qualsevol contraatac aliat fos quasi impossible. Per sort pels nord-americans, l'almirall Ernest King, el cap d'operacions navals, instà un atac a l'illa abans que l'aeròdrom fos operatiu. El 7 d'agost la primera divisió de marines va encapçalar una invasió del Guadalcanal. La primera partida incloïa un grup de navajos.

Encara que els navajos estaven convençuts que les seves habilitats serien una benedicció per la Marina, els primers intents només generaren gran confusió. Molts dels operadors de comunicacions regulars, que desconeixien el nou codi, enviaren missatges de pànic per a tota l'illa, afirmant que els japonesos estaven emetent freqüències en americà. El coronel en càrrec aturà immediatament les comunicacions amb navajo mentre es pogués convèncer que el sistema valia la pena.

Els navajo no trigaren a demostrar el que valien en el camp de batalla. Era la única comunicació totalment segura que podien rebre els soldats nord-americans, ja que no podien procedir de ningú més apart d'ells mateixos. Aquest aspecte s'exemplificà en un episodi a la península hispànica, on un batalló de marines va ser bombardejat pels mateixos estatunidencs. El batalló comunicà ràpidament la seva posició en anglès, però els bombarders pensaren que eren els enemics japonesos que els volien enganyar. No va ser fins que des del batalló s'envià un missatge en navajo que el bombardeig no va aturar-se.

La reputació dels navajo es va incrementar ràpidament, i cap a finals de 1942 hi havia una llista de vuitanta-tres voluntaris per a actuar com operadors de ràdio usant el codi navajo. Aquests soldats servien a les sis divisions de la Marina, i de vegades eren menyspreats per la resta de soldats. La seva guerra en la comunicació els acabà convertint en herois de guerra. Fins al punt que els altres soldats portaven les ràdios i els seus rifles, i se'ls assignaven guardaespatlles, per a protegir-los, en part també, dels seus propis camarades. En almenys tres ocasions els navajo havien estat confosos per soldats

japonesos i eren arrestats pels propis nord-americans. Se n'adonaven només quan algun company del batalló posava la mà al foc pel soldat pres.

Il·lustració 9: Dos parlants en codi navajo durant la batalla de Bougainville de 1943

La invulnerabilitat del navajo es devia al fet que pertany a un grup de llengües coneguda com a *na-dené*. Aquest grup el formen un conjunt de llengües nord-americanes caracteritzades per ser tonals, en són exemples l'apatxe, el navajo o l'ataspà. Una altra característica vital és que no té cap semblança entre cap llengua asiàtica o europea. A més a més, en navajo els verbs es conjuguen segons el subjecte i l'objecte, per tant el sufix dels verbs depenen de la categoria gramatical de l'objecte. El verb també incorpora el significat d'un adverbi, i reflecteix si el que comunica l'emissor ho ha viscut en primera persona o li han dit. Per tant, un sol verb pot equivaler a una oració sencera, fent impossible pels desentesos de la llengua a interpretar el seu significat.

El destí dels navajo va ser el mateix que el dels criptoanalistes britànics, que van haver de mantenir el secret de la seva participació. No va ser fins el 1982, quan van ser homenatjats, tenint el seu propi dia, el 14 d'agost, National Navajo Code Talkers Day, el dia dels codificadors orals navajo. Tot i això, el major mèrit que poden rebre és el fet que el seu xifrat és un dels que mai s'ha trencat. Fins i tot el cap d'intel·ligència japonesa, el general Seizo Arisue, acceptà que tot i haver trencat el xifratge de les forces aèries nord-americanes, van fracassar completament al fer el més mínim progrés per trencar el navajo.

5 LA CRIPTOGRAFIA MODERNA

Durant la Segona Guerra Mundial, els criptoanalistes britànics van superar els criptògrafs alemanys, principalment perquè la gent de Bletchley Park, seguint els passos dels polonesos, desenvoluparen algunes de les primeres tecnologies de desxifratge. A més a més de les bombes de Turing, que es van fer servir per trencar Enigma, els britànics també inventaren un altre aparell per desxifrar missatges, Colossus, per combatre una forma d'encriptació més forta, el codi alemany Lorenz. De les dues màquines, va ser Colossus la que va determinar el desenvolupament de la criptografia durant la segona meitat del segle XX.

El codi Lorenz es va fer servir per comunicacions d'alta importància i per a als càrrecs militars, mentre Enigma era per les tropes de combat. L'encriptació es feia en màquines Lorenz SZ40 o les SZ42, que funcionaven d'una manera similar a Enigma, amb rotors, però de manera més sofisticada, el qual proporcionà a Bletchley Park un major repte. Tot i això, dos criptoanalistes, John Tiltman i Bill Tutte, descobriren un punt feble en el xifratge de Lorenz.

Per a poder trencar el codi Lorenz, primer calia construir una màquina SZ40 o SZ42 per a poder saber-ne el funcionament. No va ser fins el 30 d'agost del 1941, quan s'envià un missatge de 4000 paraules codificat, però aquest no es va rebre correctament, i els receptors van sol·licitar una retransmissió del missatge, però de l'original. El missatge va ser enviat en configuració de clau HQIBPEXEZMUG, i el segon cop que l'envià modificaren el text mínimament, fent petites alteracions. A partir dels dos texts xifrats Tiltman va poder recuperar els dos missatges originals i el codi de xifratge. A partir d'aquest codi la màquina va ser reconstruïda completament per Tutte.

Ara només faltava trencar el codi Lorenz, i no era una tasca fàcil, ja que requeria una barreja de buscar, lligar, analitzar estadísticament i un judici exhaustiu, tot el que va fer possible la fabricació de les bombes. Aquestes últimes eren capaces de fer una feina molt específica amb gran rapidesa, però no eren prou flexibles per operar la subtilesa de Lorenz. En un inici es tenien que desxifrar els missatges xifrats amb el codi Lorenz a mà, i això implicava un temps d'unes dues setmanes, temps en el que el missatge estava fora de data, és a dir, que ja no proporcionava informació essencial. Amb el temps, el matemàtic Max Newman, de Bletchley, sorgí amb la idea de mecanitzar el desxifratge de Lorenz. Inspirat en les idees de la Turing per a construir la seva màquina, Newman

dissenyà un aparell capaç de modificar-se per a resoldre varis problemes, el que coneixem avui dia com un ordinador programable.

El disseny de Newman va ser considerat tècnicament impossible de construir, i els oficials de Bletchley rebutjaren el projecte. Per sort, Tommy Flowers, un enginyer que havia pres part en les discussions sobre el disseny, decidí ignorar els oficials. Va construir la màquina a partir de les idees de Newman, i trigà deu mesos a tenir-la acabada, la màquina Colossus Mark I, la qual donà a Bletchley Park el vuit de desembre de 1943. Aquesta consistia en 1500 vàlvules electròniques, que la feien molt més ràpida que qualsevol altra màquina. Però el més important va ser el fet que era programable.

Al llarg de la guerra se'n van construir onze, però totes estaven formades per 2500 vàlvules, i es nombraren Colossus Mark II. Fins i tot la original es modificà per a convertir-se en aquest segon model, cinc vegades més ràpida que la primera.

Colossus, igual que tot el que es podia relacionar amb Bletchley Park, va ser destruït després de la guerra, i els qui havien treballat allà se'ls hi va prohibir parlar-ne. Es destruïren deu de les màquines el 1946, per ordre directa de Winston Churchill, ho va fer el mateix Tommy Flowers. L'única que sobrevisqué va ser desmantellada al 1960, quan es van cremar els plànols i els diagrames dels seus circuits. Les raons no van ser només militars, sinó que també polítiques, ja que es sap que almenys es podria haver evitat un bombardeig alemany a una ciutat anglesa gràcies a Colossus, però es va deixar actuar per protegir un dels secrets més ben guardats de la Segona Guerra Mundial.

Al 1945 John Presper Eckert i John William Mauchly, desenvoluparen ENIAC (Electronical Numerical Integrator And Computer), un computador i integrador numèric electrònic. Aquesta contenia quasi divuit-mil vàlvules, capaces de computar cinc-mil operacions per segon. Durant dècades s'ha cregut que era la mare de tots els ordinadors, enlloc de Colossus.

Al final de la guerra i amb el naixement dels computadors moderns, els criptoanalistes es centraren en desenvolupar tecnologia computacional enlloc de trencar tots els tipus de xifrats. Ara podien treballar amb una alta velocitat i flexibilitat gràcies als computadors programables. Els criptògrafs també començaren a treballar amb les noves tecnologies per a crear un xifrat més potent i segur. En poc temps les computadores jugaren un rol que definiria la lluita entre criptògrafs i criptoanalistes.

Usar la computació per encriptar missatges és molt similar a les formes tradicionals. Tot i que hi ha tres diferències bàsiques entre l'ús de l'electrònica i la mecanització en que es basava Enigma. La primera diferència és que la màquina de

xifratge mecànica presenta una limitació pel que respecta al que podem construir, mentre una computadora pot imitar una hipotètica màquina de xifratge immensament complexa. Per exemple, una computadora pot programar-se per imitar l'acció de cents de rotors, uns rotant en sentit horari, altres en sentit antihorari, uns rotant més ràpid i altres més lents, fet que proporciona una encriptació molt més segura. Una màquina mecànica com aquesta seria pràcticament impossible de construir, però virtualment es pot, i això proporciona un major nivell de seguretat dels xifrats.

La segona diferència es una simple qüestió de velocitat. Els circuits electrònics poden operar molt més ràpid que els rotors mecànics. Un ordinador programat per imitar el xifrat d'Enigma podria encriptar un llarg missatge en un instant. Altrament, un ordinador programat per a dur a terme una encriptació molt més complexa trigaria un temps raonable.

La tercera, i possiblement la més significativa diferència, és que un ordinador treballa en números enlloc de lletres. Només treballen amb nombres binaris – seqüències de 0 i 1, coneguts com bits (de l'anglès *binary digit*). Abans d'encriptar qualsevol missatge cal convertir-lo en dígits binaris. Aquest pas es pot produir seguint varis protocols, com l'ASCII, l'acrònim d'American Standart Code for Information Interchange, conegut en català com <<codi estàndard nord-americà per a l'intercanvi d'informació>>. ASCII assigna set dígits binaris a cada lletra de l'alfabet, igual que feu Morse amb punts i barres. Hi ha 128 (2 elevat a 7) combinacions dels set dígits, per tant pot definir 128 caràcters diferents. També existeixen codis ASCII estesos de 8 bits cada caràcter, i serveixen per a representar símbols addicionals com pot ser la <<ç>> del català. Inicialment ASCII utilitzava 7 bits per representar els caràcters i afegia un bit addicional, de paritat, que servia per detectar errors en les transmissions.

En els 128 caràcters anglesos trobem l'alfabet en majúscules i minúscules i tots els signes de puntuació, com es veu en la següent taula. També defineix els codis per a 33 caràcters no imprimibles, els quals eren de control, com per exemple el 127 que servia per cancel·lar alguna transmissió.

Per a possibilitar la comunicació, cal abans de tot convertir el missatge en una seqüència de dígits binaris. Un cop s'ha convertit el missatge en seqüències de zeros i uns, ja pot iniciar-se l'encriptació. Encara que al treballar amb ordinadors i números, i no amb màquines que emprin lletres, la codificació procedeix com es feia tradicionalment.

Per exemple, imaginem que volem encriptar el missatge **Hola** usant una simple versió de substitució. Primer de tot caldrà passar el text al llenguatge ASCII, com indica la taula inferior:

Taula ASCII per a tots els caràcters anglesos imprimibles								
Binari	Dec	Caràcter	Binari	Dec	Caràcter	Binari	Dec	Caràcter
00100000	32	espai ( )	0100 0000	64	@	0110 0000	96	`
00100001	33	!	0100 0001	65	A	0110 0001	97	a
00100010	34	“	0100 0010	66	B	0110 0010	98	b
00100011	35	#	0100 0011	67	C	0110 0011	99	c
00100100	36	$	0100 0100	68	D	0110 0100	100	d
00100101	37	%	0100 0101	69	E	0110 0101	101	e
00100110	38	&	0100 0110	70	F	0110 0110	102	f
00100111	39	‘	0100 0111	71	G	0110 0111	103	g
00101000	40	(	0100 1000	72	H	0110 1000	104	h
00101001	41	)	0100 1001	73	I	0110 1001	105	i
00101010	42	*	0100 1010	74	J	0110 1010	106	j
00101011	43	+	0100 1011	75	K	0110 1011	107	k
00101100	44	,	0100 1100	76	L	0110 1100	108	l
00101101	45	-	0100 1101	77	M	0110 1101	109	m
00101110	46	.	0100 1110	78	N	0110 1110	110	n
00101111	47	/	0100 1111	79	O	0110 1111	111	o
00110000	48	0	0101 0000	80	P	0111 0000	112	p
00110001	49	1	0101 0001	81	Q	0111 0001	113	q
00110010	50	2	0101 0010	82	R	0111 0010	114	r
00110011	51	3	0101 0011	83	S	0111 0011	115	s
00110100	52	4	0101 0100	84	T	0111 0100	116	t
00110101	53	5	0101 0101	85	U	0111 0101	117	u
00110110	54	6	0101 0110	86	V	0111 0110	118	v
00110111	55	7	0101 0111	87	W	0111 0111	119	w
00111000	56	8	0101 1000	88	X	0111 1000	120	x
00111001	57	9	0101 1001	89	Y	0111 1001	121	y
00111010	58	:	0101 1010	90	Z	0111 1010	122	z
00111011	59	;	0101 1011	91	[	0111 1011	123	{
00111100	60	<	0101 1100	92	\	0111 1100	124	|
00111101	61	=	0101 1101	93	]	0111 1101	125	}
00111110	62	>	0101 1110	94	^	0111 1110	126	~
00111111	63	?	0101 1111	95	_			

Taula 14: Taula ASCII per a tots els caràcters anglesos imprimibles.

Com és evident, per a dur a terme un xifrat per substitució, es necessita una clau, com pot ser **Juan**, que també s’haurà d’escriure en llenguatge ASCII. Les dues seqüències numerals es comparen, de manera que si els dos nombres són els mateixos,

el text xifrat serà un 0, i si són diferents un 1. A continuació es mostra l'exemple exposat:

Missatge	**Hola**
Missatge en ASCII	**01001000011011110110110001100001**
Clau = **Juan**	**01001010011101010110000101101110**
Text xifrat	**00000010000110100000110100001111**

El resultat final és una simple cadena de trenta-dos dígits binaris que es poden enviar al receptor, qui farà servir la mateixa clau per desxifrar el missatge, i interpretar el missatge via ASCII per regenerar el missatge **Hola**.

Els que tenien a l'abast aquesta tecnologia, en un principi, només eren els militars i els governs. Tot i que més tard alguns científics, enginyers principalment, van construir ordinadors. No va ser fins el 1953 que IBM va treure a la venda el primer ordinador, i quatre anys més tard s'introduí Fortran, un llenguatge de programació amb el qual qualsevol podia escriure programes informàtics. Després, en el 1959 s'inventà el circuit integrat, que significà una nova era de la informàtica.

Durant els anys 60 els ordinadors eren més potents que anteriorment, i al mateix temps més econòmics. Les empreses creixeren gràcies a les noves tecnologies, i es feien servir per encriptar missatges amb informació confidencial, com podien ser transferències bancàries o negociacions delicades. A mesura que les empreses usaven més els ordinadors, i la codificació de les comunicacions en el món del negoci augmentava, els criptògrafs s'enfrontaven amb un gran problema conegut com la distribució de la clau.

Imaginem que un banc vol enviar informació privada a un client. Via telèfon no pot fer-ho ja que corre el risc que algú hagi manipulat la línia telefònica. Una altre manera és enviar un missatge, però el problema d'ésser interceptat perdura. La solució era encriptar el missatge i després enviar-lo al client, però el receptor havia de posseir un ordinador, tenir el mateix programa informàtic i, a més a més, tenir coneixement de la clau. El principal problema va ser com enviar la clau al client?

En la dècada del 1970 alguns bancs distribuïren les claus per mitja d'empleats d'alta confiança, els quals eren investigats prèviament. Aquests recorrien el món donant les claus personalment, i aquestes claus eren vàlides durant una setmana. El mètode

suposava un gran mal de cap a mesura que el negoci creixia, principalment per l'enorme despesa econòmica.

El problema de la distribució de la clau ha estat un dels grans problemes de la història. Per exemple, durant la Segona Guerra Mundial els alemanys distribuïen mensualment un manual amb les claus d'Enigma que farien servir cada dia, això suposava un gran problema que comprometia la seguretat de les comunicacions. El mateix problema suposava el xifratge de Vigenère, el problema de la distribució de la clau era un malson pels criptògrafs, ja que no importava quan segur pogués ser un xifratge si la clau no es podia compartir de manera igual de segura.

La solució al problema de la distribució de la clau no va arribar fins a meitats dels 70s. Una brillant solució basada en un sistema d'encriptació que combatia contra la lògica, ja que la transmissió de la clau és en si un missatge que s'ha d'encriptar i s'ha de compartir prèviament al missatge xifrat.

Aquesta innovació va ser la major revolució en el camp de la criptografia del segle XX. De fet, l'assoliment és considerat el major èxit criptogràfic des de la invenció del xifrat monoalfabètic, més de dos mil anys abans.

5.1 La criptografia de clau pública

Whitfield Diffie és un dels criptògrafs més coneguts per la recerca de la solució del problema de la distribució de la clau. Estudià matemàtiques a l'institut de tecnologia de Massachusetts, i es graduà el 1965 amb vint-i-un anys. Treballà uns cinc anys en feines relacionades amb la seguretat informàtica. A principis dels 70s s'independitzà com un dels millors experts en seguretat, un criptògraf independent i lliurepensador.

Diffie estava totalment interessat en aquest problema, ja que sense un intercanvi de claus, i l'imminent ús d'internet hagués acabat amb la privacitat de la població que es volgués comunicar per la xarxa. Si als militars i al govern els suposava un greu problema, a les persones del carrer els seria impossible solucionar-lo. Per això Diffie imaginà dues persones que es coneixien via internet, i es trencà el cap pensant com podien enviar-se missatges encriptats. També considerà l'escenari en que una persona volgués comprar alguna cosa per internet, com podria aquesta enviar la informació encriptada de la targeta de crèdit per tal que el receptor fos l'únic capaç de desxifrar-la? En els dos casos es necessita compartir la clau, però com ho podien fer d'una manera

segura? Per aquest motiu Diffie s'obsessionà en trobar una solució, per a garantir la privacitat digital.

El 1974, Diffie, anà a visitar el laboratori d'IBM de Thomas J. Watson, on va ser invitat per fer una xerrada. Parlà sobre varies estratègies d'atacar el problema de la distribució de la clau, però totes les seves idees eren indefinides i provisionals, i els seus oients eren escèptics en les solucions del tema. La única resposta positiva que va rebre de la seva presentació, va ser de Alan Konheim, un dels criptògrafs experts d'IBM, qui mencionà que algú altre va fer una presentació sobre el mateix problema. Aquest era Martin Hellman, un professor de la universitat de Stanford de California. Diffie volgué conèixer la única persona a qui li obsessionava el mateix que a ell. L'aliança Diffie-Hellman esdevindria una de les parelles més innovadores en el món de la criptografia.

Hellman va néixer al 1945 en un barri del Bronx, però amb quatre anys la família es traslladà a un barri catòlic. Ell volia ser com la resta de nens del barri, tenir Nadal, i rebre regals per aquestes dates, i com a autodefensa pensà que ningú vol ser com tothom. En aquest context comença el seu interès per la criptografia, per a ser diferent. Tots els seus amics el consideraven boig per voler competir contra la NSA (Agència de Seguretat Nacional) i el seu pressupost milionari. Com podia una persona descobrir alguna cosa que ells no haguessin desenvolupat ja? Tot i això, Hellman seguí sempre endavant.

Al setembre del 1974 va rebre una trucada inesperada de Whitfield Diffie. Hellman mai havia sentit a parlar d'ell, però acceptà una cita amb ell aquell mateix dia. Al final de la trobada, Hellman s'adonà que Diffie era una de les persones més ben informades que havia conegut mai. Aquest motiu, i la semblança de les mateixes obsessions, els uní i treballaren desesperadament per a trobar una alternativa al fatigós transport físic de la clau entre grans distàncies. En aquest curs els va ajudar Ralph Merkle, un investigador que deixà el seu grup perquè no compartien el somni de resoldre el gran problema de la distribució de la clau.

Per resoldre aquest problema, imaginaren dues persones que es volguessin escriure, l'Alice i el Bob, però que una tercera persona, l'Eve, no pogués llegir els seus missatges. Per comunicar-se havien d'enviar texts xifrats, per a això era necessària una clau, i si volien compartir la clau ho havien de fer encriptant-la, de manera que no arribaven a cap conclusió viable. Una alternativa era passar la clau en privat, però calia canviar la clau per a cada missatge per a què l'Eve no pogués desxifrar tots els missatges. Per tant, la solució de compartir les claus en privat era segura, però si un dels

dos estava malalt, o no podien veure's l'un a l'altre, no podrien escriure's amb una nova clau, que feia vulnerable la comunicació. Durant més de dos mil anys havia perdurat el problema de la distribució de la clau, havia estat considerat un axioma de la criptografia. Tot i això, hi ha un escenari en el que l'axioma falla.

Imaginem que Alice i Bob viuen en un país on el sistema postal és completament immoral, i els empleats llegeixen totes les cartes no diplomàtiques. Un dia, Alice vol enviar un missatge intensament íntim a Bob. Ella posa el missatge en una caixa metàl·lica, la tanca amb un cadenat. Llavors envia la capsa, però no la clau. Tot i que, quan la caixa arriba a Bob, no és capaç d'obrir-la perquè no té la clau. Llavors Alice es veu obligada a enviar la clau en una caixa també tancada. Tornem a arribar al mateix problema, però exposat de manera diferent. En termes criptogràfics Alice ha d'encriptar el missatge de manera que Bob sigui l'únic que el pugui desxifrar, per tant li ha de donar una còpia de la clau. La distribució de la clau sembla ser inevitable, o no?

Ara imaginem la següent situació. Com abans, Alice vol enviar un missatge a Bob. Altra vegada ella posa el missatge en una caixa metàl·lica i la tanca amb cadenat. Quan Bob la rep no la pot obrir, però la tanca amb el seu propi cadenat i l'envia a Alice, de manera que la caixa està tancada per dos cadenats. Alice treu el seu amb la clau i l'envia a Bob, qui té la clau per a poder obrir la capsa i ja pot llegir el missatge.

Les conclusions d'aquesta petita història són innegables. Demostra que un missatge secret pot ser compartit de manera segura sense establir contacte directe entre emissor i receptor, sense compartir la clau. Per primera vegada en la criptografia sembla que el problema de la distribució de la clau és evitable. Criptogràficament podem interpretar la història. Alice encripta el missatge amb la seva clau i l'envia a Bob, qui l'encripta amb la seva pròpia clau i li retorna. Quan ella rep el text doblement xifrat, remou la seva encriptació i el retorna a Bob, qui el pot desxifrar i, posteriorment, llegir el missatge original.

Sembla que el problema de la distribució de la clau està resolt gràcies a la doble encriptació. No obstant això, hi ha varis obstacles per implementar un sistema on Alice encripta, Bob encripta, Alice desxifra i Bob desxifra. Un dels grans problemes és l'ordre en que es duen a terme les encriptacions i les descodificacions. En general, l'ordre en la criptografia és crucial, per tant, l'últim que ha estat encriptat ha de ser el primer en desxifrar-se. En l'escenari anterior, Bob hauria de ser el primer en descodificar amb la seva clau el missatge, i després que ho fes Alice. Desafortunadament, molts dels sistemes criptogràfics són molt més sensibles en l'ordre pel que fa als cadenats. La

importància de l'ordre resulta més entenedora amb un exemple diari. Al matí ens posem primer els mitjons i després les sabates, i a la nit ens traiem les sabates i després els mitjons, ja que seria impossible treure els segons en primer lloc. L'exemple de la caixa funciona ja que els cadenats es poden afegir i treure sense importar l'ordre.

Diffie i Hellman comprovaren que l'exemple exposat no servia en el món de la criptografia on vivim. No va ser envà, ja que els inspirà per a buscar un mètode pràctic per solucionar el problema de la distribució de claus. Després, el 1975, Diffie va tenir una idea brillant. Elaborà un nou sistema de xifratge, al qual va anomenar xifratge de clau asimètrica. Fins ara totes les tècniques d'encriptació que hem vist han sigut de clau simètrica, el que significa que el procés de descodificació és just el contrari que el de codificació. Per exemple, la màquina Enigma fa servir una clau basada en l'ordre i posició dels rotors, i el receptor havia d'emprar la mateixa clau per a desxifrar el missatge. La relació entre les claus és la mateixa, de manera que parlem de claus simètriques. En una encriptació de clau asimètrica, com el nom suggereix, la clau de xifratge i la de desxifratge no són idèntiques. En un xifrat asimètric, Alice pot encriptar el missatge si coneix la clau de codificació, però no el podrà desxifrar, però Bob, qui ha compartit la clau de codificació, serà l'únic que podrà desencriptar el missatge. Aquest nou descobriment és el que fa aquest sistema criptogràfic tan especial.

Tot i això, Diffie només tenia la idea, el concepte general d'un xifrat de clau asimètrica, encara no tenia cap exemple concret, però només el concepte ja era una idea revolucionaria. Si els criptògrafs aconseguien trobar un criptosistema que es basés amb la clau asimètrica, que complís els requeriments de Diffie, les conseqüències serien enormement útils per a la vida quotidiana, i en l'exemple exposat, per l'Alice i el Bob. Llavors tant l'Alice com el Bob crearien un parell de claus cada un, una de xifratge i una de desxifratge. Cada clau tindria un valor diferent, la d'encriptar de cada un la publicarien, és el que es coneix com a clau pública. Per altra banda mantindrien en secret la clau per desxifrar el missatge, coneguda com a clau privada. Si l'Alice volgués enviar un missatge al Bob, només tindria que localitzar la seva clau pública, encriptar el missatge segons aquesta i enviar-lo. Només faria falta que el Bob utilitzés la seva clau privada i pogués llegir el text en clar. En el cas que el Bob li volgués enviar un missatge seria el mateix, però a la inversa. De manera que qualsevol que es vulgui comunicar amb l'Alice o el Bob només ha d'encriptar el seu missatge amb la clau pública del receptor, que serà l'únic propietari de la clau privada per entendre el text.

El gran avantatge d'aquest criptosistema és la solució del problema de la distribució de la clau. A partir d'aquest moment ja no es necessitava establir contacte físic per intercanviar les claus, o manuals com feien servir els alemanys, al contrari que els xifrats simètrics tradicionals. Encara que tot el món conegués la clau pública, ningú en podria llegir el contingut d'un missatge encriptat amb aquesta, a no ser que aconseguís trencar per força bruta l'algoritme. Tot i així, a partir de la clau pública no podem desxifrar el text, només podrà la persona en possessió de la clau privada.

Tornant a recuperar l'exemple dels cadenats, les clau asimètriques funcionarien com un cadenat simple que tothom pot tancar clicant, però només aquella que té la clau el pot obrir. Per tant, tancar-lo (encriptar) és fàcil, qualsevol ho por fer, però només pot obrir-lo (desxifrar) el propietari de la clau. El coneixement de com tancar-ne un no ajuda a obrir-lo, de la mateixa manera funcionen les claus asimètriques. El Bob dissenyaria un cadenat i la seva clau. Guardaria la clau, i fabricaria milers de cadenats iguals i els distribuiria pel món. Si Alice li volgués enviar un missatge només hauria de posar-lo en una caixa, tancar-la amb el cadenat que ha distribuït el Bob, i enviar-li. El procés de tancar el cadenat amb un clic és el procés d'encriptar, disponible per a tothom. La clau del qual equival a la clau privada, ja que només la posseeix una persona, en aquest cas el Bob, l'únic capaç d'obrir el cadenat, l'únic capaç de desxifrar el missatge.

El sistema sembla fàcil a nivell teòric i exemplificat amb cadenats, però es trobava lluny de la funció matemàtica que possibilités el sistema criptogràfic. Per a tal de convertir la idea del xifrat asimètric en una invenció pràctica, calia primer descobrir una funció matemàtica que actués com el cadenat, és a dir, irreversible. Una funció és qualsevol operació que converteix un número en un altre. Per exemple, triplicar és un tipus de funció, perquè transforma el nombre 2 al 6 o el nombre 10 al 30. Encara més, podem pensar en totes les formes d'encriptació computacional com a funcions, ja que canvien un valor (el text en clar), en un altre valor (el text xifrat).

Moltes de les funcions que coneixem són bidireccionals, el qual significa que són fàcils de desenvolupar i recuperar el valor inicial a partir del resultat. Per exemple, triplicar un nombre és una funció bidireccional, anomenada en matemàtiques bijectiva, perquè és fàcil trobar-ne la imatge i l'antimatge. Per exemple, triplicar un nombre és una funció bijectiva perquè és fàcil triplicar un nombre i del resultat obtenir el nombre original. Si coneixem que el valor triplicat és 27, fent la inversa de la funció es pot deduir el nombre original, 9. També es pot entendre com un acte quotidià. Una funció

bijectiva funciona com un interruptor d'una bombeta, ja que si trobem la bombeta encesa només hem d'apagar-la per trobar l'estat original de l'interruptor.

Altrament, Diffie i Hellman, no estaven interessats en una funció bidireccional, sinó les funcions irreversibles, unidireccionals. Com el nom suggereix, una funció d'aquest tipus, és fàcil de desenvolupar, però molt complicat fer la inversa. Aquestes funcions, en termes matemàtics s'anomenen no invertibles. En altres paraules, les funcions bijectives són reversibles. Per explicar la funció invertible podem imaginar un ou com la nostre funció, i en trencar-lo estem desenvolupant la funció, però a partir de l'ou trencat és quasi impossible retornar l'ou en el seu estat original.

L'exemple dels cadenats és també una mostra de funció irreversible, atès que és fàcil tancar-lo, però difícil d'obrir. La idea de Diffie es basava en un cadenat matemàtic, i és en aquest context que l'equip de Standford de Diffie, Hellman i Merkle fixaren la seva atenció en estudiar les funcions irreversibles.

L'aritmètica modular és una branca de les matemàtiques basada en aquest tipus de funcions, és un conjunt de mètodes que permeten la resolució de problemes sobre nombres enters. Estan basats en els residus de les divisions, ja que les solucions són aquestes, i no el quocient. Per exemple, el mòdul de 5 només té 5 solucions possibles, els nombres del 0 al 4. Per tant si hem d'operar un nombre en mòdul de 5 es mostrarà el següent:

$$3 + 6 = 4 \text{ (mòd. 5)} \quad , \quad 6 + 5 = 1 \text{ (mòd. 5)} \quad \text{i} \quad 4 + 1 = 0 \text{ (mòd. 5)}$$

El resultat prové del residu de la divisió del nombre de l'esquerra entre 5, el mòdul. L'aritmètica modular és relativament senzilla, i en canvi la trobem a diari, com en el temps. Si són les deu i hem quedat amb els amics quatre hores després, ens trobarem a les dues, i no a les catorze. Hem calculat mentalment:

$$10 + 4 = 2 \text{ (mòd. 12)}$$

Però calcular mentalment una divisió de grans nombres resulta de gran complexitat, per això si volem trobar el resultat de 23 x 5 en el mòdul de 17, faríem les següents operacions:

$$23 \times 5 = 115$$

$$115 / 17 = 6, \text{ i el residu és } 13$$

$$23 \times 5 = 13 \text{ (mòd. 17)}$$

Les funcions en aritmètica modular tendeixen a comportar-se de manera irregular, erràtica, el que les fa majoritàriament funcions unidireccionals. Això es mostra clarament quan comparem una funció com les que coneixem amb una funció en aritmètica modular. En les funcions bidireccionals és fàcil fer la inversa, en canvi en les altres és més complicat. Com a exemple imaginem la funció 4^x, i agafem un valor x, i multipliquem 4 per ell mateix x vegades per aconseguir el nombre resultant. Per exemple, si x = 3 i substituïm a la funció:

$$4^3 = 4 \times 4 \times 4 = 64$$

En altres paraules, la funció transforma el 3 en 64, i a mesura que creix la x, també ho farà el seu resultat. Per això si ens donen el resultat d'aquesta funció seria relativament senzill treballar a la inversa per deduir el nombre original. Per exemple, si el resultat és 1024, podem suposar que el resultat és x = 6, i calcularíem $4^6 = 4096$. el resultat és massa gran, però tot i haver-nos equivocat en la resposta, el resultat erroni ens proporciona la informació que el valor de x és massa gran. Per tant podem suposar que x = 5, i si fem el càlcul: $4^5 = 1024$. En conclusió, cada vegada que suposem un valor per a x ens trobarem més proper de la resposta, i serà més fàcil deduir-la.

Tot i així, en aritmètica modular, la mateixa funció es torna més irregular. Imaginem que tenim la funció 4^x en mòdul de 13, i el seu resultat és 1, i ens demanen obtenir el valor de x. No ens ve en ment ja que no estem acostumats a l'aritmètica modular. Podríem suposar que x = 4, i treballaríem per trobar el resultat de 4^4 (mòd. 13). La solució és 10, el qual és massa gran, ja que busquem una solució que sigui 1. El que suposaríem a continuació seria reduir el valor de x. Però, com veiem en la taula següent la solució no es troba en valors menors, sinó majors, ja que la solució a aquest és x = 6.

x	1	2	3	4	5	6
4^x	4	16	64	256	1024	4096
4^x (mòd. 13)	4	3	12	9	10	1

Taula 15: Taula de valors.

De manera que hem demostrat que en aritmètica modular qualsevol resposta equívoca no ens acosta, ni ens dóna informació, sobre la solució de la funció inversa. L'únic mètode per a obtenir un resultat de la inversa d'una funció en aritmètica modular, és construir una taula donant valors a x, fins a obtenir el resultat que esperem, tal i com hem fet anteriorment. Tot i que en l'exemple exposat hem treballat amb nombres relativament petits, per això la labor era simple, si treballéssim amb nombres més grans, dissenyar una taula de valors ens ocuparia molt temps, hores i hores d'intents sense arribar a obtenir cap conclusió clara.

A continuació, ara que ja tenien la idea, només calia posar-ho a la pràctica. Així que suposaren que l'Alice i el Bob es volen comunicar de manera segura sense que una tercera persona, l'Eve, pugui interceptar els missatges. La idea era la següent:

1-. L'Alice escull un nombre qualsevol que manté secret, i l'anomenarem a.

2-. El Bob fa el mateix, amb un altre número al qual ens referirem com a b.

3-. Tot seguit, els dos, apliquen els seus respectius números a una funció del tipus: $f(x) = g^x$(mòd. P), sent p un nombre primer conegut.

Tant l'Alice com el Bob obtindran un nou número de l'operació, el qual s'enviaran entre ells. Ella obtindrà el nombre a_1 i ell el b_1, els quals seran coneguts per ambdós.

4-. L'Alice resol l'equació del tipus $(g^b[\text{mòd.p}])^a$(mòd.p), que equival a $b_1{}^a$(mòd.p), i obté un nombre c.

5-. En Bob calcula el valor obtingut de $(g^a[\text{mòd.p}])^b$(mòd.p), que equival a $a_1{}^b$(mòd.p), que serà c, el mateix resultat que l'Alice, i la clau del sistema.

L'única comunicació que hi ha hagut és l'acord en la funció i en el moment de comunicar-se a_1 i b_1. Per tant, la clau general del sistema serà:

$$g^{a*b} \text{ en mòdul p}$$

Per a entendre de manera més visual com funciona n'exposarem un exemple en concret:

1. L'Alice i el Bob escullen un nombre primer p i una base g. En el nostre exemple p = 11 i g = 7.

2. L'Alice escull un nombre secret, a =3.

3. Envia a en Bob el valor $g^a[\text{mòd.p}] = 7^3[11] = 2$.

4. El Bob escull un nombre secret, b =6.

5. Li envia a l'Alice el valor $g^b[\text{mòd.p}] = 7^6[11] = 4$.

6. Ara ella pot obtenir la clau secreta: $(g^b[\text{mòd.p}])^a[\text{mòd.p}] = 4^3[11] = 9$.

7. Ell fa el mateix i calcula la mateixa clau que ha obtingut l'Alice: $(g^a[\text{mòd.p}])^b[\text{mòd.p}] = 2^6[11] = 9$.

8. El valor 9 serà la clau del sistema, ja que ells dos són els únics que el posseeixen.

Ara suposem que l'Eve coneix tant la funció com els nombres que s'envien els dos. El problema serà resoldre l'equivalència $7^a = 2$ i $7^b = 4$ en mòdul 11, sent a i b els nombres secrets i arbitraris escollits per l'Alice i el Bob. En el cas que aconsegueixi trobar els dos valors serà capaç de resoldre g^{a*b} en mòdul p. La solució a aquest problema s'anomena en matemàtiques un logaritme discret. Per exemple en el cas

$$f(x) = 4^x \text{ [mòd. 13]}$$

s'observa que $4^x = 12$ [mòd. 13] i, provant diferents valors, trobem que la solució és $x = 3$.

En l'exemple exposat es diu que 3 és el logaritme discret de 12 en base 4 amb mòdul 13.

Com s'ha esmentat amb anterioritat, el que fa aquest sistema criptogràfic tan particular, és el fet de treballar amb clau asimètriques, i que són difícilment reversibles. Per a valors més p amb més de 300 xifres, i valors d'a amb més de 100, la ruptura de la clau es torna exageradament complicada.

L'algoritme Diffie-Hellman, exposat a les pàgines anteriors, demostrà teòricament la possibilitat de crear un sistema criptogràfic asimètric en el qual no caldria un intercanvi de claus. No obstant això, necessitava una comunicació pública en el procés de generar la clau.

Dit d'una altra manera, s'havia demostrat que per establir una comunicació entre emissor i receptor ja no calia una cita prèvia, i física, per establir la clau. Tot i això quedaven certs aspectes per resoldre, ja que si l'Alice li volgués enviar un missatge al Bob mentre aquest dormís o estigués ocupat, hauria d'esperar per poder compartir la informació per generar la clau.

No obstant, aquesta funció asimètrica no és adequada per actuar com un cadenat matemàtic, ja que es necessiten un tipus especial de funcions no invertibles. És fàcil tancar el cadenat, però realment complicat poder-lo obrir..., a no ser, com és evident, que es posseeixi la clau. La clau és allò què fa que el cadenat sigui tan especial. Per tant, la veritable funció matemàtica és aquella fàcil de desenvolupar, però generalment difícil de fer en sentit oposat, a menys que es tingui una informació concreta, anomenada clau.

L'equip de Diffie, Hellman i Merkle estaven fent més fort el món criptogràfic. Havien demostrat que la solució al problema de la distribució de la clau era possible, i es trobava en l'horitzó. Havien proposat el concepte de xifrat asimètric, un perfecte però encara incompatible sistema. Continuaren les investigacions a la universitat de Standford, lluitant intel·lectualment per trobar una funció no invertible que fes possible, real, el xifrat asimètric. Tot i que fallaren en el descobriment d'aquest, el teoritzaren. Com en l'exemple dels cadenats, una mateixa persona havia de posseir una clau per encriptar, pública, i una de diferent per desxifrar, privada, i que les dues fossin dependents només del receptor, i no del receptor i l'emissor.

5.2 Els nombres primers

A l'agost del 1977 un divulgador científic estatunidenc, Martin Gardner, publicà en la seva columna de recreacions matemàtiques de la revista *Scientific American* un article titulat << Un nou tipus de xifrat que costaria milions d'anys desxifrar>>. Després d'explicar els fonaments del sistema de claus pública, afegí un missatge xifrat amb la clau pública següent:

N = 114.381.625.757.888.867.669.235.779.976.146.612.010.218.296.721.242.362.562.
561.842.935.706.935.245.733.897.830.597.123.563.958.705.058.989.075.147.599.290.
026.879.543.541

Gardner plantejà als seus lectors el repte de desxifrar un missatge a partir de la informació donada, i donà la pista que la solució necessitava factoritzar N en els seus components primers p i q, i el primer capaç d'aconseguir la solució rebria un premi de 100 dòlars. Tot aquell que estigués interessat en la labor podia enviar una petició al Laboratori d'Informàtica del MIT, on treballaven els seus creadors; Ron Rivest, Adi Shamir i Len Adelman.

Van rebre més de tres mil peticions, tot i que la solució no es va rebre fins disset anys més tard, el temps que trigaren en trencar el xifrat. El dia 26 d'abril, un equip de sis-centes persones anunciaren els factors de N:

q = 3.490.529.510.847.650.949.147.849.619.903.898.133.417.764.638.493.387.843.
990.820.577
p = 32.769.132.993.266.709.549.961.988.190.834.461.413.177.642.967.992.942.539.
798.288.533

Fent servir aquests valors com a clau privada van ser capaços de desxifrar el missatge. Aquest era una successió de nombres, però al convertir-se en lletres, es llegia: <<*The magic words are squeamish ossifrage.*>> (<<les paraules màgiques són un sensible trencalòs>>). Algú podria pensar que es trigà un temps relativament curt tenint en compte els nous avenços en tecnologia, tot i que Gardner feu servir una clau pública relativament petita, de l'ordre de 10^{129} xifres. Avui en dia, els usuaris de RSA trien nombres molt més llargs.

Els tres Adleman, Rivest i Shamir s'uniren per a resoldre el problema de Diffie i Hellman, però no per interessos criptogràfics, sinó per afecte a les matemàtiques. El trio

formava un equip perfecte. Rivest és un científic computacional amb una increïble habilitat per incorporar idees noves i aplicar-les on calgués. Sempre estava al dia de les notícies científiques, el que l'inspirà a buscar candidats per a la funció de trobar un xifrat asimètric. Tot i així, tots els candidats eren rebutjats d'alguna manera o altra. Shamir era un altre científic computacional, intel·ligent i amb una capacitat brillant de centrar-se en el nucli del problema. Proposà moltes idees per a formular un xifrat asimètric, però les seves idees eren defectuoses. Adleman, un matemàtic amb una enorme resistència, rigor i paciència, va ser el gran responsable de detectar els problemes de les idees de Rivest i Shamir, assegurant que no perdien el temps seguint aquests projectes falsos. Rivest i Shamir es passaren un any innovant les seves idees, mentre Adleman es passà un any trobant els punts febles d'aquestes. El trio començà a perdre l'esperança, però eren totalment conscients que cada fracàs els aproximava més a la solució. No trigaren en ser recompensats per la fortuna, o pel seu enginy.

A l'abril de 1977, Rivest, mentre es trobava a casa seva, es preguntà si era possible dissenyar un xifrat asimètric, o si era possible crear una funció que només pot ser invertida en el cas de posseir una informació especial. Portava setmanes fent-se aquestes preguntes quan se li va ocórrer finalment una idea brillant. Es passà tota la nit formulant la revelació abans que el sol aixequés el cap. Rivest havia fet un gran assoliment, però l'havia aconseguit gràcies a un any de contínues col·laboracions amb Shamir i Adleman, i no hauria estat possible sense ells. Acabà l'escrit escrivint els tres noms en ordre alfabètic: Adleman, Rivest i Shamir.

El següent matí Rivest proporcionà la formulació de la seva idea a Adleman, qui acostumava a revisar totes les idees en busca d'errors, però no en trobà. L'única crítica que va rebre per part d'Adleman va ser que el seu nom sobrava del document amb la idea, però Rivest es negà a esborrar-lo. Després de discutir sobre aquest afer aparentment insignificant, Adleman acceptà l'aparició del seu nom, però com a tercer autor, ja que creia que no era de vital importància . No podria haver estat més equivocat. El sistema s'anomenà RSA (Rivest, Shamir, Adleman) enlloc d'ARS, i fou el xifratge que més influencià en la criptografia moderna.

El cor del xifrat asimètric proposat per Rivest era una funció unidireccional basada en l'aritmètica modular. La funció era capaç d'encriptar un missatge, transformant el missatge en nombres, els quals es transformen en altres en la funció. El seu funcionament es basa en els nombres primers, es descriu de la següent manera:

1-. L'Alice escull dos nombres primers amb moltes xifres. Els primers poden ser enormes, però per simplificar-ho suposem que escull $p = 17$ i $q = 23$. Aquests dos han de ser completament secrets.

2-. En multiplica els dos per obtenir un nombre, *N*. En aquest cas $N = 391$. Ara escull un altre nombre, *e*, i escull que $e = 15$ (e i $(p - 1) * (q - 1)$ han de ser coprimers, és a dir que no han de tenir cap primer comú.

En el cas exposat calculem el valor $m = (p - 1) * (q - 1)$, i obtenim el resultat $m = 352$. Aquest s'ha de factoritzar, igual que el nombre *e*:

$m = 352 = 2 * 2 * 2 * 2 * 2 * 11$

$e = 15 = 3 * 5$

Així es demostra que entre *m* i *e* no hi ha factors comuns.

3-. L'Alice publica *e* i *N* en algun lloc on tothom ho pugui buscar, com en internet avui en dia, o en una direcció telefònica. Si els dos nombres són necessaris per encriptar, han de poder-se trobar fàcilment per qualsevol que li vulgui enviar un missatge. Els dos junts formen el que anomenem clau pública.

4-. Per encriptar un missatge, aquest s'ha de convertir en nombres, *M*. Per exemple, si volem convertir una paraula ho podem fer amb ASCII, és a dir, amb dígits binaris, o fent una taula com la següent:

*	0	1	2	3	4	5	6	7	8	9
0	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
1	XX	A	B	C	D	E	F	G	H	I
2	J	K	L	M	N	O	P	Q	R	S
3	T	U	V	W	X	Y	Z	a	b	c
4	d	e	f	g	h	i	j	k	l	m
5	n	o	p	q	r	s	t	u	v	w
6	x	y	z	.	,	:	;	‘	“	`
7	!	@	#	$	%	^	&	*	-	+
8	(	)	[	]	{	}	?	/	<	>
9	0	1	2	3	4	5	6	7	8	9

Taula 16: Taula d'equivalència de valors als símbols.

En l'exemple exposarem segons els valors de la taula, on la lletra *K* equival a 21. Per tant, el missatge *M*, és encriptat per obtenir el text xifrat, *C*, amb la fórmula:

$$C = M^e \text{ [mòd. } N\text{]}$$

5-. En Bob només ha de mirar la clau pública de l'Alice i observar que N = =391 i e = 15. Ara ja posseeix tota la informació per aplicar la fórmula i calcular:

$$C = 21^{15}\text{[mòd. 391]}$$

6-. Treballar amb aquest nombre en una calculadora és una feina complicada, ja que no agafa nombres tan llargs. No obstant podem calcular exponencials en aritmètica modular gràcies a l'equivalència 15 = 6 + 5 + 4

$$21^{15}\text{[mòd. 391]} = 21^6\text{[mòd. 391]} * 21^5\text{[mòd. 391]} * 21^4\text{[mòd. 391]}$$

$21^4 = 194481 = 154$ [mòd. 391]
$21^5 = 4084101 = 106$ [mòd. 391]
$21^6 = 85766121 = 271$ [mòd. 391]

$21^{15} = 21^4 * 21^5 * 21^6 = 154 * 106 * 271 = 221.190.200 = 30$ [mòd. 391]

Per a calcular-ho amb la calculadora es multiplica tot obtenint 4.423.804, i aquest es divideix entre 391, aconseguint així el número 11.314,0767263427, li traiem la part entera i multipliquem el resultat per 391 aconseguint el resultat del mòdul.

El Bob ja li pot enviar el seu text xifrat, C = 30.

7-. Ja sabem que treballar exponencials en aritmètica modular són funcions unidireccionals, per això és molt difícil treballar a partir de C = 30, i recuperar el missatge, *M*. Per tant l'Eve no podrà desxifrar el missatge.

8-. Tot i que l'Alice podrà desxifrar el missatge perquè té una informació especial, el coneixement dels valors de p i q. Ara ha de calcular un nombre essencial, d, que és la clau per a desxifrar, la clau privada. Es pot trobar gràcies al petit teorema de Fermat. Aquest diu que si $a > 0$ i enter, i p un nombre primer, es compleix que

$a^{p-1}=1$[mòd. p], i pel teorema d'Euler, un conjunt de nombres menors que *N* que són alhora primers amb ***N***, i s'expressa com a φ, si $N = pq$, sent *p* i *q* dos nombres primers, llavors $\varphi = (p - 1) * (q - 1)$]. La funció d'Euler, exposa que donat un valor enter *n*, es defineix *φ(n)* com la quantitat de nombres naturals menors o iguals que *n* coprimers amb *n*. Per exemple, φ(10) = 4, ja que hi ha 4 nombres menors que 10 coprims amb ell: {1, 3, 7, 9}. Llavors pel teorema d'Euler, si mcd (*N*, *a*) = 1, es mostra que $a^{\varphi(N)} = 1$ [mòd. N]. Per a calcular l'únic valor *d* en mòdul φ(*N*) que verifica $d * e = 1$, és a dir, la inversa d'*e* en mòdul φ(*N*). Es sap que aquest existeix ja que existeix mcd (φ(*N*), *e*) = 1.

El nombre *d* es calcula segons la fórmula:

e $* d = 1$ [mòd. $(p - 1) * (q - 1)$]

$15 * d = 1$ [mòd. 352]

Per a resoldre apliquem el teorema d'Euclides i busquem l'invers de 15 en mòdul 352:

$$352 = 23 * 15 + 7$$

$$15 = 7 * 2 + 1 \; ; \; 1 = 15 - 7 * 2 = 15 - 2\,(352 - 23 * 15) = 47 * 15 - 2 * 352$$

Ara passem l'última equació a mòdul 352, de manera que l'únic que varia és el 352, quedant l'equivalència següent:

$$1 = 47 * 15 - 2 * 0$$

$$1 = 47 * 15$$

Això vol dir que l'invers de 15 en mòdul 352 és 47, per tant:

$d = 47$

9-. Per desxifrar el missatge, l'Alice farà servir la següent fórmula:

$M = C^d$ [mòd. 391]

$M = 30^{47}$ [mòd. 391]

$M = [30^6$[mòd. 391] $* 30^6$[mòd. 391] $* 30^6$[mòd. 391] $* 30^6$[mòd. 391] $* 30^6$[mòd. 391] $* 30^6$[mòd. 391] $* 30^5$[mòd. 391] $* 30^4$ [mòd. 391] $* 30^2$[mòd. 391]] [mòd. 391]

$M = 50 * 50 * 50 * 50 * 50 * 50 * 132 * 239 * 118$ [mòd. 391]

$M = 21$ [mòd. 391]

L'Alice només a de mirar a què equival el nombre 21, i comprova que és la lletra *K*, per tant queda demostrada l'eficàcia d'aquest sistema criptogràfic.

Descrivint RSA en termes d'encriptació lletra per lletra cal aclarir que en aquest exemple el xifratge és reduït a una substitució monoalfabètica sense clau de distribució. A la pràctica, l'encriptació es fa amb nombres més grans, és a dir, no lletra per lletra, i és el que fa que sigui impossible un anàlisi freqüencial.

Un altre problema que ens pot sorgir en contemplar l'exemple, és la facilitat que té quelcom per esbrinar *N*, per tant se'ns podria passar pel cap que factoritzar un nombre com el de l'exemple és senzill. Tot i la senzillesa, és a dir, els valors petits de p i q escollits, els càlculs resultants no tenen el suficient detall en decimals per a ésser calculats amb calculadora, i ens hem hagut d'ajudar de l'ordinador. En el cas d'escollir nombres de més de 100 xifres com a factors de *N*, la factorització requereix una enorme quantitat de temps. En l'actualitat, els nombres primers que s'usen per encriptar un missatge de confidencialitat superen els 200 dígits.

Per a demostrar la complexitat de factoritzar nombres relativament llargs, podem proposar-nos trobar els dos nombres primers que multiplicats entre ells formen el número 197.111. Trigaríem unes hores en trobar la solució, però imaginem que enlloc de 6 xifres en té 200... aquesta és la particularitat que fa tan característic el sistema de claus asimètric. Com a curiositat, $N = 197.111$, està format per $p = 439$ i $q = 449$. Podem contemplar la immensitat dels càlculs sabent que entre el nombre 1 i el 50.000, és a dir en [1, 50.000], hi ha 5.133 nombres primers, els quals hauríem de provar un per un.

La seguretat del sistema criptogràfic asimètric conegut com RSA, resideix en la factorització de *N*, ja que és el que l'Eve haurà de calcular o esbrinar per a desxifrar els missatges. El temps que hauria d'emprar depèn de la velocitat del seu ordinador. L'expert en seguretat Simson Garfinkel va estimar que un ordinador de 100 MHz amb 8 MB de RAM trigaria uns quinze anys en factoritzar un nombre de 10^{130} dígits. Tot i això, els criptògrafs acostumen a tenir paranoies, i es posicionen en els casos hipotètics de pitjor grau, com que passaria si hi hagués una conspiració mundial per trencar xifratges. Per aquest motiu Garfinkel considerà que passaria si cent milions d'ordinadors personals (de la població mundial, i el nombre és el número d'ordinadors

venuts el 1995) funcionessin cooperant. El temps resultant per factoritzar un nombre tan gran com 10^{130} seria d'uns quinze segons. Per tant, és acceptada la teoria que per major seguretat es necessiten nombres primers més llargs. Per exemple, en les transaccions bancàries *N* tendeix a tenir un mínim de 10^{300}dígits. La combinació de cent milions d'ordinadors domèstics trigaria més d'un miler d'anys per a trencar el xifratge. Es demostra que amb llargs nombres de *p* i *q*, RSA és impenetrable.

El nombre primer més gran que es coneix està format per 17 milions de dígits.

5.3 El secret de la història de la criptografia de clau pública

Des dels anys 80, Diffie, Hellman i Merkle van esdevenir famosos criptògrafs, els quals inventaren el concepte de clau pública, mentre Rivest, Shamir i Adleman han estat relacionats amb el desenvolupament de RSA. Tot i així, una informació ha sorgit de l'anonimat. D'acord amb el govern britànic, la criptografia usant clau pública va ser originàriament un invent del *Government Comunicaations Headquarters* (GCHQ), el quarter de comunicacions més important del govern del Regne Unit, a Cheltenhamm, creat a partir de la desfeta de Bletchley Park. Una història d'intel·ligència, anonimat i secrets d'estat.

James Henry Ellis, un expert britànic en comunicacions segures, estudià en el GCHQ el problema de la distribució de clau, ja que estava encarregat de la seguretat nacional. Aquesta investigació sobre com resoldre el problema durà tot el 1969. Tingué unes idees molt semblants a les de Diffie, Hellman i Merkle, però les del trio van ser el 1975. Ellis va comprovar que el problema de la distribució de claus es podia resoldre desenvolupant el concepte de clau pública i clau privada (que ell anomenà encriptació pública). També arribà a la conclusió que necessitava una funció irreversible, una que només es pogués calcular la inversa a partir d'una informació especial. Desafortunadament, Ellis no era un matemàtic, i no va poder desenvolupar una funció matemàtica amb els requisits necessaris.

Durant tres anys, les ments més brillants del quarter treballaren per satisfer Ellis trobant la funció adequada. No va ser fins el 1973, que un nou matemàtic graduat en teoria numèrica a Cambridge, Clifford Cocks, trobà la solució a tal mal de cap com la funció unidireccional. Cocks, en conèixer les idees d'Ellis, pensà en com resoldre el problema de la funció, i des de l'inici es refià de la factorització de nombres primers de llargues xifres. Va ser el principi de la formulació del que després esdevindria el xifrat

asimètric RSA. Rivest, Shamir i Adleman van descobrir la fórmula per la criptografia de la clau pública el 1977, però anys abans el mateix sistema havia estat pensat per un jove graduat.

Tal i com va fer Adleman, Cocks no va acabar d'apreciar el gran descobriment que havia aconseguit fins anys més tard. Tot i que la idea del jove va ser un dels secrets més ben guardats, patia un problema important per ser tan avançat al seu temps. Cocks formulà una funció que permetia la codificació amb clau pública, però existia el problema d'implementar el sistema. L'encriptació per mitjà d'aquest tipus de claus requeria molta més potència computacional que un xifratge simètric. A principis dels 70s, els ordinadors eren encara relativament primitius, i incapaços d'operar processos de tals magnituds. Com a conseqüència, el GCHQ no estava en disposició d'explotar el sistema criptogràfic de clau pública. Cocks i Ellis van ser els primers en demostrar que allò aparentment impossible, resoldre el problema de la distribució de claus, era possible, però no van trobar la manera de fer-ho a la pràctica.

Anys més tard, cap al 1974, Williamson, un criptògraf del quarter, escoltà el treball realitzat per Cocks i no el va voler acceptar com a vàlid ja que havia de tenir un punt feble. L'analitzà detalladament, i l'intentà modificà. El resultat de la seva desconfiança amb les idees de Cocks el portà a descobrir una altra solució al problema de la distribució de la clau. Desenvolupar el protocol conegut com a intercanvi de clau Diffie-Hellman-Merkle.

Per l'any 1975, James H. Ellis, Clifford Cocks i Malcolm Williamson van descobrir tots els aspectes fonamentals de la criptografia de clau pública, encara que tots es van mantenir en secret. Els tres britànics varen haver de contemplar com les seves idees foren redescobertes per Diffie, Hellman, Merkle, Rivest, Shamir i Adleman en els posteriors tres anys.

Tot i que el GCHQ va ser el primer en descriure en detall el sistema criptogràfic asimètric, no hauríem de treure importància als èxits dels acadèmics que ho varen redescobrir. Van ser aquests últims els qui s'adonaren del potencial de l'encriptació amb clau pública, i foren els primers en implementar-la a nivell pràctic. Encara que les idees dels americans resultaren les mateixes que les dels britànics, les dues van desenvolupar-se sense mantenir cap mena de contacte amb l'altra. Això es deu a l'alt nivell de secretisme dels quarters britànics, on ningú, excepte aquells que treballen allà, tenen excés als documents que s´hi troben a l'interior. Tots els coneixements que rodegen un món classificat, amagat de la majoria de la població. En el nostre cas, els documents

secrets són l'existència, la creació de la criptografia de clau pública i la seva funció irreversible.

El grau de mantenir tot el que envolta el GCHQ és difícil de menysprear. Tot i la publicació d'RSA, el quarter es mantenia en silenci. Fins i tot en els 80s, quan l'ús ordinari d'RSA es començà a estendre pel món, el GCHQ rebutjà el coneixement del seu propi invent.

No va ser fins vint-i-vuit anys més tard, que les idees d'Ellis sorgiren a la llum. El 1977, Cocks finalitzà treballs importants sobre RSA a nivell informatiu per a la població mundial. Com a resultat d'aquests planejà fer una exposició de les seves recents investigacions davant una sala plena d'experts en criptografia. Cocks, qui parlaria sobre un dels aspectes del que ell creà, RSA, no podia esmentar que el primer descobridor del sistema no era Rivest, sinó que ell mateix. La situació era clarament ridícula, i el quarter decidí que era hora de canviar la seva política de secretisme. El britànic va rebre el permís de començar la seva xerrada amb una presentació de la història del GCHQ envers la contribució de la criptografia de clau asimètrica.

El 18 de desembre de 1997, després de més de dues dècades, Cocks revelà el reconeixement que mereixien Ellis, Williamson i ell mateix. Desafortunadament, Ellis morí un mes abans de publicar els seus èxits, de la mateixa manera que li succeí a Charles Babbage amb desxifratge del xifrat de Vigenère, on fou Kasiski qui s'endugué el mèrit de ser el primer en trencar-lo. Similarment a la situació d'Alan Turing, que no va poder esmentar el seu treball sobre Enigma per culpa del secretisme imposat pel govern britànic. Tant Ellis com Babbage, com Turing, no van viure el suficient per a veure la publicació de les seves respectives contribucions.

6 AUGMENT DE LA PRIVACITAT I UN FUTUR CRIPTOGRÀFIC

L'intercanvi d'informació via digital s'ha integrat ja a la nostra societat, ja que milions de missatges s'envien cada dia, internet ha esdevingut una important eina de mercat. Els diners viatgen per la xarxa, i s'estima que més de la meitat del capital de la població mundial es mou per aquesta. A més a més, ha arribat a la xarxa el vot polític via online, i els governs usen cada vegada més internet per a organitzar els seus països, oferint serveis com pagar els impostos online. Sens dubte, ens trobem dins l'era de la informació.

Aquesta era està marcada principalment de la dependència de l'habilitat de protegir la informació que envolta el món, la qual descansa en les mans de la criptografia. L'encriptació es pot contemplar com la distribuïdora de cadenats i claus de l'era de la informació. Durant dos milers d'anys els sistemes criptogràfics han tingut gran importància només en un sentit governamental i militar, però avui en dia també juga un paper indispensable en el món empresarial, i en la privacitat de la gent ordinària. Per sort, amb la incorporació de la nova era, hem aconseguit tenir excés a encriptacions extraordinàriament potents. El desenvolupament de la criptografia de clau pública, particularment el xifrat RSA, ha donat un gran avantatge en la seva contínua lluita contra els criptoanalistes. Si el valor de N és suficientment llarg, fa que trobar p i q sigui una labor d'un temps incalculable, i permet afirmar que l'Eve no podrà trencar el xifrat. El més important de tot, és que la combinació de clau pública-clau privada no es veu afectada pel problema de la distribució de clau. En definitiva, RSA garanteix quasi amb total seguretat els cadenats, l'encriptació indestructible usada per a la informació més valuosa.

Tot i això, com trobem en tota la tecnologia, hi ha un costat negre al voltant de l'encriptació. Igual que protegeix les comunicacions dels ciutadans, la criptografia també protegeix els criminals i terroristes. Avui en dia, les forces policials fan servir escoltes telefòniques com a mètode per a reunir proves contra organitzacions de crim organitzat o terrorisme, però seria del tot ineficaç si fessin servir xifrats indestructibles.

Ja a finals del segle XX i principi del XXI, el principal dilema de la criptografia era trobar una via que permetés a la població i les petites empreses usar l'encriptació. El dilema és degut al fet que fins els anys 80 només els governs, l'exèrcit i les grans

empreses tenien ordinadors suficientment potents per a treballar amb RSA, per tant, posseïen el monopoli de la criptografia segura. No va ser fins l'estiu del 1991, que Phil Zimmermann, un físic estatunidenc i activista en pro de la privacitat, oferí el sistema PGP (*Pretty Good Privacy*, <<Privacitat raonable>>). Aquest era un algoritme d'encriptació gratuït capaç de funcionar en ordinadors domèstics. PGP fa servir una codificació amb clau simètrica, factor que li proporciona rapidesa, però xifra la clau amb una encriptació asimètrica RSA.

Zimmermann escriví en una carta oberta una sèrie de reflexions sobre el món que ens envolta. En aquesta trobem el preu que hem de pagar per viure en l'era de la informació, on es veu amenaçada la nostre privacitat, i la facilitat del govern en interceptar comunicacions i desxifrar-les. En conseqüència, un coneixement mínim de la codificació i xifratge que ens rodeja pot ésser de vital importància per a protegir els nostres secrets. Per aquest motiu argumenta la seva distribució de PGP, que permet encriptar de manera segura el que només podia fer abans el govern, l'exèrcit, les grans empreses i els grans traficants o terroristes. En aquest comunicat es declara totalment a favor de la privacitat, per això és tan important.

En aquest context de defensa de la privacitat sorgeix el sistema PGP, que al contrari que el sistema RSA, va ser creat per a la població, i no per aquells que es poguessin permetre adquirir ordinadors de gran potència. Zimmermann creia que tothom havia de tenir el dret de privacitat. PGP està basat en la mateixa seguretat que pot donar RSA, però amb la capacitat de ser operat en un ordinador comercial. Per a tal projecte combinà l'encriptació simètrica, pel missatge, i la asimètrica, per la clau. Tot i aquesta simplicitat, a l'hora d'operar, un ordinador normal pot trigar uns minuts en xifrar el missatge o desxifrar-lo.

Zimmermann plantejà el següent escenari. Si l'Alice vol enviar un missatge encriptat a en Bob, primer haurà de codificar el missatge amb un xifrat simètric, com pot ser IDEA, paraula que suggerí el mateix Zimmermann. Per encriptar el missatge l'Alice fa servir una clau que haurà de compartir amb en Bob d'alguna manera. Soluciona aquest petit problema buscant la clau pública d'en Bob, i la fa servir per encriptar la clau IDEA. Ja li pot enviar el missatge encriptat amb el xifrat simètric, i la clau corresponent encriptada amb el xifrat RSA. A l'altra banda, en Bob només ha de desxifrar la clau IDEA amb la seva clau privada d'RSA, obtenint així la clau simètrica que li permet desxifrar el missatge. La combinació dels dos tipus de clau la va nombrar PGP.

La publicació d'aquest no es va dur a terme fins el 1991, i de forma gratuïta per aconseguir arribar al màxim nombre de persones possibles. En un inici, només els fanàtics de la criptografia descarregaren el software que permetia encriptar amb PGP. Més tard, una àmplia part dels entusiastes d'internet el feren servir, fins arribar al punt que totes les revistes parlaven del fenomen causat per PGP, que guanyava importància en la comunitat digital. La seva aportació el feu guanyar una quantitat enorme de fans, que podien comunicar les seves idees contràries a les del temps, gràcies al seu software. Va rebre varis correus informant sobre la gran ajuda a la vida dels emissors, com és el cas d'algú de Latvia, que li donà les gràcies per a poder defensar la democràcia a Rússia per mitjà de comunicacions segures.

Mentre Zimmermann es feia famós al voltant del món, al seu país no era tan popular. Al febrer de 1993 va ser acusat pel govern nord-americà per traficar amb armes, a causa de l'exportació de PGP. En els següents anys va ser investigat pels oficials del govern per grans delictes. Les investigacions sobre Zimmermann iniciaren un debat sobre els efectes positius i negatius de l'encriptació en l'era de la informació. La propagació de PGP encoratjà a molts criptògrafs, polítics i ciutadans a anar a favor del dret de la llibertat, i a les forces de la llei a pensar les conseqüències de la divulgació del sistema informàtic. Hi havia els partidaris de Zimmermann, que defensaven el dret a la privacitat digital de la societat, i els qui estaven en contra, ja que els criminals i terroristes serien capaços de comunicar-se en secret, segurs de les escoltes policials.

Les forces judicials argumentaren que les escoltes eren necessàries per mantenir l'ordre i la llei, i l'encriptació devia ser restringida per a poder desxifrar intercepcions de missatges. La policia, en els successius anys, ja havia trobat criminals que feien servir forts sistemes criptogràfics. En són exemples els càrtels de Cali, que traficava amb droga, la secta Aum Shinrikyo, responsables d'atacs gasosos al metro de Tokio, o Ramsey Yousef, un dels terroristes involucrats a l'atemptat del World Trade Center. Tots tres feien servir l'encriptació per a comunicar-se o mantenir la informació secreta. A nivell nacional també era un problema, ja que l'estació d'espionatge més gran del món a Yorkshire, posseïa un programa anomenat Echelon que detectava paraules sospitoses dels correus, com *assassinat* o *Pentàgon*. Echelon seria ineficaç en el cas que tots els correus s'encriptessin, ja que no serviria per a res.

Per altra banda trobem el debat dels llibertaris, partidaris de la democràcia, tecnologia i la fundació de fronteres electròniques. Aquests es mostraven a favor de l'encriptació, ja que creien en el dret fonamental de la població sobre la privacitat,

reconegut en l'article 12 de la Declaració Universal dels Drets Humans: "*Ningú no serà objecte d'intromissions arbitràries en la seva vida privada, la seva família, el seu domicili o la seva correspondència, ni d'atacs al seu honor i reputació. Tothom té dret a la protecció de la llei contra tals intromissions o atacs*."

Tots els qui estaven a favor d'aquest article defensaven que la recent expansió de l'encriptació era un fet essencial per a garantir el dret a la privacitat, de manera que el govern no pogués fer servir més el seu poder basat en les escoltes i intercepcions de missatges de ciutadans innocents. Un dels casos més coneguts del continu espionatge afectà a Martin Luther King Jr., qui va ser controlat durant molts anys. L'agència de l'FBI compartí certa informació privada de King, que es feia servir per desacreditar-lo distribuint aquesta a amics, periodistes i, fins i tot, a la seva pròpia família. Els consecutius intents pretenien que finalitzés la seva lluita contra els drets civils. Per a realitzar aquest propòsit, arribaren a l'extrem d'invitar-lo a suïcidar-se.

Possiblement la major infracció a la privacitat mundial és el programa Echelon. Aquest no té perquè justificar cap de les seves intercepcions, ja que no es basa en cap font individual, sinó en l'aparició de certs mots en els nostres missatges, els quals reboten en els satèl·lits. En cas que les comunicacions continguin els mots que formen Echelon, el missatge passa a ser investigat automàticament, amb possibles comunicacions terroristes o grups polítics radicals. Mentre la llei reforça el punt de vista que argumenta que l'encriptació ha de ser suprimida perquè faria Echelon inefectiu, els llibertaris opinen just el contrari, que no ha d'ésser prohibida perquè faria inefectiu Echelon.

Un altre argument a favor de la privacitat, i segurament el més rellevant en la permanència de l'encriptació a les nostres vides, és l'ús del comerç via internet. El comerç online ha augmentat any rere any, fins a disminuir la venda de CDs, llibres... i el mercat computacional ha guanyat molt de terreny als supermercats, companyies de viatges i altres negocis. La major part de les compres que dominen el mercat, es realitzen via internet, però qui ens garanteix la seguretat i la confiança d'aquest tipus de comerç? Ho fa l'ús d'una forta encriptació, sense la qual no hi hauria privacitat, ni seguretat en transaccions de capital.

En especial ho fa el sistema criptogràfic de clau pública. El criptosistema que assegura la transmissió del número de targeta de crèdit, o informació privada de l'estil, es coneix com a TLS (de l'anglès *Transport Layer Securety*, o <<Seguretat de transport de capa>>), dissenyat per l'empresa de software Netscape el 1994.

El protocol TLS combina clau pública i clau simètrica en un procés molt similar a PGP. TLS funciona de la manera resumida a continuació. En primer lloc, el navegador d'internet del comprador verifica que el venedor posseeixi un certificat de clau pública vàlida. Si és el cas, usa la clau pública per encriptar una segona clau, aquest cop simètrica, que s'usa per encriptar el missatge que s'enviarà al receptor. Aquest venedor, amb la seva clau privada, ja pot disposar de la clau simètrica que li permetrà desxifrar el missatge. Tot aquest procés es realitza automàticament, i en el cas que un espia, l'Eve, vulgui obtenir el número de la targeta de crèdit de qualsevol transacció haurà de trencar dos criptosistemes, tot i que el simètric és relativament ràpid i senzill, el de clau pública és el que ofereix la seguretat.

6.1 El futur de la criptografia

Segons el mateix Phil Zimmermann, en la criptografia moderna, és possible crear xifratges els quals els criptoanalistes no poden desxifrar. Com s'ha demostrat, tant la invulnerabilitat de RSA com la de PGP o TLS es troba més enllà de la velocitat de càlcul del més ràpid dels ordinadors actuals. La veritable pregunta és, podem esperar un mètode que faciliti la complexitat de factoritzar grans nombres primers? Segons Zimmermann és una opció massa improbable, s'haurà resolt per fi el conflicte mil·lenari entre criptògrafs i criptoanalistes?

La resposta és que no exactament. En els últims anys del segle XX, ha aparegut una nova forma de dissenyar i operar amb ordinadors, la computació quàntica. Tot i que aquesta només es pot visualitzar a nivell teòric, amenaça tot sistema criptogràfic conegut fins ara gràcies a l'augment de la potència de càlcul.

Aquesta revolucionària tecnologia es basa en la mecànica quàntica, una teoria exposada pel danès Niels Bohr (1885-1962) i els alemanys Max Plank (1858-1947), Erwin Schrödinger (1887-1961) i Werner Heisenberg (1901-1976), entre altres. La mecànica quàntica és la teoria física que regeix el món microscòpic, és a dir, les lleis físiques i paranormals que segueixen les partícules subatòmiques, com els quarks, els fotons o els electrons. Aquesta ha estat demostrada i verificada per tota la comunitat científica, tot i que Einstein, davant una teoria tan poc intuïtiva, la negà rotundament.

Un experiment que ens explica el funcionament de la superposició d'estats, una part de la mecànica quàntica, és el de la paradoxa del gat de Schrödinger. La teoria diu que una partícula està en un mateix instant en més d'una posició, i conté quantitats

diferents d'energia. Quan un observador mesura una de les variables, i no abans, la partícula decideix de manera misteriosa, posseir una quantitat d'energia o una altra, o adoptar una posició o una altra. L'experiment imaginari de l'alemany il·lustra aquesta paradoxa. Imaginem que dins una caixa, opaca i tancada, hi ha un gat i un recipient de gas tòxic connectat a una partícula radioactiva, de manera que si aquesta es desintegra, el gas escaparà i el felí morirà. Suposem que la partícula esmentada té un 50% de probabilitats de desintegrar-se en un període de temps determinat. Passat el temps determinat, el gat estarà viu o mort? El sistema de la caixa-gat es trobarà en una superposició d'estats, ja que fins que un observador no obri la caixa i miri dins, el gat no estarà ni viu, ni mort, sinó ambdues alhora. Si imaginem la caixa amb el gas mortal, la partícula i el gat com un sistema, al dependre d'una sola partícula, està sotmès a les lleis de la física quàntica.

L'experiment del gat de Schrödinger no és l'únic que n'explica la llei, sinó que també n'és un la creença en mons paral·lels, en els quals les partícules adopten una altra posició i una altra energia a la del món en que vivim. Per tant, en un univers paral·lel, amb el seu món, les seves estrelles, les seves cases, etc., en obrir la caixa del gat el trobem mort, però en el món que presenciem està viu. Aquest és un altre experiment que explica la superposició d'estats. Com podem veure, la realitat microscòpica de la física és el comportament il·lògic de les subpartícules.

Tot i així, quina és la relació entre la superposició d'estats i la computació? La idea d'implementar a un ordinador les lleis de la física quàntica, i no les de la clàssica, sorgí el 1984 en la ment del britànic David Deutsch. Com serien aquests ordinadors? De quina manera podria treure partit la computació de la superposició d'estats?

Per a respondre tals qüestions cal que recordem que els ordinadors gestionen unitats mínimes d'informació anomenades bits, capaços d'adquirir un dels dos valors possibles, el 0 i l'1. En canvi un ordinador quàntic agafaria com a unitat mínima d'informació una partícula que presentés els dos estats possibles, per tant el seu valor podria ser l'1, el 0, o els dos alhora. A aquesta unitat d'informació se l'anomena *qubit*, acrònim de *quantum bit* (en anglès <<bit quantum>>). Aplicar la superposició d'estats incrementaria la potència computacional d'una manera incalculable.

Quina relació tindria la invenció d'un ordinador quàntic en la criptografia? La resposta sembla evident, donaria un clara avantatge als criptoanalistes, qui podrien trencar un xifrat per força bruta en un temps curt. Suposem que tenim la informació numèrica continguda en 32 bits. Amb aquest nombre de bits poden codificar-se els

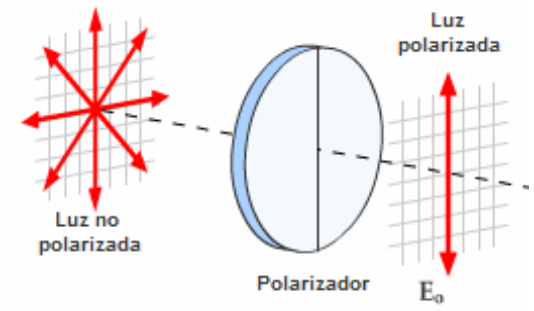
números de l'1 fins el 4.292.967.296 (2 a la 32 = 2^{32} = 4.292.967.296). Si un ordinador regit per la mecànica clàssica hagués de trobar un número concret ho hauria de fer bit per bit. Però un ordinador quàntic podria provar totes les possibilitats amb un sol intent. Suposem que cada *qubit* és l'espín d'un electró, que només el podem trobar en dues posicions, amunt i avall. Aquesta partícula podria representar el valor 0 (espín avall), el valor 1 (espín amunt) i la superposició d'espins, espín amunt-espín avall. Imaginem una caixa opaca on dipositem 32 electrons i els fem entrar en una superposició d'estats. Aquests *qubits* representats com electrons prendrien tots els valors possibles alhora, de manera que la recerca del nombre es faria en una sola vegada, reduint el temps en comparació amb un ordinador convencional. És evident que la potència computacional augmentaria desmesuradament, però quantes operacions simultànies seria capaç de fer?

A nivell teòric es podrien fer 10^{75} càlculs d'una sola vegada, tot i que els treballs de Deutsch dels ordinadors quàntics no eren a nivell pràctic. La realitat d'aquests està en mans de molts investigadors de tot el món. Hi ha experts que consideren impossible la fabricació d'aquests, altres que ens haurem d'esperar entre una o dues dècades, però qui ens pot assegurar que ja no se n'ha construït un i és un dels secrets més ben guardats de la humanitat? Aquesta tecnologia aportaria al propietari un poder inimaginable, ja que no hi hauria comunicacions que poguessin resistir el desxifratge per força bruta.

La computació quàntica acabaria del tot amb la criptografia gràcies a la seva potència? Suposem que fem servir l'algoritme modern RSA, un dels més segurs, per no dir el que més. La seva seguretat es basa en la dificultat de factoritzar un nombre *N* de milers de xifres. La resposta a la pregunta, afirmativa, la donà Peter Shor el 1994. Dissenyà un algoritme capaç de funcionar en un ordinador quàntic, que descomposaria nombres primers de la llargada que usen les claus RSA en un temps infinitament inferior al que trigaria l'ordinador basat en les lleis de la física clàssica més potent. Tots els altres sistemes criptogràfics existents seguirien el mateix camí que RSA, la vulnerabilitat a la força bruta.

Per sort no tot és tan fosc com sembla. Ara ens basarem en el principi d'incertesa de Heisenberg, un dels més importants en la mecànica quàntica. Aquest principi es postulà el 1927, i segons el qual és impossible determinar amb precisió la posició d'una partícula quàntica, ja que no tenen una extensió fixa, i per tant no actuen com a corpuscles localitzats, i deixa de ser lògic parlar de la seva posició. Agafem l'exemple les partícules de la llum o fotons. Una de les característiques fonamentals d'aquests és la capacitat de polarització, la oscil·lació o vibració d'un camp elèctric.

[Tot i que els fotons vibren en totes les direccions possibles suposarem que ho fan en quatre direccions: vertical (↕), horitzontal (↔), diagonal esquerra(↖↘) i diagonal dreta(↗↙)]. Segons el principi de Heisenberg l'únic mètode per a conèixer alguna cosa de la polarització d'un fotó qualsevol, és fer-lo passar per un filtre (polaritzador) en forma vertical, horitzontal, diagonal esquerra o diagonal dreta. Si el filtre és vertical, els fotons polaritzats verticalment travessaran intactes el polaritzador, mentre que els diagonals ho faran només el 50%, i els horitzontals rebotaran, de manera que un cop polaritzat és totalment improbable trobar la polarització original, tal i com es veu en la següent imatge:



Il·lustració 1: Funcionament d'un polaritzador. Fem passar la llum per un filtre vertical, i s'observa que només obtenim fotons verticals, que seran els verticals i la meitat dels diagonals (els fotons són cada una de les fletxes vermelles).

Quina és la relació del principi d'incertesa i la criptografia? La resposta és que íntima. Imaginem que un investigador desitja saber quina és la polarització d'una sèrie de fotons. Per a això no té més remei que escollir un polaritzador amb una orientació específica, com pot ser la vertical. Si el fotó supera el filtre, podem assegurar que la seva orientació original no era horitzontal, aquesta és la única afirmació que podem fer. Podríem suposar que hi ha més probabilitat que l'original estigués orientat verticalment, però hem de tenir en compte que la meitat dels diagonals també el podrien travessar, i hi ha el doble de diagonals, per tant, hi ha una probabilitat del 50% a que l'original fos igual que la direcció del polaritzador. Aquest fet és producte de la física quàntica, i és com actua la naturalesa. Podem aprofitar aquesta particularitat per construir un criptosistema absolutament indesxifrable, com a mínim a nivell teòric.

El 1984, l'estatunidenc Charles Benett i el canadenc Gilles Brassard idearen un criptosistema basat en el principi de Heisenberg, i els fotons polaritzats. El primer pas es basa en un acord en l'assignació de zeros i uns a una polarització o una altra. En l'exemple que exposarem hi ha dos esquemes per determinar-ne el valor: el primer

representat pel signe + (recta), fa equivaldre el 0 a la polarització horitzontal i l'1 al vertical; el segon es representa amb la lletra X (diagonal), que assigna el valor 0 a la diagonal dreta i l'1 a l'esquerra. Per tant, si tenim el missatge 00101101 es podria transmetre de la següent manera:

Missatge	**1**	**0**	**1**	**1**	**1**	**0**	**1**	**1**
Esquema	**+**	**X**	**X**	**+**	**X**	**+**	**+**	**X**
Transmissió	↕	⤢	⤡	↕	⤡	↔	↕	⤡

Taula 17: Conversió d'un missatge a fotons polaritzats.

Si un espia interceptés la comunicació l'hauria de passar per un polaritzador d'una orientació concreta, suposem que fa servir la recta (+):

Missatge interceptat	↕	⤢	⤡	↕	⤡	↔	↕	⤡
Polaritzador	+							
Polarització resultant	↕	↕ o ↔	↕ o ↔	↕	↕ o ↔	↔	↕	↕ **o** ↔
Possible missatge	↕ ⤡ ⤢	⤡ ⤢ ↕ ↔	⤡ ⤢ ↕ ↔	↕ ⤡ ⤢	⤡ ⤢ ↕ ↔	↔ ⤡ ⤢	↕ ⤡ ⤢	⤡ ⤢ ↕ ↔

Taula 18: Interpretació d'un possible espia.

Tal i com es pot comprovar, sense conèixer l'esquema emprat per xifrar el missatge, l'espia és incapaç de desxifrar-lo a partir de la polarització resultant. Tot i que aconseguís obtenir quina assignació de 0 i 1 s'ha fet servir, sense conèixer l'esquema, s'equivocarà un terç de les vegades, tal i com s'exposa en la taula 19. El problema d'aquest sistema és obvi, la distribució de la clau torna a ser un inconvenient.

Esquema de l'emissor	Bit de l'emissor	Fotó enviat	Detector del receptor	El detector és correcte?	El receptor detecta	Bit del receptor	És correcte el bit del receptor?
DIAGONAL	1	⤡	+	No	↕	1	Sí
					↔	0	No
			X	Sí	⤡	1	Sí
	0	⤢	+	No	↕	1	No
					↔	0	Sí
			X	Sí	⤢	0	Sí
RECTA	1	↕	+	Sí	↕	1	Sí
			X	No	⤢	0	No
					⤡	1	Sí
	0	↔	+	Sí	↔	0	Sí
			X	No	⤡	1	No
					⤢	0	Sí

Taula 19: Possibles combinacions d'enviar i rebre un missatge representat amb fotons.

Arribats a aquest punt, podríem imaginar que encriptant la clau amb sistemes criptogràfics de clau pública, com RSA, resoldríem el problema, però la potència dels ordinadors quàntics el farien vulnerable a un atac per força bruta. La solució a aquest problema la trobaren Brassard i Bennett en el quadre de Vigenère, el qual era susceptible d'ésser desxifrat analitzant regularitats en el text, gràcies a l'ús de claus curtes i repetides. La innovació dels dos científics va ser usar claus més llargues que el propi missatge, i anar-les modificant cada vegada que es fessin servir. Aquesta idea proporcionava un xifrat indesxifrable. El primer en idealitzar aquest mètode va ser Joseph Mauborgne, el qual imaginà quaderns amb claus de més d'un centenar de lletres que serviria per encriptar un missatge. Aquest sistema, conegut com a la xifra de quadern d'ús únic és indesxifrable, i ha estat demostrat matemàticament. De fet, es fa servir en algunes comunicacions d'Estat.

L'únic problema d'aquest sistema és el mateix que ha afectat a tota la criptografia, i que la moderna ha aconseguit resoldre, el de la distribució de la clau. Però la comunicació per mitjà de fotons polaritzats és el canal idoni per a transmetre una clau única, i es necessiten uns passos previs:

1. L'emissor envia al receptor un seguit d'uns i zeros escollits aleatòriament, i usa els diferents filtres també a l'atzar, tant els verticals, com horitzontals, com els dos diagonals.

2. El receptor polaritza els fotons rebuts amb esquemes rectes (+) i diagonals (X), alternats aleatòriament, amb la qual cosa concloem que una gran part de la informació rebuda serà errònia.

3. L'emissor i el receptor només s'han de posar en contacte, de manera segura o no, i intercanvien la seqüència de rectes i diagonals que s'han de fer servir per interpretar correctament cada fotó, però sense esmentar la seva polarització (el filtre fet servir). El receptor comenta en quins casos ha rebut el mateix bit que l'emissor li ha enviat, però no sabem si cada un dels bits ha estat trobat perquè s'havia escollit a l'atzar el mateix esquema (recta o diagonal), o per probabilitat (tal i com es mostra en la taula 19, on si el detector és incorrecte, tenim un 50% de rebre el bit original). Finalment els dos interlocutors, ja de manera privada, desfan els bits corresponents als fotons que el receptor ha detectat amb la base equivocada.

Ara ja poden comunicar-se de manera segura, ja que posseeixen una seqüencia d'uns i zeros formada de manera aleatòria, igual que l'elecció de filtres usats per l'emissor, i el conjunt de rectes i diagonals emprada pel receptor. Exposem a continuació un petit exemple de 12 bits del procés descrit anteriorment:

Bits de l'emissor	**0**	**1**	**1**	**0**	**1**	**0**	**0**	**1**	**1**	**1**	**0**	**0**
Esquema	**X**	+	**X**	**X**	+	+	**X**	+	**X**	+	+	**X**
Fotó enviat	⤢	↕	⤡	⤢	↕	↔	⤢	↕	⤡	↕	↔	⤢
Detector del receptor	+	**X**	**X**	+	+	+	**X**	**X**	+	+	**X**	**X**
El receptor detecta	↕	⤡	⤢	↕	↕	↔	⤢	⤢	↕	↕	⤡	⤢
Bit corresponent	**1**	**1**	**0**	**1**	**1**	**0**	**0**	**0**	**1**	**1**	**1**	**0**
Bits retinguts	**-**	**-**	**0**	**-**	**1**	**0**	**0**	**-**	**-**	**1**	**-**	**0**

Taula 20: Exemple de transmissió de 12 bits, i la seva interpretació.

Com es pot veure, es retenen alguns bits que s'han detectat de manera correcta, però com que no s'ha fet servir el mateix esquema i el mateix detector, és a dir, filtres diferents per a un mateix bit, la certesa ha esdevingut mera probabilitat.

Ens posem a la pell d'un espia que ha interceptat tant els fotons enviats com les conversacions públiques entre emissor i receptor. Tot i posseir aquesta informació, no sabem quin filtre de polarització ha fet servir l'emissor, per tant és impossible detectar la polarització correcta. La informació que hem interceptat no ens ajuda, ja que no s'especifiquen les polaritzacions.

Tot i que el pitjor problema d'un possible espia no és aquest, sinó, que en el cas de no haver encertat el filtre correcte, alterarà la polarització del fotó, fent visible la intromissió al receptor. Aquesta modificació no es pot invertir i solucionar-la, o amagar-la. En definitiva, només caldria que emissor i receptor comparessin una part extensa de la clau per detectar qualsevol manipulació de polarització dels fotons.

Per a tal de dur a terme tot aquest procés de verificació de clau, relativament senzill, només fa falta comprovar que cap espia no ha interceptat i intentat desxifrar la comunicació. Per a fer-ho emissor i receptor només han de contactar, no fa falta que de manera segura, i revisar un nombre de bits escollits a l'atzar, suposem que 50. Si coincideixen tots podran estar segurs que ningú ha intentat llegir el missatge transmès, i ja poden donar per bona la seqüència com a clau de quadern d'ús únic. Si es donés el cas que la clau hagués estat verificada, i que un espia aconseguís desxifrar un missatge, les repercucions serien catastròfiques. Significaria que la teoria quàntica té una feblesa, el que tindria conseqüències devastadores pels físics, que es veurien obligats a reconsiderar les lleis de les partícules més petites.

Havent teoritzat com fer un sistema criptogràfic compatible amb ordinadors quàntics, només queda posar-ho en pràctica. El 1989, més d'un any després de dur treball, Bennett es disposà a verificar que la teoria es podia dur a la realitat. Per fer-ho disposà de dos ordinadors separats per 32 centímetres, un dels quals faria d'emissor, i l'altra de receptor. Després de varies hores de proves i ajustaments, l'experiment es donà per finalitzat amb èxit, finalitzant amb la verificació de la clau de quadern d'ús únic. S'havia demostrat que la criptografia quàntica era viable.

L'experiment de Bennet tenia un petit inconvenient, la distància. Tot i això, inspirà a investigadors de la Universitat de Ginebra, els quals aconseguiren un èxit a 23 quilòmetres de distància gràcies al cable de fibra òptica (el 1995), o a un equip del Laboratori Nacional de Los Álamos, d'Estats Units, que arribaren a 107 quilòmetres

amb el mateix procediment (el 2006). Encara que no són distàncies suficients per a la comunicació convencional, ho poden ser per àrees més reduïdes, com per exemple edificis governamentals, seus d'empreses o polítiques.

Si el sistema de criptografia quàntica aconsegueix ser operatiu a llargues distàncies, l'evolució dels xifrats s'aturarà. La demanda de privacitat arribarà a un final. La tecnologia podrà garantir les comunicacions segures per governs, militars, empreses i la població. L'única qüestió que queda per resoldre és si els governs accediran o no a permetre'ns l'ús de tal tecnologia.

7 VALORACIÓ PERSONAL

7.1 Conclusions

Aquest treball de recerca sobre la criptografia i la història d'ella mateixa des dels inicis fins l'actualitat ha sigut, per mi, una gran experiència. Tot i haver suposat un gran esforç i una dedicació enorme de treball continu, he gaudit realitzant-lo.

Penso que he superat amb escreix les expectatives que tenia des d'un principi, doncs a mesura que vaig anar recopilant informació de diferents fonts, tant d'internet com de diversos llibres que tracten aquesta matèria, vaig veure com augmentava considerablement el meu interès i curiositat sobre el tema.

D'altra banda el fet de fer aquest treball m'ha fet endinsar, conèixer i aprendre el funcionament del món secret que envolta les nostres vides i ha sigut tant fonamental al llarg de la història de la humanitat des dels seus orígens.

Crec que el procés d'elaborar el treball m'ha ajudat a aclarir el meu futur, i la decisió d'estudiar Matemàtiques és la principal opció avui en dia.

8 BIBLIOGRAFIA

8.1 Llibres

- GÓMEZ URGELLÉS, Joan. *Matemáticos, espías y piratas informáticos. Codificación y criptografía.* Editorial RBA Coleccionables S.A., Barcelona 2010.
- SINGH, Simon. *The Code Book, HOW TO MAKE IT, BREAK IT, HACK IT, CRACK IT.* Editorial Random House Children's Books, 1540 Broadway, New York, 2001.

8.2 Pàgines Web

- Genbeta Dev: **> http://www.genbetadev.com/seguridad-informatica/tipos-de-criptografia-simetrica-asimetrica-e-hibrida>** (consultes vàries entre març i abril de 2015).
- Revista Digital Universitaria: **>http://www.revista.unam.mx/vol.10/num1/art01/int01-5.htm>** (consultes vàries entre març i octubre de 2015).
- El Diario Turing: **> http://www.eldiario.es/turing/criptografia/Nuevas-velaciones-Snowden-resisten-NSA_0_340515951.html>** (consultes vàries entre març i maig de 2015).
- Wikipedia: **>https://es.wikipedia.org/wiki/Historia_de_la_criptograf%C3%ADa>** (consultes vàries de març a octubre de 2015).
- Durán Díaz, Raúl. Departamento de tratamiento de la Información y Codificación, Instituto de Física Aplicada, CSIC. Revista SIC: **>https://es.wikipedia.org/wiki/Historia_de_la_criptograf%C3%ADa>** (consultes vàries de març a octubre).
- Taringa. **> http://www.taringa.net/posts/info/18350244/Breve-historia-de-la-criptografia-Libros-de-Criptografia.html>** (consultes vàries de març a setembre).

- Ribagorda Garnacho, Arturo. Catedràtic i director del departament d'informàtica de la Universidad Carlos III de Madrid. Revista Sic, *Introducción a la criptografia, 2a Edición actualizada,* 2003: **>http://revistasic.com/revista54/pdf_54/SIC_54_bibliografia.PDF>** (consultes vàries de març a maig).
- Taringa: **> http://www.taringa.net/post/info/17012980/Que-es-eso-de-cifrar-o-encriptar.html**> (consultes vàries de març a setembre).
- El Diario: **> http://www.eldiario.es/hojaderouter/seguridad/criptografia-cuantica-seguridad-ciberespionaje_0_315669050.html>** (consultes vàries de març a octubre).
- Biografías y vidas: **>http://www.biografiasyvidas.com/biografia/h/herodoto.htm>** (consultes al maig).
- Histoblog: **>http://histoblogymas.blogspot.com.es/2009/06/demarato-el-rey-exiliado.html>** (consultes al maig).
- Historia Universal: **>http://mihistoriauniversal.com/edad-antigua/batalla-de-salamina/>** (consultes al maig).
- Wikipedia: >**https://es.wikipedia.org/wiki/Esc%C3%ADtala>** (consultes al juny).
- González, José. Security Art Work: **>http://www.securityartwork.es/2015/06/19/criptografia-el-patito-feo-de-la-informatica-i/>** (consultes al juny).
- Emden, Toby. Code Project: **>http://www.codeproject.com/Articles/15280/Cryptography-for-the-NET-Framework>** (consultes vàries de juny a agost).
- La cambra negra: **>http://www-ma4.upc.edu/cambranegra/crackingsubstitution.html>** (consultes vàries de juny a juliol).
- La cambra negra: **>http://www-ma4.upc.edu/cambranegra/maryqueen.html>** (consultes vàries de juny a juliol).

- La cambra negra: **>http://www-ma4.upc.edu/cambranegra/digraphcipher.htm>** (consultes vàries de juny a juliol).
- Muslim Heritage: **> http://www.muslimheritage.com/article/al-kindi-cryptography-code-breaking-and-ciphers>** (consultes vàries al juliol).
- Digits, dels número al bit: **>http://www.digits.cat/colaboracions/criptografia**> (consultes vàries al juliol).
- Redy Seguridad. Fundamentos de la criptografía. Universidad Nacional Autónoma de México, facultad de ingeniería: **> http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/>** (consultes de juliol a setembre).
- Llistat de paraules més frqüents en català: **>https://docs.google.com/file/d/0B_wvOxuXHTZ-WnJyVllKNFRLdWM/edit>** (consulta el 28 de juliol).
- Wikipedia: > **https://en.wikipedia.org/wiki/Giovanni_Soro**> (consulta el 5 d'agost).
- Wikipedia: >**https://en.wikipedia.org/wiki/Substitution_cipher#Homophonic_substitution>** (consultes vàries durant l'agost).
- Kriptópolis, criptogrfía y seguridad: >**http://www.kriptopolis.com/entender-rsa>** (cunsultes vàries d'agost a octubre).
- Hipertextual, *La máquina Enigma, el sistema de cifrado que puso en jaque a Europa*: **>http://hipertextual.com/2011/07/la-maquina-enigma-el-sistema-de-cifrado-que-puso-en-jaque-a-europa>** (consultes vàries d'agost a setembre).
- Vikipèdia: **>https://ca.wikipedia.org/wiki/Batalla_de_l%27Atl%C3%A0ntic_(1939-1945)#Enigma_desxifrat>** (consultes vàries d'agost a setembre).
- Wikipedia: **>https://ca.wikipedia.org/wiki/Batalla_de_l%27Atl%C3%A0ntic_(1939-1945)#Enigma_desxifrat>** (consultes vàries durant el setembre).
- Te interesa saber, *Los traductores del código navajo en la Segunda Guerra Mundial*: **> http://www.teinteresasaber.com/2014/03/los-traductores-del-codigo-navajo-en-la.html**> (consultes vàries durant el setembre).

- Wikipedia: > **https://es.wikipedia.org/wiki/C%C3%B3digo_Lorenz>** (consulta el 26 de setembre).
- Viquipèdia: **>https://ca.wikipedia.org/wiki/ASCII#Els_car.C3.A0cters_de_control_ASCII>** (consultes el 3 i 4 d'octubre).
- Wikipedia: **>https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange**> (consultes vàries a l'octubre).
- Wikipedia: >**https://en.wikipedia.org/wiki/Government_Communications_Headquarters#Public_key_encryption**> (consultes vàries a l'octubre).
- Wikipedia: **> https://es.wikipedia.org/wiki/Phil_Zimmermann>** (consultes vàries a l'octubre).
- Zimmermann, Philip: **>http://groups.csail.mit.edu/mac/classes/6.805/articles/export/zimmermann-oct93.txt>** (consultes vàries a l'octubre).