XIFRES, CODIS I ALTRES MÈTODES CRIPTOGRÀFICS

Amargo Azulón

Curs 2009-2010

Presento els meus agraïments a Jordi Mompart, Noelia González, David Juher i Gabriel Molina, així com a als meus pares pel seu suport.

ÍNDEX

“L’impuls de descobrir secrets està molt arrelat a la naturalesa humana; fins i tot la menys curiosa de les ments reacciona davant la promesa de compartir informació d’amagat dels altres. Alguns són prou afortunats per trobar una feina que consisteix en la solució de misteris, però la majoria hem d’aplacar aquest impuls resolent enigmes artificials concebuts per entretenir-nos. Les històries de detectius i els encreuats satisfan a la majoria; la solució de codis secrets només està a l’abast de pocs.”

John Cadwick (1920-1998), lingüista britànic que va participar en el desxiframent del Linear B, sistema d’escriptura utilitzat a Grècia el segon mil·lenni aC.

1. INTRODUCCIÓ

Abans de començar a fer el treball de recerca tenia dues opcions al cap: criptografia i domòtica. Finalment em vaig decantar per la criptografia per dues raons: tenia més clars els meus objectius i "ja sabia de què anava". O això era el que jo creia.

Els dos objectius que em vaig plantejar quan vaig començar a fer el treball van ser esbrinar quin rol té la criptografia en l'actualitat i saber si existeix un criptosistema totalment segur.

Vaig apuntar-me al programa Argó de la UAB per poder tenir un tutor extern del treball de recerca que m'assessorés i m'ajudés. El meu tutor va resultar ser un professor de Física, Jordi Mompart, que m'ha ajudat molt al moment de poder comprendre la criptografia quàntica. A més a més, gràcies a ell vaig poder anar a visitar l'Institut de Ciències Fotòniques de Castelldefels (ICFO), on vaig poder veure com es realitzava la duplicació de fotons i on em van explicar com funcionava el protocol de criptografia quàntica E91.

Més tard vaig comprar-me diversos llibres, *Introducció a la Criptografia* i *L'art de la comunicació secreta*, ambdós de David Juher, i *The Code Book*, de Simon Singh. Aquest últim llibre vaig haver de comprar-lo en anglès ja que no el trobava enlloc en castellà. Era, a més, un llibre imprescindible, ja que sortia esmentat a tot arreu on buscava informació de criptografia.

També vaig decidir contactar amb David Juher, l'autor de dos dels llibres esmentats abans i professor del Departament d'Informàtica i Matemàtica Aplicada de la UdG. Ell va acceptar ajudar-me, i a partir de llavors li enviava totes les actualitzacions del treball que també enviava als meus dos tutors, en Martí Llauró i en Jordi Mompart.

Pel fet de ser un tema bàsicament teòric, no sabia què podia fer de part pràctica. Vaig decidir que passaria diverses parts d'un text xifrat amb un sistema molt dèbil a un grup d'alumnes de 1r de Batxillerat per veure quan tardaven, per on començaven, etc. amb uns quants ajuts. Malauradament, molt pocs d'aquests alumnes han fet la feina i no he pogut treure conclusions d'aquesta pràctica.

Llavors vaig decidir que desxifraria jo mateix tres missatges xifrats que apareixen al final del llibre *The Code Book*. Val a dir que m'he ajudat de diversos programes on-line per dur a terme la pràctica.

Quan ja tenia tota la part teòrica acabada vaig rebre un correu electrònic d'en David Juher en el qual m'informava de què hi havia novetats recents en el món de la criptografia quàntica i m'enviava un enllaç a una pàgina de Miquel Duran, professor de la UdG, en la qual afirmava "he vist que s'ha trobat un mètode per interceptar-los [els missatges criptoquàntics] sense que se sàpiga". Aquesta informació em va obligar a reescriure el final del treball.

He intentat que el meu treball no fos ni massa teòric ni massa divulgatiu, intentant trobar un punt intermedi entre els dos extrems. El contingut matemàtic és el just per poder explicar alguns dels mètodes que presento, encara que evidentment els fonaments matemàtics reals són molt més profunds. Tots els gràfic i taules que surten al treball i dels quals no esmento la font els he fet jo.

El treball m'ha ajudat a desprendre'm de la imatge tan romàntica que tenia de la criptografia, una imatge d'intrigues novel·lesques i espionatge, i a veure la importància cabdal i l'omnipresència de la criptografia a les nostres vides, des que enviem un e-mail o utilitzem una televisió de pagament fins quan paguem amb la targeta de crèdit o parlem per telèfon.

2. CONCEPTES CLAU

Criptografia: La paraula “criptografia” prové del grec κρύπτω *krypto*, “ocult”, i γράφω *grapho*, “escriure”, així que la definició literal del terme seria “escriptura oculta”. Actualment es defineix criptografia com a “art o ciència d’ocultar informació” (en criptografia el mot “ocultar” és sovint substituït per altres com “encriptar” o “xifrar”). L’objectiu bàsic de la criptografia és “disfressar” un missatge per tal que tan sols l’emissor i el receptor el puguin entendre mitjançant un mètode el més difícil de desxifrar possible. Quan es xifra un missatge, els signes de puntuació i els espais s’ometen, per tal de no donar pistes a un lector no desitjat, i es divideix la frase en blocs del mateix nombre de símbols, per tal de facilitar la seva lectura.

Esteganografia: la paraula prové del grec στεγανω *stegano* “encobert” i γράφω *grapho*, “escriure”, i literalment significa “escriptura amagada”. Es diferencia de la criptografia en el fet que “amaga” el missatge en comptes de transformar-lo.

Criptoanàlisi: és la ciència que s’ocupa d’intentar desxifrar els missatges xifrats mitjançant un mètode criptogràfic. Juntament amb la criptografia formen la **criptologia**.

Mètode criptogràfic: també anomenat xifra o xifratge. Consisteix en un algorisme[1] que s’aplica al text que es vol xifrar i el transforma.

Clau: és una informació curta necessària per xifrar i desxifrar l’algorisme. Pot ser un nombre, una paraula o frase, un símbol, etc.

Text pla: és el missatge original que es vol encriptar, així com també el missatge que resulta quan el text ha sigut correctament desencriptat.

[1] És un conjunt finit d'instruccions o passos que serveixen per executar una tasca o resoldre un problema.

Text xifrat o criptograma: tal com el seu nom indica, és el text que resulta després d'aplicar l'algorisme d'encriptació al text pla. No sempre té el mateix nombre de símbols que el missatge original. Normalment, tant el text xifrat com el text pla són textos escrits, tot i que també poden ser orals.

Mètodes de transposició: els algorismes de transposició "desordenen" els símbols (lletres, nombres, etc.) del text pla creant el que popularment s'anomena "anagrama".

Mètodes de substitució: els algorismes de substitució "substitueixen" els símbols del text pla per uns altres de diferents. N'hi ha de dos tipus: els xifratges monoalfabètics i els polialfabètics.

Xifratge monoalfabètic: es substitueix l'alfabet[2] original per un altre de diferent[3], de manera que a cada lletra del text pla li correspongui sempre la mateixa en el text encriptat.

Xifratge polialfabètic: una mateixa lletra del text pla pot estar representada per lletres diferents al text xifrat.

Criptografia de clau simètrica: Un algorisme criptogràfic es diu de clau simètrica quan es fa servir la mateixa clau per xifrar i per desxifrar. Cal, doncs que aquesta clau es faci arribar al destinatari del missatge per algun mitjà alternatiu. Aquesta clau es manté en secret i per això es coneix també com a *criptografia de clau secreta.*

Criptografia de clau asimètrica: coneguda també com a *criptografia de clau pública*, és una forma de criptografia en la qual la clau utilitzada per xifrar un missatge difereix de la clau utilitzada per desxifrar-lo. La primera és una clau pública (pot ser coneguda per tothom), però la segona és una clau privada que només coneix el receptor.

[2] L'alfabet pot ser el d'una llegua coneguda, una successió de nombres o símbols, una combinació alfanumèrica, etc.

[3] Pot ser el mateix que l'utilitzat en el text pla però en un altre ordre.

Alice[4]**:** és el nom donat en el textos teòrics sobre criptologia a l'emissor del missatge.

Bob[4]**:** és el nom que rep el receptor del missatge. Ell i l'Alice coneixen la clau o claus utilitzades en el xifratge.

Eve[4]**:** és el nom que es dóna a un atacant passiu (algú que intercepta el missatge però no el pot modificar).

Criptografia quàntica: és la criptografia que utilitza principis de la mecànica quàntica per tal de garantir confidencialitat absoluta en la informació transmesa, ja que a més a més de permetre crear una clau secreta permet saber si algú ha interceptat la transferència d'informació realitzada.

[4] Aquests noms es van utilitzar per primer cop l'any 1978 a l'article *"Communications of the ACM"* en el qual Ron Rivest va presentar el sistema criptogràfic RSA

PART TEÒRICA

3. CRIPTOGRAFIA CLÀSSICA

La primera vegada que es té constància de què es va utilitzar la criptografia va ser a l'Antic Egipte, on els sacerdots escrivien jeroglífics que no significaven res, tan sols eren uns dibuixos fets per a divertir a altres sacerdots. Potser no haurien de ser considerats com a criptografia, ja que no eren utilitzats com a mètode per a transmetre informació de manera oculta.

3.1. Esteganografia

Els primers mètodes per mantenir ocults missatges a un tercer no eren realment criptogràfics, sinó que eren esteganogràfics. Un exemple es troba en l'antic general atenenc Histieu[5], que va rapar un dels seus esclaus més fidels, li tatuà un missatge al cap i va esperar que li creixessin un altre cop els cabells per tal que el missatge quedés ocult. Tenia l'avantatge que el missatger no coneixia el missatge.

Vuelo audaz, glorioso portento
Icaro y Pegaso confiados
Salva a vosotros, que supisteis unidos
Coronar dichosos el sublime intento.
A vos, Franco, la patria os aclama.

Con Ruiz, el hidalgo artillero
Al experto rada, vuestro compañero
Tocado por el dedo de la fama.
América delirante que os abraza
Lloros os da por la viril hazaña.
Un grito universal; Esa es España
No morirá la inolvidable raza.
Ya se mustiaba el laurel fecundo
Aquél de Belloa y de cortés.

La gesta del nauto Genovés
Lustros hacía no asombrando el mundo
Ilustre Franco, hidalgo Español,
Un vuelo del «Plus Ultra» ha demostrado
Recio adagio un poco olvidado
En la ruta de España no se pone el Sol.

Acròstic amagat al poema dedicat a Franco de Màrius Serra al seu llibre Verbàlia

D'altres exemples serien: tauletes de fusta on es gravaven els missatges i es tapaven amb cera, utilitzat molt a l'Antiga Grècia; a la Xina s'escrivia el text en un teixit de seda, es feia una boleta recoberta de cera i es feia menjar al missatger, després només era qüestió de paciència recuperar el missatge; les tintes invisibles, o, ja molt més recentment, els acròstics (paraules o frases amagades en un text aparentment inofensiu, molt utilitzat

[5] Visqué al segle VI aC. Fou nomenat tirà de Milet pel rei persa Darios I el Gran, al qual més tard traí iniciant una revolta per part dels grecs contra els perses.

a l'Anglaterra victoriana) o els micropunts (missatges molt reduïts i amagats al punt d'una lletra "i", utilitzats pels nazis a la Segona Guerra Mundial)

3.2. Xifres de transposició. L'*escítala.*

Un dels primers mètodes de xifratges coneguts va ser l'**Escítala espartana**, que consistia en una vara de fusta d'un diàmetre determinat que es partia en dos, i cada una de les seves parts se la quedava un dels dos reis espartans. Llavors, durant la guerra, un dels reis enrotllava una tira de cuir o papir al voltant de la vara i hi escrivia el missatge longitudinalment. Després es desenrotllava la tira i s'enviava a l'altre rei. D'aquesta manera, si algú agafava la tira, només veia un seguit de lletres sense sentit i no entenia el missatge. El xifratge que usava l'*Escítala* era un mètode de transposició, on els caràcters del missatge sense xifrar (el text pla) es desordenaven, fent el missatge inintel·ligible. L'algorisme matemàtic que defineix la posició dels caràcters al text xifrat en una *Escítala* és aquest:

$$P=n(h-1)+v$$

On "P" és la posició final del caràcter, "n" és el nombre de caràcters que s'escriuen a cada volta, "h" és la posició horitzontal del caràcter a l'*Escítala* i "v" és la posició vertical del caràcter a aquesta última. Un dibuix ho explicarà millor:

Font: elaboració pròpia

Per exemple, si l'*Escítala* emprada tenia una "n" de 4 i una "h" total (nombre de caràcters que hi caben longitudinalment) de 8, el missatge ATAQUEMDEMAALESQUATREPELFLANCEST quedaria convertit en AEUFTMALAATAQARNULECEEPEMSESDQLT. Per tal de poder desencriptar el missatge, tan sols es necessita saber la "n" de l'*Escítala* utilitzada i llavors separar el text xifrat en blocs de la longitud de la clau (n), que en aquest cas és 4, així:

AEUF TMAL AATA QARN ULEC EEPE MSES DQLT

Després, s'agafen les lletres que estan a les mateixes posicions de cada bloc i s'ajunten, formant el text pla, així:

AEUF TMAL AATA QARN ULEC EEPE MSES DQLT

ATAQUEMD EMAALESQ UATREPEL FLANCEST

ATAQUEM DEMA A LES QUATRE PEL FLANC EST

ATAQUEM DEMA A LES QUATRE PEL FLANC EST

Tot i així la criptoanàlisi encara no existia, i l'existència de l'*Escítala* era desconeguda per tothom fora dels reis i la seva gent de confiança, i, per tant, no se sap de ningú que trenqués el mètode de l'*Escítala* mentre es va utilitzar.

3.3. Xifratges de substitució monoalfabètics

3.3.1. Atbash

Erudits hebreus van dissenyar el primer mètode de substitució monoalfabètic, el mètode Atbash, que rep aquest nom per la unió de les primeres i últimes lletres de l'alfabet hebreu: **A**lef-**T**au-**B**et-(**a**)-**Sh**in, on Alef i Bet son les dues primeres lletres i Tau i Shin les dues últimes. Aquest mètode consistia en "plegar" l'alfabet pel mig i escriure la primera lletra en comptes de la última i a l'inrevés, la segona en comptes de la penúltima i al revés, etc. En l'alfabet llatí estàndard (l'alfabet anglès, de 26 lletres) quedaria així:

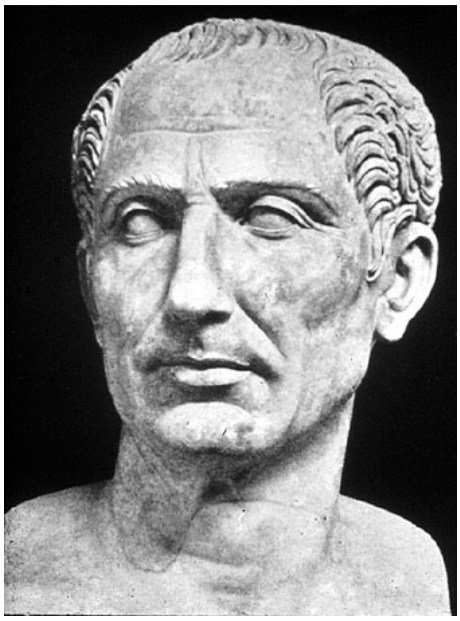
A B C D E F G H I J K L M

Z Y X W V U T S R Q P O N

De tal manera que en comptes de la A s'escriuria la Z, en comptes de la B la Y i així successivament fins a arribar a la Z, que s'escriuria com una A. Per tant, el text "ATAQUEM DEMA A LES QUATRE PEL FLANC EST" quedaria "ZGZJFVN WVNZ Z OVH JFZGIV KVO UOZMX VHG". El xifratge Atbash no té una clau variable, com sí que té l'*Escítala* (la clau d'aquesta és la seva "n"), i el procés de desxiframent del xifratge Atbash és el propi mètode mateix. Per tant, per desencriptar un xifratge Atbash només fa falta aplicar-li el mateix xifratge Atbash.

3.3.2. El Mètode de Juli Cèsar

Més tard, el cònsol romà Juli Cèsar va idear un mètode criptogràfic per a enviar missatges als seus generals amb seguretat. Aquest mètode, anomenat senzillament **Mètode de Juli Cèsar**, consistia en substituir cada lletra de l'alfabet llatí per la lletra situada tres llocs més endavant, tornant a començar quan s'acabava l'alfabet (a la Z li correspon la C).



Gaius Iulius Caesar. Font: *Google*

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

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

Aquí he utilitzat l'alfabet llatí vigent durant l'època de Juli Cèsar. Utilitzant aquest mètode, la famosa frase del cònsol romà "ALEA IACTA EST" s'encriptaria de la següent manera: "DOHD MDFYD HXY". L'algorisme[6] que s'utilitza amb aquest

[6] La operació K (mod n) – en aquest cas x+n (mod p) – consisteix en dividir "K" entre "n" i "agafar" el residu. Per exemple, 35 (mod 16) es calcula dividint 35 entre 16: 35=16x2 + 3. En aquest cas, 35 (mod 16) és 3.

procediment és:

$$f(x)=x+n \pmod p$$

On “f” és la lletra en el text xifrat, de variable “x”, la qual simbolitza la lletra en el text pla, “n” és el nombre de posicions que es mou la lletra a l’alfabet i “p” és el nombre de lletres de l’alfabet, que en el cas de l’alfabet llatí del Segle I aC. era de 23, en els alfabets català i castellà és de 27 i en l’anglès és de 26. Més tard, el successor de Juli Cèsar, l’emperador Octavi August, va utilitzar una variant del mètode del seu antecessor, on la “n” ja no era 3 i passava a ser 1.

Per a poder utilitzar l’algorisme hem de donar a cada lletra de l’alfabet que utilitzem un valor:

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

(taula 1)

Llavors, existeixen *n – 1* variants del xifratge Juli Cèsar per a cada alfabet, on n és el nombre de lletres d’aquell alfabet. Per exemple, en l’alfabet llatí estàndard, de 26 lletres, hi ha 25 variants diferents del mètode Juli Cèsar, cadascuna amb una diferent “n”. Per tant, “n” és la clau del mètode.

3.3.3. Criptosistemes afins

Una manera de reforçar un xifratge de Juli Cèsar és complicant una mica l’algorisme. Si en un Cèsar genèric l’algorisme de xifrat és $f(x)=x + n \pmod p$ on *n* pot prendre valors de 0 a *p-1*, una alternativa és prendre per exemple $f(x)=mx + n \pmod p$, on *n* i *m* són nombres entre 0 i *p-1*. És a dir, si *x* és el valor numèric d’una lletra, multipliquem aquest valor per *m* i després sumen *n*. Aquesta funció és un xic més complicada que la de la xifra de Juli Cèsar, s’anomena *afinitat* i genera un **Criptosistema afí**. Per exemple, si prenem $n = 7$ i $m = 3$ i utilitzem l’alfabet llatí estàndard, tindrem la funció $f(x)=3x + 7 \pmod{26}$. Com quedarà xifrada la lletra “A” amb aquest criptosistema?

Com que el valor numèric de la “A” és 0, calculem f(0)= 3·0 + 7 (mod 26)= 7 (mod 26) = 7, que correspon a la lletra “H”. I com es xifraria la “P”? Com que el seu valor numèric és 15, llavors: f(15)= 3·15 + 7 (mod 26) = 52 (mod 26) = 0, que correspon a la

lletra “A”. Si repetim aquest càlcul per a totes les lletres obtenim la taula següent:

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

(taula 2)

Malgrat tot, s’ha de tenir en compte que no totes les parelles *m*, *n* proporcionen una clau adequada. Per exemple, considerem *m = 8* i *n = 7*, de manera que l’algorisme de xifrat quedi *f(x)= 8x + 7 (mod 26)*. Si prenem la “D”, aquesta quedarà xifrada com f(3)= 8·3 + 7 (mod 26) = 31 (mod 26) = 5, que correspon a la lletra “F”. Si llavors prenem la lletra “Q”, quedarà xifrada com f(16)= 8·16 + 7 (mod 26) = 135 (mod 26) = 5, que també correspon a la F. Si ho provem amb la resta de lletres veurem que això es va repetint, i que la “A” es xifraria igual que la “N”, la “B” igual que la “M”, etc. Està demostrat[7] que, utilitzant un xifratge afí amb un alfabet de 26 lletres, els únics valors vàlids de *m* són el nombres senars de l’1 al 25 exceptuant el 13. No hi ha cap restricció pel que fa al valor de la *n*. Per tant, hi ha 12 · 26 = 312 codis diferents per als xifratges afins, contraposant-se als només 26 codis diferents del Juli Cèsar estàndard.

Es pot obtenir una altra variant de la xifra Juli Cèsar afegint-hi una paraula clau. L’algorisme consisteix en escriure la clau (per exemple, ESPANTAOCELLS) sense repetir les lletres (ESPANTOCL) i continuar escrivint les lletres de l’abecedari que falten en ordre alfabètic començant després de l’última lletra (ESPANTOCLMQRUVWXYZBDFGHIJK). L’alfabet resultant és el que s’utilitza per xifrar, de manera que, en l’exemple, la “A” s’escriuria com una “E”, la “B” com una “S”...

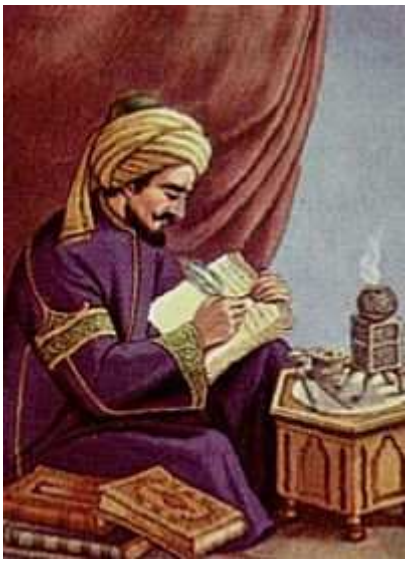
[7] [PER VEURE-HO I APLIAR CONEIXEMENTS SOBRE ELS CRIPTOSISTEMES AFINS VEURE ANNEXOS A i B]

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

(taula 3)

3.3.4. Anàlisi de freqüències

Per a poder desxifrar un mètode Juli Cèsar, es pot fer “per força bruta” (provant totes les claus fins que alguna funcioni), ja que hi ha molt poca quantitat de claus a escollir (n-1), o amb l’**anàlisi de freqüències**.



Abu-Yusuf Ya’qub ibn Ishaq al-Kindi. Font: *Google*

L’anàlisi de freqüències va ser el primer avenç important en el camp del criptoanàlisi. Va ser inventat pel filòsof àrab Al-Kindi al s. IX. Aquest mètode va fer inservibles els xifratges monoalfabètics (com el de Juli Cèsar), i consisteix en analitzar la freqüència amb la qual apareix una lletra en el text xifrat i relacionar aquesta freqüència amb la que presenta cada una de les lletres de l’alfabet de l’idioma que sigui. Per exemple, tant al castellà com al català les dues lletres més abundants són la “E” i la “A”, però la tercera lletra més freqüent és diferent a cada idioma. Al primer és la “O” i al segon la “S”. Això canvia també amb l’anglès, el francès o l’alemany.

3.3.5. Xifra de Polibi

Altres xifratges monoalfabètics menys coneguts, però que poden ser igualment trencats per anàlisi de freqüències són la **Xifra de Polibi** i la Xifra Pig Pen.

La primera es basa en crear una quadrícula de 5x5 amb totes les lletres de l’alfabet llatí estàndard (col·locant la “q” i la ”k” en un mateix quadre), i assignant a cada lletra

un codi de dos nombres, que corresponen a la seva posició a la quadrícula. El primer nombre indica la fila, i el segon indica la columna. Així:

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i	j
3	k/q	l	m	n	o
4	p	r	s	t	u
5	v	w	x	y	z

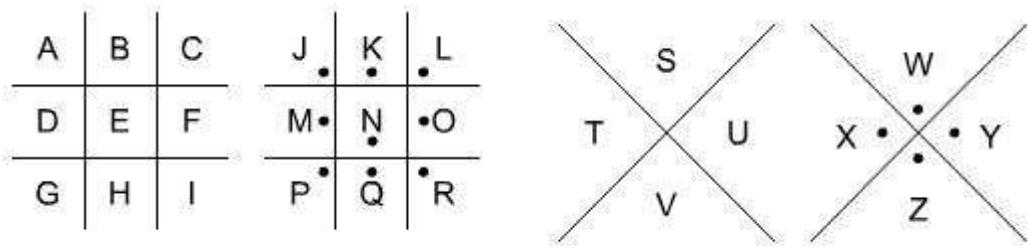
(taula 4)

Per tant, si volem escriure “quedem al parc a les cinc”, ho escriurem així “31 45 15 14 15 33 11 32 41 11 42 13 11 32 55 43 13 24 34 13”. Com ja hem dit abans, aquest xifratge es pot trencar molt fàcilment amb l’Anàlisi de freqüències. Però Polibi va ser el primer a esmentar aquest mètode, i ell visqué a Grècia durant el Segle III aC., mil dos-cents anys abans de la creació de l’anàlisi de freqüències. Per tant, la xifra de Polibi feia la seva feina. Evidentment, el mètode original no utilitzava l’alfabet llatí estàndard de vint-i-sis lletres, ni la numeració aràbiga.

3.3.6. Xifra Pig Pen

Una altra xifra monoalfabètica semblant a la de Polibi és la **Xifra Pig Pen** o “Pigpen”. Aquesta va ser inventada per Heinrich Cornelius Agrippa al s. XVI i es va fer servir durant com a mínim dos segles més, sobretot per part de la comunitat maçònica.

El mètode per a aconseguir la clau consisteix en dibuixar dues graelles de 3x3 i dues aspes creades amb dos segments. Llavors, a una de les aspes i a una de les graelles es dibuixa un punt a cada apartat, per tal de diferenciar-les de l’altra graella o aspa.



Per a xifrar el missatge, cada una de les lletres es substitueix pel fragment de graella o aspa que ocupa. D'aquesta manera, la paraula CALAIXERA queda xifrada així:

3.3.7. Xifra de Bacon

Una altra xifra monoalfabètica molt interessant és la **Xifra de Bacon** (s. XVI-XVII), que combina criptografia, usant un codi binari, i un mètode esteganogràfic ben curiós.

A	**aaaaa**	**H**	**aabbb**	**O**	**abbba**	**U**	**babaa**
B	**aaaab**	**I**	**abaaa**	**P**	**abbbb**	**V**	**babab**
C	**aaaba**	**J**	**abaab**	**Q**	**baaaa**	**W**	**babba**
D	**aaabb**	**K**	**ababa**	**R**	**baaab**	**X**	**babbb**
E	**aabaa**	**L**	**ababb**	**S**	**baaba**	**Y**	**bbaaa**
F	**aabab**	**M**	**abbaa**	**T**	**baabb**	**Z**	**bbaab**
G	**aabba**	**N**	**abbab**				

(taula 5)

Francis Bacon. Font: *Wikipedia*

Per amagar el missatge s'escriu un text innocent i, entre cada línia i a sota de cada lletra el missatge secret codificat. Després la lletra que queda a sobre de cada **b** del codi l'escrivia de forma diferent (amb majúscula, cursiva, negreta...). D'aquesta manera cada lletra normal es traduiria com una **a** i cada lletra especial com una **b**.

Així, si volem codificar la paraula CRIPTOGRAFIA, seguiríem aquest procés:

- Primer es codifica cada lletra amb el codi binari:

C R I P T O G R A F I A

aaa**b**a **b**aaa**b** a**b**aaa a**bbbb** **b**aa**bb** a**bbb**a aa**bb**a **b**aaa**b** aaaaa aa**b**a**b** a**b**aaa aaaaa

- Llavors s'escriu una frase innocent i se separa el text xifrat en blocs de la llargada de les paraules:

De moment, crec que en aquesta frase no hi ha cap paraula amagada, sí, de debò.

Aa a**b**a**b**aa a**b**a**b** aaa a**b** **bbbb**aa**b** **b**a**bbb** aa a**b** **b**a **b**aa a**b**aaaaa aa**b**a**b**a**b** aa aa aaaa

- Ara s'escriu la frase innocent una altra vegada, però fent que les lletres que corresponen a les "b" tinguin un tret distintiu, en aquest cas escrivint-ho en negreta, però en un cas real es pot fer de forma més subtil, com dibuixant un petit punt al costat de cada lletra "b":

Aa a**b**a**b**aa a**b**a**b** aaa a**b** **bbbb**aa**b** **b**a**bbb** aa a**b** **b**a **b**aa a**b**aaaaa aa**b**a**b**a**b** aa aa aaaa

De m**o**m**e**nt, c**r**e**c** que e**n** **aque**st**a** **f**r**ase** no h**i** **h**a **c**ap p**a**raula am**a**g**a**d**a**, sí, de debò.

Per a desencriptar-la només es fa el procés a la inversa, tenint en compte que els blocs d'"a"s i "b"s són de cinc dígits.

3.3.8. Increment de la seguretat combinant tècniques

Tant "Xifra de Pig Pen" com la "Xifra de Polibi", presenten l'inconvenient de no poder canviar la clau, igual que amb la Xifra Atbash. És a dir, ambdues xifres sempre utilitzen el mateix codi. Per tant, a la facilitat de desxifrar el codi a través de l'anàlisi de freqüències, se li afegeix el fet que si l'enemic descobreix la clau a través d'algun dels usuaris o d'un llibre de codis, el mètode ja no es pot tornar a utilitzar perquè la clau ja és coneguda per l'enemic. Per això, és molt important en la utilització de la criptografia clàssica (abans de l'informàtica) mantenir fortament el secret combinant tècniques.

Per exemple, es pot combinar la “Xifra de Polibi” amb la “Xifra de Bacon”, convertint els nombres amb els quals es xifren les lletres amb al primer mètode al codi binari. D’aquesta manera, la A (11 amb Polibi) seria 001011, la B (12) seria 001100, i així fins a la Z, que seria 110111. Llavors, tal com amb Bacon, s’escriu un text innocent en un full de paper, i a les lletres a les quals les correspon un 1, s’hi escriu amb tinta invisible una marca. Llavors es lliura el missatge (el text xifrat) al receptor, d’alguna manera discreta, com per exemple introduint el missatge a la seva butxaca enmig de la multitud.

D’aquesta manera es fa molt complicat que algú s’assabenti del contingut de la carta, ja que, a més a més d’utilitzar una Xifra (en aquest cas la combinació de dues), es combina amb l’esteganografia, tant amb la tinta invisible com amb el fet d’entregar el missatge secretament.

3.3.9. Xifra ADFGVX

Un altre exemple d’una Xifra que combina mètodes (com la Xifra de Bacon) és la **Xifra ADFGVX**, emprada pels alemanys durant la Primera Guerra Mundial. Aquesta Xifra barreja un mètode de transposició amb un de substitució. S’utilitzaven les lletres “ADFGVX” perquè aquestes són prou diferents al Codi Morse (els missatges es transmetien per telègraf) per no donar peu a confusions. El xifratge consta de dues fases:

La fase de **substitució** consisteix en crear una graella de 6x6 amb les 26 lletres de l’alfabet llatí estàndard (la lletra “ß” de l’alfabet alemany es substituïa per una “ss”) i els números del 0 al 9 ordenats com es vulgui, per exemple així:

	A	D	F	G	V	X
A	n	1	t	9	f	r
D	g	a	3	s	m	4
F	8	p	h	2	y	d
G	v	j	5	b	u	0
V	k	c	6	o	x	i
X	q	z	l	7	e	w

(taula 6)

Llavors es substitueix cada símbol de la mateixa manera que amb la “Xifra de Polibi”, primer escrivint la lletra de la fila i llavors la de la columna. D’aquesta manera, la frase “Demà a les 8 al parc” es codifica així: FX XV DV DD DD XF XV DG FA DD XF FD DD AX VD.

Ara és quan comença el xifratge de **transposició**. S’escull una paraula clau, en aquest exemple usarem “CLAU”. En aquest pas es segueix aquest procés:

1. S’escriu cada parell de lletres de la codificació a sota de cada lletra de la clau.

2. Si cal, s’acaba d'omplir la taula amb un signe que no trenqui el sentit. Pot ser un signe inventat o no (hi posaré un “0”, que a la graella anterior era GX):

C	L	A	U
FX	XV	DV	DD
DD	XF	XV	DG
FA	DD	XF	FD
DD	AX	VD	GX

3. S’ordenen les lletres de la clau alfabèticament i es reordenen les columnes segons l'ordre alfabètic anterior:

A	C	L	U
DV	FX	XV	DD
XV	DD	XF	DG
XF	FA	DD	FD
VD	DD	AX	GX

4. Es copia horitzontalment cada columna, i s'obté el text xifrat:

DV XV XF VD FX DD FA DD XV XF DD AX DD DG FD GX

Per a **descodificar** el missatge, primer de tot es fa una graella ordenant la paraula clau (CLAU) per ordre alfabètic (ACLU). Tot seguit es separa el text xifrat en blocs de longitud "L", on "L" és la quantitat de parelles de lletres al text xifrat (16) dividida per les lletres de la paraula clau (4). Aquest blocs de longitud "L" (4) es distribueixen verticalment a cada columna:

A	C	L	U

A	C	L	U
DV	FX	XV	DD
XV	DD	XF	DG
XF	FA	DD	FD
VD	DD	AX	GX

Llavors s'ordenen les columnes segons el seu ordre com a paraula clau, i en aquest moment s'escriuen les parelles de lletres segons el seu ordre a les files. Ara només queda substituir cada parella de lletres pel símbol que li pertoqui segons la taula 6.

C	L	A	U
FX	XV	DV	DD
DD	XF	XV	DG
FA	DD	XF	FD
DD	AX	VD	GX

FX XV DV DD DD XF XV DG FA DD XF FD DD AX VD GX

DEMAALES8ALPARC0

Demà a les 8 al parc ϴ

Però aquest mètode, tot i combinar diferents maneres de xifrar, és fàcil de desxifrar per un criptoanalista professional, el qual, gràcies a l'anàlisi de freqüències d'Al-Kindi, seria capaç de trencar el procés de substitució. Llavors, la ruptura de la xifra tan sols consisteix en resoldre un senzill anagrama.

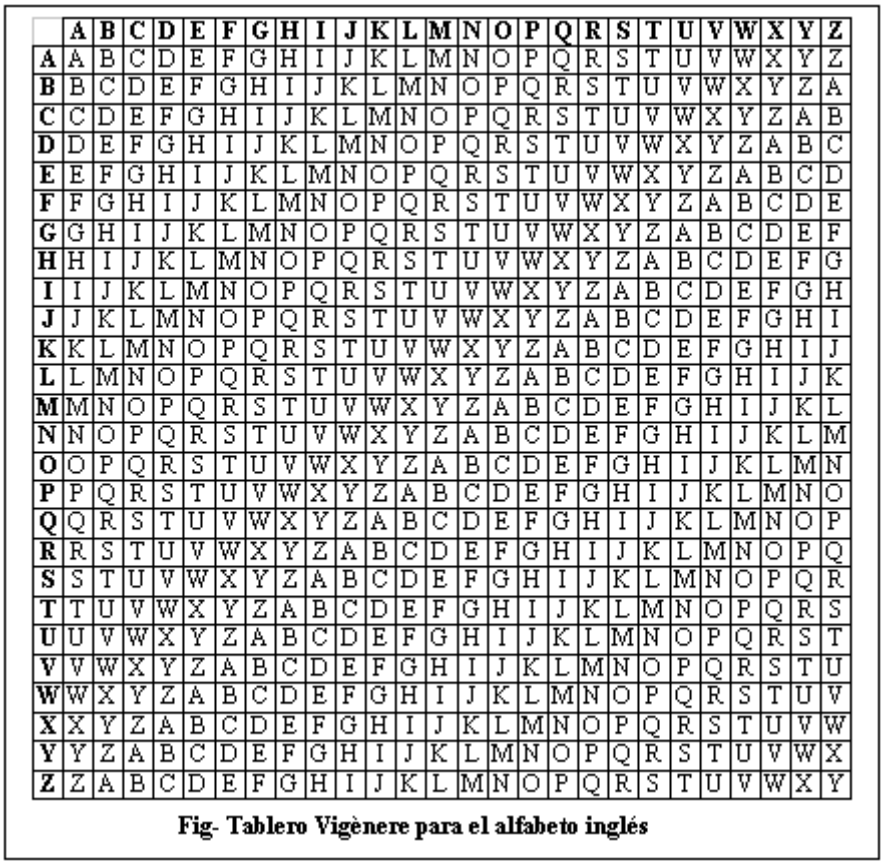
3.4. Xifratges de substitució polialfabètics

3.4.1. Xifra de Vigenère. *Le chiffre indéchiffrable*

Per això, al segle XVI el francès Blaise de Vigenère va millorar unes idees del segle anterior de l'artista-matemàtic italià Leon Battista Alberti. Vigenère va publicar un llibre titulat *« Traité des chiffres où secrètes manières d'écrire »* on explicava una forma de xifratge polialfabètic. Aquest mètode, que anomenaré a partir d'ara **Xifra de Vigenère**, va ser la primera xifra polialfabètica coneguda. Això va ser un gran avenç en la criptografia, ja que d'aquesta manera la "A" unes vegades era codificada com una "T", unes altres com una "H", però, ¡atenció!, no sempre la "T" o la "H" representarà la "A".

Blaise de Vigenère. Font: *Wikipedia*

Per a utilitzar la Xifra Vigenère primer de tot fa falta tenir un Quadre de Vigenère, de 26x26, on a cada línea s'escriu l'alfabet però cada cop començant amb la lletra de després. D'aquesta manera, el primer alfabet comença amb la "A", el segon amb la "B", etc.



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

Fig- Tablero Vigènere para el alfabeto inglés

(taula 7)

Un cop tenim el quadre fet, procedim a encriptar la frase “De moment, crec que en aquesta frase no hi ha cap paraula amagada” (que he usat quan he explicat la Xifra de Bacon) seguint aquest passos:

1. S'ha de decidir una paraula clau. Jo utilitzaré “PARET”. Aquesta paraula només l'han de conèixer la persona emissora i la receptora.

2. Eliminem els signes de puntuació i llavors escrivim el text pla en majúscules (per tal de facilitar-ne la transcripció):

De moment, crec que en aquesta frase no hi ha cap paraula amagada

DE MOMENT CREC QUE EN AQUESTA FRASE NO HI HA CAP PARAUL A AMAGADA

3. A sota de cada lletra del missatge es va repetint la paraula clau:

DE	MOMENT	CREC	QUE	EN	AQUEST	FRASE	NO	HI	HA	CAP	PARAULA	AMAGADA
PA	**RETPAR**	**ETPA**	**RET**	**PA**	**RETPARE**	**TPARE**	**TP**	**AR**	**ET**	**PAR**	**ETPARET**	**PARETPA**

4. Per a codificar el missatge, només fa falta substituir cada lletra del text pla per la que li toca quan s'aparella amb la lletra de la paraula clau. D'aquesta manera, la primera lletra del text pla és una "D" que s'aparella amb una "P", per tant, la lletra que li pertoca és la "S":

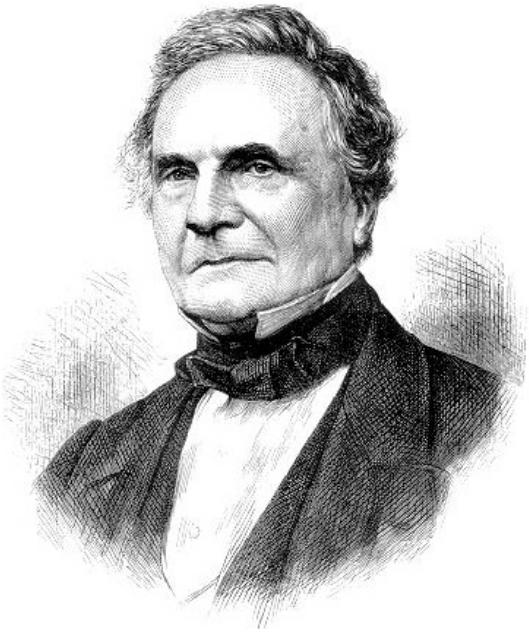
SEDSF TNKGK TCHYX TNRUN TSKEY GAJIG DHZLT RAGTT GALPT PMRKT SA

Gràcies al xifratge polialfabètic, la "M" es xifra en aquest cas unes vegades com una "M" i d'altres com una "D" o una "F"; i la "T" al text xifrat xifra quatre cops a la lletra "E", quatre més a la "A" i un cop a la "P".

3.4.2. Atac de Kasiski

Durant molt de temps es va pensar que la Xifra Vigenère era indesxifrable, fins que a mitjans del s. XIX arribaren F.W. Kasiski i Charles Babbage. De forma independent, tant el general prussià com el matemàtic anglès, ambdós també criptoanalistes, van saber per on vèncer la Xifra.

El que era fonamental d'esbrinar en la Xifra de Vigenère era la clau. Però la clau té dues característiques: la longitud de la paraula i les lletres concretes que la formen.



Charles Babbage. Font: *Google*

D'aquesta manera, l'**Atac de Kasiski** a la Xifra Vigenère segueix aquest passos:

- 1a fase: Com saber la longitud de la clau

- Si un missatge és prou llarg és possible que determinats grups de lletres, per exemple la paraula QUE, coincideixi alguna o algunes vegades sobre el

mateixos llocs de la paraula clau, per tant quedaran codificats també amb les mateixes lletres.

- Podem buscar uns quants casos i anotar quina distància en lletres els separen.
- Aquesta distància ha de ser, forçosament, un múltiple de la longitud de la clau.
- Quantes més repeticions tinguem, ja sigui d'un mateix grup o de grups diferents, millor, perquè tindrem més informació
- La clau serà un divisor comú de totes aquestes distàncies.

Observem un exemple per desxifrar aquest text, en el qual he marcat unes quantes repeticions:

YHXEK IGLXZ GUYEM EWLQZ RUYXG IFNED TCPRK VIMEI YHAEJ XICED FYWWV YLLQR XXPBR MMWMM EXTVR ZYFVV WCUSR GIYWV KOPMO SWZQG XUCIC WMPYJ BUTWV RGPRP WXPGZ RWDIX SHDQV RXZRR VUFRR PUBYR PWZWR IFAEJ XICGF RNPWK EUQMI QUEMM EGPRK XIETV RMLRK IHWEZ QJZWJ MVTPZ XUEHL RWZQG XUEKV XUYVR TCOTV VIGIK EKFMH YYPPD ENPQR XCNIJ GIYGV RNCEZ EVLRJ HYWWT MHNWV KIYWC MWZQL RCNER PJLWK SLBYV EFCED ENSMY EPTEK VYDGV RNDUL ELLRK EHZYO ECDIC TUDXF VPLLR ZYCHR GWPTK ELBYV IFXEK IGLXZ GBLZZ EAFEE CUEMV WUTBZ GIXEH YYDXT ELCIX EYWWV YAFEE CUWIJ TUEPC ECNSD IHNER GUXME ELESK GIYXV RNAII SYWTR WNZVV WGLTV VXFXG IFBYV EWLFR ZUOIM IOCIT VCOER PGLXV QUEMT IMNSC XCAEI MZLVR IFQEM SLOIK SLYEI QYPPX SM

Si busquem totes les repeticions de grups de 3, 4, 5 o 6 lletres podem obtenir una taula de distàncies de repetició, totes múltiple de la llargada de la clau.

Al text superior la clau és de **5 lletres**, ja que 5 és el màxim comú divisor entre les diferents repeticions que hi apareixen, que són de: 375, 150, 370, 175, 120 i 200.

- 2a fase: trobar la paraula clau

Sabem que la clau té cinc lletres i, per tant, que s'han fet servir, ordenadament, cinc alfabets diferents. Cada cinc lletres estan ordenades amb el mateix alfabet:

- **Grup 1**: lletres 1, 6, 11, 16, 21...
- **Grup 2**: lletres 2, 7, 12, 17, 22...
- **Grup 3**: lletres 3, 8, 13, 18, 23...
- **Grup 4**: lletres 4, 9, 14, 24, 29...

- **Grup 5**: lletres 5, 10, 15, 20, 25...

El que s'ha de fer ara és separar cada grup de lletres, fer a cada grup el seu anàlisi de freqüències i buscar a quina fila de la taula de Vigenère correspon. Així, descobrim que la clau del text anterior era "**EULER**", i que si el desxifrem ens surt això:

UNMAT EMATI CANAV ACAMI NANTP ELCAM PIENT ROBAR UNPAS TORAM BELSE URAMA TDEXA ISLIV ADIRA VEURE SIJOA CONSE GUEIX OCOMP TAREL SSEUS XAISE NMENY SDECI NCSEG ONSME NDONA RAUNA LAQUA LCOSA ELPAS TORCO NTEST AAFIR MATIV AMENT TOTPE NSANT ENLAI MPOSS IBILI TATDU NCOMP TATGE TANRA PIDPE ROVET AQUIQ UEELM ATEMA TICES CONCE NTRAI ABANS DELSC INCSE GONSL ICOMU NICAA LPAST ORQUE ALRAM ATHIH AVIAT RESCE NTSQU ARANT ANOUX AISEL PASTO RVAHA VERDA CCEPT ARQUE ELMAT EMATI CHAVI AGUAN YATIE SAIXI COMAQ UESTC ARREG AELSE UGUAN YALES PATLL AICOM ENCAA CAMIN ARTOT CONTE NTPER OELPA STORE SMAPE RDUTP ELQUE ACABA VADEV EUREC RIDAA LMATE MATIC ESCOL TIPAR IFARA ELFAV ORDET ORNAR MEELG OS

Ara només fa falta ajuntar les lletres en paraules i posar punts, comes i accents per tal de fer el text còmode de llegir, i ens apareix un acudit de matemàtics:

> Un matemàtic anava caminant pel camp, i en trobar un pastor amb el seu ramat de xais li va dir: "A veure, ¿si jo aconsegueixo comptar els seus xais en menys de cinc segons me'n donarà un?" A la qual cosa el pastor contestà afirmativament, tot pensant en la impossibilitat d'un comptatge tan ràpid. Però vet aquí que el matemàtic es concentrà i abans dels cinc segons li comunicà al pastor que al ramat hi havia "tres-cents quaranta-nou xais". El pastor va haver d'acceptar que el matemàtic havia guanyat, i es així com aquest carregà el seu guany a l'espatlla i començà a caminar tot content. Però el pastor, esmaperdut pel que acabava de veure, crida al matemàtic: "Escolti!!! Pari!!! Farà el favor de tornar-me el gos?!"

Davant d'això, podem preguntar-nos: ¿com es pot contraatacar a l'atac de Kasiski? Com que el punt feble del qual s'aprofita aquest atac és la longitud de la clau, hem de reforçar-la. Podem fer-ho de diverses maneres:

- **La clau infinita**

Si tenim una clau tan llarga com el propi text no ens la podran trobar. Però, com aconseguir una clau prou llarga? Un bon truc és fer servir la mateixa pàgina de la mateixa edició d'un llibre. Per exemple, ens podem posar d'acord en utilitzar el llibre "El caso Bourne" de *Robert Ludlum* en l'edició de *Debolsillo* de l'any 2009. Això només ho sabem les dues persones interessades. Al començament del missatge només caldria escriure un 79 per entendre que la clau és la pàgina 79 del llibre. Amb aquest truc la clau serà:

DADSEPROLONGABANUEVAMENTEYALLIENELESCENARIOFRENTEAELLOSPORENCIMADEELLOS...

Encara que aquesta clau és molt llarga la millor seria una clau infinita. No la tenim, però ens hi acostem.

- **La clau a l'atzar**

Els criptoanalistes tenen molta paciència i si pensem que la clau són paraules conegudes podem fer proves fins trobar el llibre-clau. A més la llengua repeteix paraules (que, de, en...) que, per força es repetiran a la clau. Seria molt millor una clau a l'atzar. Tot i així, utilitzar una clau a l'atzar comporta l'inconvenient de que és impossible de recordar i pesada d'utilitzar

Aquesta manera és la que utilitza la **Xifra de Vernam**, la clau de la qual es transmet en secret gràcies a la criptografia quàntica, tema del qual parlaré a la següent part del treball.

3.4.3. Xifra de Playfair

Un altre Xifra polialfabètica bastant coneguda és la **Xifra de Playfair**, inventada el s. XIX per Charles Wheatstone. Per utilitzar-la s'han de seguir aquests passos. El text pla és la paraula "CRIPTOGRAFIA":

1. Es tria una paraula clau que només sabran les persones interessades en el secret. Jo utilitzaré PLAYFAIR.

2. Es fa un alfabet en una quadrícula de 5x5 començant per posar les lletres de la paraula clau (sense repeticions). S'acaba d'omplir, ordenadament amb les lletres que falten de l'alfabet. Com que la quadrícula té 25 caselles i hi ha una lletra que no hi cap es pot fer una casella doble (per exemple I/J) o ometre una lletra. Jo ometré la "w".

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

(taula 8)

3. Es separen les lletres del missatge per codificar de dues en dues. Si falta una lletra, al final s'afegeix una lletra qualsevol. Important! Si en fer parelles queden dues lletres iguals, per exemple a *carreta* (CA **RR** ET AX) es separen amb una X (CA **RX R**E TA)

CR IP TO GR AF IA

4. Per codificar cada lletra s'agafa cada parella i s'apliquen aquestes regles:

   - **Regla 1:** Si les dues lletres de la parella són a la mateixa línia s'agafa la de la dreta de cadascuna. Si una de les lletres és l'última de la fila s'agafa la primera:

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

Pla: GJ **Xifrat:** HK

- **Regla 2:** Si són a la mateixa columna s'agafen les de sota. Si una de les lletres és la de sota de tot s'agafa la de dalt:

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

Pla: ZK **Xifrat:** FS

- **Regla 3:** Si són en línies diferents s'agafen les que "tanquen el rectangle" i cada lletra es canvia per la de la seva fila.

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

Pla: RZ **Xifrat:** DU

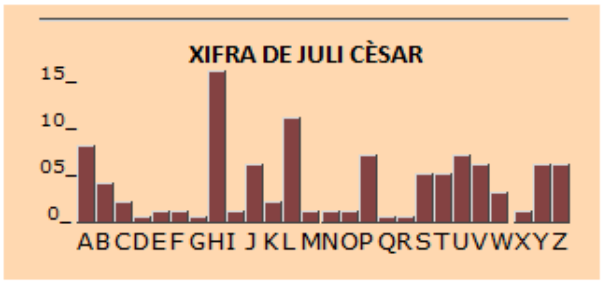
- Seguint aquest algorisme, “CRIPTOGRAFIA” es xifraria així:

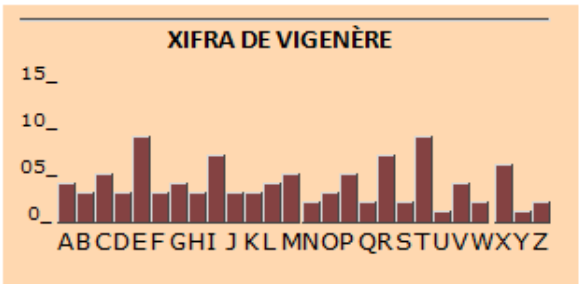
CR	IP	TO	GR	AF	IA
DB	EI	VM	NG	YP	BP

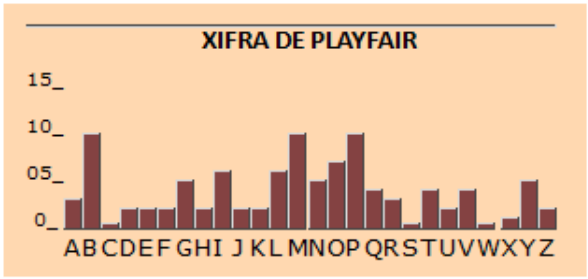
Charles Wheatstone. Font: *Google*

Aquí podem veure el mateix que presentava la Xifra de Vigenère. La “R”, per exemple, es xifra un cop com a una “B” i un altre com una “G”. I la “P” del text xifrat, un cop substitueix a una “F” i un altre a una “A”.

Podem comparar també com queda la gràfica d'un text xifrat (en aquest cas xifraré l’acudit que he desxifrat abans amb Kasiski) amb una Xifra monoalfabètica, la de Juli Cèsar, i amb dues polialfabètiques, la de Playfair i la de Vigenère. Es pot veure que als codis polialfabètics les freqüències queden més igualades, no hi ha barres tan llargues.







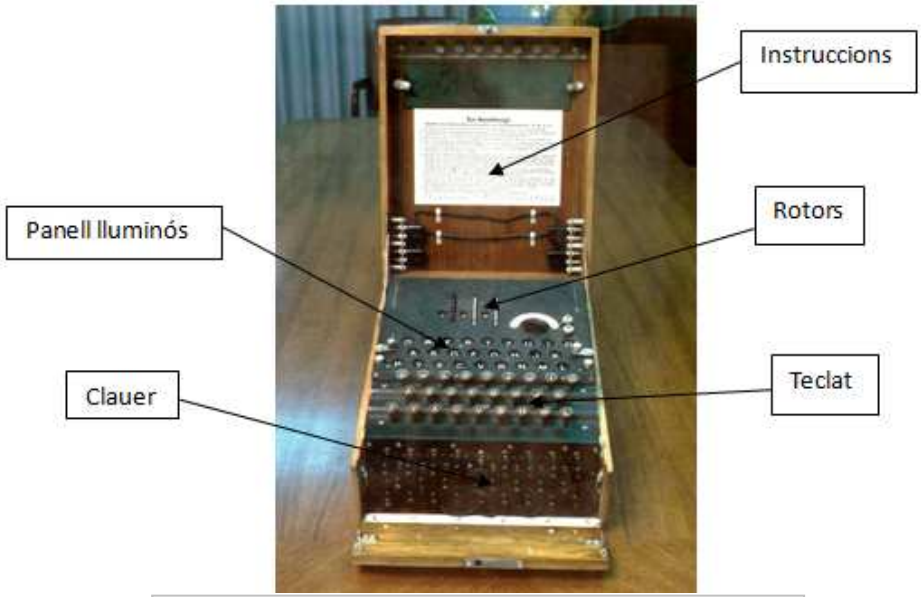
Font: elaboració pròpia

3.4.4. La Màquina ENIGMA

La segona guerra mundial va ser el marc perfecte per al desenvolupament de la criptografia i la criptologia. Els EUA, per exemple, van emprar (i amb gran enginy), indis navajo com a operaris de ràdio. Com que l'idioma navajo només era conegut per aquests indis, els japonesos mai van poder desxifrar les comunicacions nord-americanes. Malauradament, molts d'aquests indis eren víctimes del racisme per part dels seus camarades malgrat que desenvolupessin una tasca molt important.

En qualsevol cas, sense cap mena de dubte la Xifra més famosa usada durant la Segona Guerra Mundial és la **Màquina Enigma**. Els alemanys creien que era indesxifrable però un equip de criptoanalistes britànics a Bletchey Park, on matemàtics i criptògrafs treballaven pels aliats, van poder trencar la xifra. Aquest fet es creu que va acurtar la durada de la guerra en dos anys.

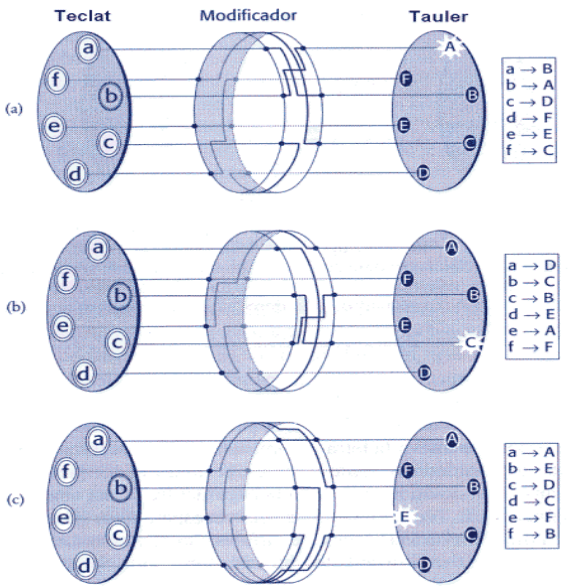
La màquina Enigma, a més a més, tenia l'avantatge que podia ser transportada per un sol home i que el seu ús era molt senzill. Només feia falta pitjar una lletra al teclat (ordenat com qualsevol altra màquina d'escriure alemanya) i el panell lluminós indicava quina era la lletra en el text xifrat.



Màquina Enigma. Font: *Google* i formatejat propi

La màquina Enigma estàndard (la utilitzada per la Wehrmacht) constava de tres rotors. Aquests rotors connectaven cada punt d'entrada amb un altre de sortida descol·locat respecte al primer. Cada vegada que es picava una lletra el modificador girava una posició. La imatge et presenta un esquema amb només sis lletres, però els rotors de l'Enigma en tenien 26.

El funcionament de l'Enigma de tres rotors era aquest: quan el primer havia completat una volta feia girar una posició al següent. D'aquesta forma els rotors no tornaven a estar en la mateixa posició fins a 26x26x26 moviments: 17.576 girs. Pel mateix criteri hi ha 17.576 posicions inicials possibles dels tres modificadors. Cada posició és una clau específica: **F-G-P** significaria posar el primer en **F**, el segon en **G** i el tercer en **P**.



Esquema del funcionament dels rotors de l'ENIGMA. Font: *The Code Book*

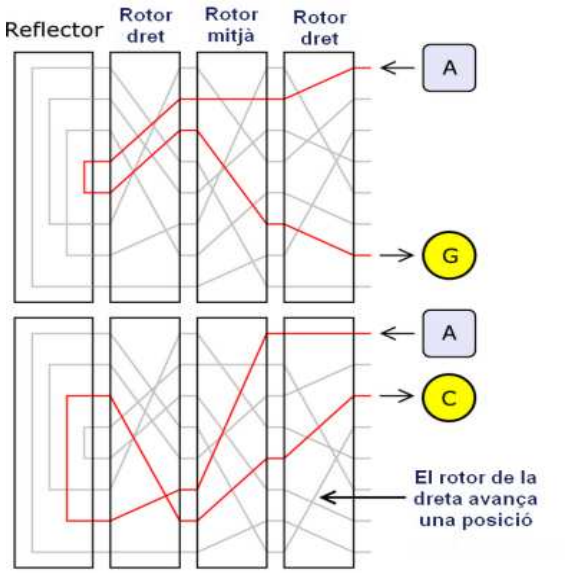
Els rotors, però, eren intercanviables; si en tenim tres[8], hi ha sis disposicions possibles (1-2-3, 1-3-2, 2-1-3, 2-3-1, 3-2-1, 3-1-2). D'aquesta manera es multipliquen per 6 les possibilitats inicials (6x17.576 = 105 456 possibilitats).

A més la màquina tenia un clauer que permetia alterar el teclat de forma que la A es convertís en G (i la G en A) o la B en U (i la U en B). Es podien intercanviar sis parells de lletres, la qual cosa dóna més de cent milions de formes diferents! Si això ho multipliquem per les posicions possibles dels rotors ens surt ¡més de 10 bilions (10^{13})

[8] Més tard, a l'Enigma de la Wehrmacht se li van afegir dos rotors més, passant a ser 60 les diferents disposicions de l'ordre en què es trobaven els rotors.

de possibilitats! Per això, la màquina Enigma usada per l'Armada alemanya que disposava de 5 posicions per als rotors, va ser indesxifrable durant molt de temps.

Al final del camí dels modificadors hi havia un reflector que feia a tornar passar el corrent en direcció contrària per encendre la bombeta del panell lluminós.



Esquema del funcionament dels rotors de l'ENIGMA amb el reflector. Font: *Google*

La cosa no acabava aquí; l'exèrcit alemany disposava d'un llibre de claus per determinar la posició inicial del dia de clauers i rotors. Però al començament del missatge s'enviava un codi de tres lletres que indicava com reorientar els rotors per descodificar la resta del missatge. **Aquest codi de tres lletres s'escrivia dues vegades per a confirmar-lo**. És a dir:

- El codificador posava tota la màquina en la posició del dia que indicava el llibre de claus. Per exemple: **213 – PKO – AD, ES, NM, OF, YC, PL**. Això significava que el rotor número 2 es col·locava en primer lloc, l'1 en segon lloc i el 3 en el tercer; que les primeres lletres de cada rotor eren P, K i O respectivament; i que al clauer de la màquina s'intercanviaven les lletres esmentades anteriorment (A per D i a la inversa, E per S i a la inversa, etc.).

- Escollia unes noves lletres inicials per a cada rotor, per exemple ZFD. Llavors teclejava (encara amb la clau del dia) ZFDZFD (l'aspecte del qual podia ser CHFMIS).

- Col·locava els rotors orientats en ZFD i codificava la resta del missatge.

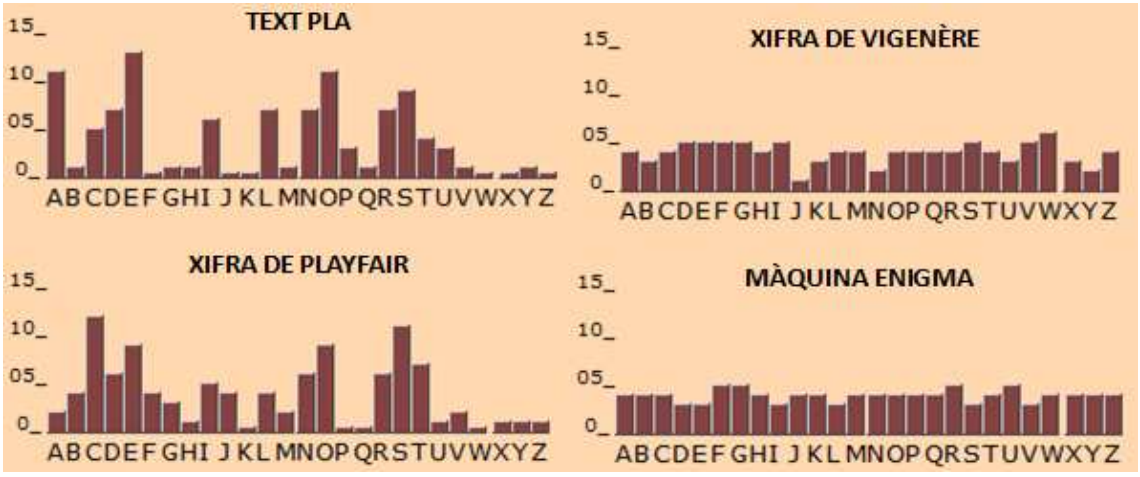
Per a descodificar es repetia la operació a la inversa:

- El descodificador posava tota la màquina en la posició del dia, **213 – PKO – AD, ES, NM, OF, YC, PL**.

- Descodificava les sis primeres lletres i li sortia una seqüència repetida, en l'exemple ZFDZFD.

- Col·locava els rotors orientats en ZFD i descodificava la resta del missatge.

La màquina Enigma aconseguia que l'anàlisi de freqüències del text xifrat sortís gairebé uniforme. Tot seguit mostro l'anàlisi de freqüències d'un text (Articles del 10 al 13 de la Constitució Espanyola de 1978, 1622 lletres) xifrat amb la Xifra de Playfair, amb la Xifra de Vigenère (ambdues amb clau ESTERNOCLEIDOMASTOIDAL) i amb la màquina Enigma (clau: 213 – PKO – AD, ES, NM, OF, YC, PL):



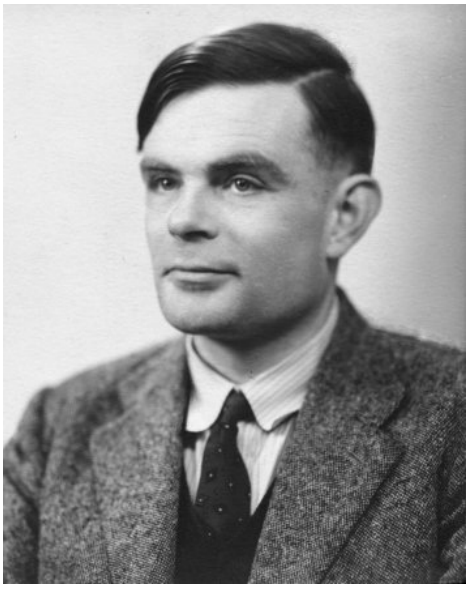
Font: elaboració pròpia

Podem apreciar, doncs, com les freqüències de la màquina Enigma són gairebé uniformes, i que cap lletra destaca sobre una altra.

Tot i així, l'Enigma presentava dos punts dèbils, que van saber aprofitar molt bé l'equip de criptoanalistes de Bletchey Park, a Londres.

El primer d'ells era la repetició de la clau temporal a l'inici del missatge, i aquest punt feble va ser molt utilitzat pels criptoanalistes durant els primers anys de la utilització de la màquina. A causa de la repetició, si un criptoanalista es trobava amb un text que començava per QNYGHX sabia que la "Q" i la "G" xifraven a una mateixa lletra però avançant la posició dels rotors en tres llocs, i passava el mateix amb la "N" i la "H" i amb la "Y" i la "X". Com que els analistes ja disposaven de diverses màquines Enigma i dels seus jocs de rotors, trobar la clau usada en aquell missatge es convertia en una tasca possible. Això sí, s'ha de dir que no provaven totes les claus possibles a mà, sinó que disposaven d'unes enormes màquines que anaven provant tots els codis possibles, anomenades *Bombes*. Són els antecedents dels moderns ordinadors.

Quan l'Estat Major alemany es va assabentar que la repetició de la clau temporal a l'inici de cada missatge era un punt dèbil en el xifratge de l'Enigma, va donar l'ordre que aquest pas en el procés d'utilització de la màquina es deixés de fer, la qual cosa va provocar més maldecaps als criptoanalistes de Bletchey Park.



Alan Turing. Font: *Google*

El segon punt dèbil era el fet que, degut al reflector, una lletra mai es podia xifrar com a ella mateixa. Els experts de Bletchey Park, més concretament el gran matemàtic anglès Alan Turing, van observar que els primers missatges de cada dia donaven informacions meteorològiques. Per tant hi havia tot un conjunt de paraules (temps, vent, temperatura...) que normalment hi apareixerien. A aquestes paraules especials els criptoanalistes les anomenen

puntals. Llavors s'havia de buscar un lloc on el *puntal* (per exemple TEMPERATUR – "temperatura" en alemany) no coincidís amb cap lletra igual. Si es pensava que la paraula apareixia al començament del text la recerca es començava per aquí. A partir del joc d'equivalències obtingut, les *bombes* es posaven a treballar per poder esbrinar la posició dels modificadors, cosa que feia possible desxifrar la resta dels missatges.

Tota la informació sobre la gesta dels criptoanalistes de Bletchey Park no es va descobrir al món fins més de 15 anys després de la fi de la guerra.

3.5. Epíleg

Els diferents tipus de xifratges que he explicat tan sols són un esbós de la gran quantitat de xifratges diferents que existeixen. Per això, només he agafat els més importants o que més van transcendir en la història.

De fet, podem fer servir tècniques molt més senzilles que utilitzar una xifra "amb nom i cognoms" (p.e. la de Polibi o la Vigenère) per amagar informació, com ara escriure en un altre alfabet (com ara el ciríl·lic o el grec) o parlar en una altra llengua. S'ha de dir, però, que això només es pot fer quan el que volem xifrar són missatges amb poca importància, que de ben segur no seran analitzats per criptògrafs (com per exemple textos secrets entre amants, tal i com recomana el Kamasutra). Si ho fem amb missatges d'una importància cabdal (com ara missatges militars o polítics) hem d'estar molt segurs que la llengua que utilitzem és pràcticament desconeguda, com van fer els Estats Units amb els indis navajo durant la Segona Guerra Mundial. En cas contrari, els nostres missatges seran llegits lliurement per l'enemic. Això els va passar als russos, que, durant la Primera Guerra Mundial, van creure amb molta supèrbia que no tenien cap necessitat de xifrar els seus missatges perquè el rus seria inintel·ligible als

ulls dels seus enemics de la Triple Aliança[9]. No fa falta dir que els missatges de l'Imperi Rus eren llegits amb tota tranquil·litat tant per part dels seus enemics com dels seus aliats.

De tota manera, no tots els codis serveixen per ocultar missatges. Aquest és el cas del Codi Morse, l'Alfabet Braille, les diferents Llengües de Signes per als sordmuts, l'Alfabet Fonètic de l'OTAN, les Banderes de Signes, etc. Tots aquests codis tenen un ús en l'àmbit públic i s'utilitzen per a substituir diferents llengües o alfabets quan aquests no poden ser usats de forma tradicional.[10]

A la fi de la Segona Guerra Mundial, va aparèixer una nova tecnologia que canviaria el panorama de la criptografia per sempre, la informàtica. Gràcies a aquest nou invent, la facilitat en el procés de la ruptura d'un missatge ja no depenia de la velocitat de treball del criptoanalista, sinó que depenia (i encara en depèn) de la potència de l'ordinador emprat. Amb aquesta nova eina, la ruptura de l'Enigma hauria sigut tan fàcil com provar les més de deu bilions (10^{13}) de claus possibles utilitzant la computadora més potent de l'actualitat, el "Roadrunner" d'IBM, que pot realitzar més de mil bilions (10^{15}) de càlculs per segon.

Això és només un exemple del canvi tan brusc que va suposar l'aparició de la informàtica per a la criptografia. Ja no es tractava de mantenir l'algorisme del sistema el més amagat possible, sinó de trobar aquell sistema que tan sols es pogués trencar coneixent la clau. Era el naixement de la criptografia moderna.

[9] Aliança entre l'Imperi Alemany, l'Imperi Austrohongarès i Itàlia (tot i que més tard va canviar de bàndol, passant a substituir-la l'Imperi Otomà) durant la Primera Guerra Mundial. Era l'aliança de països enemiga de la Triple Entesa, constituïda pel Regne Unit, França i l'Imperi Rus (que més tard es va retirar a causa de la Revolució russa), als quals s'hi van afegir més tard els Estats Units i Itàlia.

[10] [PER A VEURE UNA DESCRIPCIÓ DE CADA UN DELS CODIS VEURE ANNEX C]

4. CRIPTOGRAFIA MODERNA

4.1. Teoria de la informació i principi de Kerckhoffs

El 1948, Claude E. Shannon publica l'article *A mathematical theory of communication* al *Bell System Technical Journal*, que constitueix l'acta de naixement de la teoria de la informació. L'any 1949 Shannon aplica la seva teoria a la criptografia en l'article *Communication theory of secrecy systems*. En aquests treballs, l'enginyer i matemàtic nord-americà aconsegueix definir de forma rigorosa la noció de *quantitat d'informació*. Si reflexioneu, trobareu certament difícil intentar mesurar la quantitat d'informació o calcular-la amb una fórmula. Shannon ens aconsegueix resoldre aquest problema. Abans, però, he de definir un concepte que és essencial en la criptografia, però sobretot en la criptografia moderna, en la qual els diferents algorismes d'encriptació existents són fàcilment coneguts arreu del món.

4.1.1. Principis de Kerckhoffs

Auguste Kerckhoffs (1835-1903), fou un lingüista i criptògraf holandès que ensenyà alemany a l'Escola Parisenca d'Estudis Comercials Avançats. És conegut per la seva publicació *La Cryptographie Militaire* (1883), on va fixar els sis principis sobre com ha de ser un xifratge pràctic:

Auguste Kerckhoffs. Font: *Google*

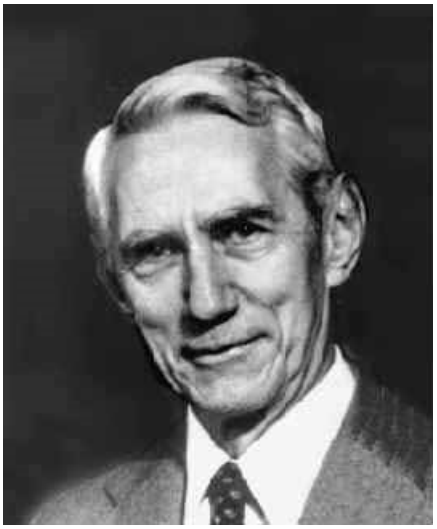
1- El sistema ha de ser impenetrable, si no en teoria, sí en la pràctica.
2- No ha de fer falta que l'algorisme sigui secret, i ha de ser capaç de caure en mans no desitjades sense que la seguritat del sistema perilli.

3- La clau s'ha de poder memoritzar sense l'ajut de notes i ha de ser fàcilment intercanviable.
4- Els criptogrames s'han de poder transmetre per telègraf.
5- La maquinària o documents necessaris han de poder ser transportats i utilitzats per una sola persona.
6- El sistema ha de ser fàcil, sense que faci falta el coneixement de llargues llistes de normes o que provoqui una alta tensió mental.

El principi número dos és el més conegut de tots i se'l coneix com a "**Principi de Kerckhoffs**". C.E. Shannon va reformular-lo com "L'enemic coneix el sistema". En aquesta forma, es coneix com a "**Màxim de Shannon**".

Si ens hi fixem, la majoria, si no tots, els mètodes de xifratge esmentats a la primera part no compleixen el Principi de Kerckhoffs, ja que tots ells disposen d'un mètode per trencar-los. Això significa que si l'enemic (a partir d'ara Eve) descobreix quin mètode de criptografia clàssica hem estat utilitzant per xifrar els nostres missatges, tard o d'hora podrà llegir-los.

4.1.2. Teoria de la informació



Claude E. Shannon. Font: *Google*

Un cop explicat el Principi de Kerckoffs, prossegueixo a explicar detalladament la **teoria de la informació**. Com he dit abans, Claude Shannon ens resol el dilema de com poder *mesurar* la informació. Ho explicaré a través d'un exemple:

Suposem que la policia sap que dos estudiants, un de l'Escola Politècnica de la UdG (diguem-li A) i un de la UPC (diguem-li B) es dediquen a estafar a la

gent a través de la Xarxa. La Guàrdia Civil de Girona sap que l'alumne A és una dona, i els Mossos d'Esquadra de Barcelona saben que l'alumne B estudia Arquitectura Tècnica. Sabent que aquestes són les úniques dades que coneix cada cos policial, ¿qui creieu que té més quantitat d'informació?

Podem adonar-nos que cada un dels estudiants disposa d'una variable aleatòria, que en el cas de l'alumne A és *sexe* i en el de l'alumne B és *carrera*, que pot prendre un nombre finit d'estats. Comencem amb l'alumne A. Sigui *X*, doncs, la variable *sexe*, que admet dos estats: x_1 = home, x_2 = dona. A partir de les dades de la matrícula de l'Escola Politècnica Superior (EPS) de la UdG, la probabilitat p_1 que un estudiant triat a l'atzar sigui un home és d'un 93%, mentre que la probabilitat p_2 que un estudiant triat a l'atzar sigui una dona és d'un 7%. Obtenim, així, la taula següent:

x_i	p_i
x_1 = home	p_1 = 0.93
x_2 = dona	p_2 = 0.07

(taula 9)

¿Quina *quantitat d'informació* té la Guàrdia Civil pel fet de conèixer que l'alumne A és una dona? Observem que, si la quantitat d'alumnes de l'EPS és de 1000, hi haurà 930 homes i 70 dones. Per tant, si la Guardia Civil sap que el delinqüent és una dona, el nombre de sospitosos serà més reduït que si sabés que és un home. Sembla clar, doncs, que com més baixa és la probabilitat de la variable, més quantitat d'informació es té. Així, per tal de definir la quantitat d'informació que aporta un estat variable mitjançant una fórmula matemàtica, haurem de trobar una funció que depengui de la probabilitat p_i d'aquest estat variable i que creixi quan p_i decreix. Es defineix la *quantitat d'informació d'un estat* x_i com l'oposat del logaritme en base 2 de p_i, i s'anota I_i. O sigui:

$$I_i = -\log_2 (p_i)$$

Si apliquem la fórmula a la variable *sexe* obtenim la següent taula:

x_i	p_i	I_i
x_1 = home	p_1 = 0.93	0.1047
x_2 = dona	p_2 = 0.07	3.837

(taula 10)

Podem observar que, efectivament, com més gran es fa p_i més petit queda I_i, i això es pot demostrar amb límits matemàtics. Degut a la seva condició de probabilitat, p_i pot estar entre 0 i 1. Si fem el límit en aquests extrems tenim: si p_i s'acosta a 1 (que simbolitzaria que x_i és un estat segur), llavors $\lim_{p_i \to 1}(-\log_2(p_i)) = 0$, que s'interpreta dient que com més gran és p_i (com més s'acosti a 1), de menys informació disposem; i si p_i s'acosta a 0 (que simbolitzaria que x_i és un estat impossible), llavors $\lim_{p_i \to 0}(-\log_2(p_i)) = +\infty$, que significa que com més petita és la probabilitat de l'estat x_i, més quantitat d'informació es té.

Pel que fa als Mossos d'Esquadra, sabem que aquests busquen a un alumne de la UPC que estudia Arquitectura Tècnica. Abans hem vist que la variable en l'alumne *B*, que ara anomenarem *Y*, era *carrera*. Aquesta pot prendre un nombre finit d'estats: Enginyeria Industrial (EI), Telecomunicacions (TC), Matemàtiques (M), Arquitectura Tècnica (AT), Informàtica (I) i Ponts i Camins (PC). Tenint en compte que hi ha 10000 estudiants a la UPC, la taula de probabilitats i de quantitat d'informació del fet que un alumne sigui d'una carrera determinada és:

x_i	**alumnes**	p_i	I_i
EI	4500	0.45	1.152
TC	900	0.09	3.474
M	300	0.03	5.059
AT	1800	0.18	2.474
I	2000	0.2	2.321
PC	500	0.05	4.322

(taula 11)

Aquí veiem, doncs, que la quantitat d'informació de la que disposen el Mossos si saben que l'alumne estudia Arquitectura Tècnica és de 2.474, que és inferior al 3.837 del que disposa la Guardia Civil, o sigui que aquesta última disposa de més informació.

4.2. Evolució de la informàtica (1945-1970)

Un cop explicada aquesta part de la teoria de la informació, procediré a explicar els diferents mètodes d'encriptació que s'han emprat en la informàtica des dels seus inicis fins a l'actualitat. Val a dir que la teoria de la informació de Shannon inclou moltes més coses que la simple mesura de la quantitat d'informació, com ara el concepte d'entropia, la mesura de la incertesa, la ràtio d'un idioma, etc. però no les he inclòs a causa de la seva complexitat matemàtica, més enllà de les intencions d'aquest treball. S'ha de tenir en compte que moltes d'aquestes coses tenen moltes aplicacions en la nostra vida diària. L'entropia criptogràfica, per exemple, s'utilitza quan es comprimeixen arxius informàtics, aplicant més quantitat de bits als caràcters menys probables.

Durant els any posteriors a la Segona Guerra Mundial, la criptografia encara estava restringida als organismes governamentals i militars. La principal diferència, però, amb la criptografia que s'havia estat usant fins aleshores, era l'ús de la informàtica. Encara que ambdues parteixen de bases molt similars, la criptografia informàtica presenta tres grans diferències amb la criptografia mecànica com la màquina Enigma. La primera és que una màquina física està limitada per la practicitat de la seva construcció, mentre que un ordinador pot emular una màquina hipotètica d'enorme complexitat.

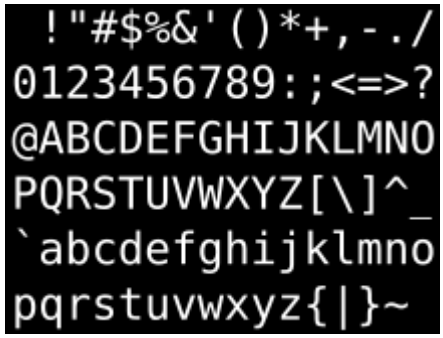
La segona diferència és la velocitat. Els aparells electrònics poden funcionar molt més ràpidament que els mecànics: un ordinador programat per a emular el comportament

de l'Enigma podria xifrar un missatge llarg en un instant, mentre que un operador humà tardaria una bona estona.

Finalment, la tercera i potser més significativa diferència és que els ordinadors funcionen amb nombres en comptes de amb alfabets. Aquests són nombres binaris, seqüències de zeros i uns, coneguts com a *dígits binaris* o *bits* (acrònim de l'anglès ***bi**nary digi**ts***). El fet que es treballi només amb zeros i uns i no amb les xifres de l'u al nou té una explicació ben senzilla. El funcionament d'un ordinador es basa en els *transistors*, petits dispositius que tenen dos estats possibles: quan hi passa corrent elèctric, representat amb un 1; i quan no n'hi passa, representat amb un 0.

Abans d'encriptar qualsevol missatge, les lletres i números d'aquests han de ser canviats per seqüències de bits per tal que els ordinadors el puguin processar. Alguns dels mètodes per fer-ho són l'**ASCII**, que utilitza l'alfabet anglès, o diverses de les versions de la seva ampliació, com l'**ISO 8859**, que incorpora caràcters d'altres alfabets com "ç", "€" o "ñ". El primer utilitza seqüències de 7 bits, que li permet codificar 128 caràcters diferents; i el segon n'utilitza 8, que li permeten codificar 256 caràcters diferents. Per simplicitat explicaré l'ASCII (de *American Standard Code for Information Interchange* – Codi Estàndard dels EUA per l'Intercanvi d'Informació).

Aquest utilitza seqüències de 7 xifres de uns i zeros, des del 0000000 (0 en base decimal) fins al 1111111 (127 en base decimal). Els caràcters del 0 al 31 més el 127 són caràcters de control, i els del 32 al 126 són els caràcters imprimibles que apareixen el la següent taula, incloent-hi l'espai en blanc:



Caràcters imprimibles d'ASCII.
Font: *Wikipedia*

D'aquesta manera, la paraula "Espia!" es codifica com "1000101 1110011 1110000 1101001 1100001 0100001" que en base 10 corresponen a la

seqüència numèrica “69 115 112 105 97 33”. Encara que la criptografia moderna utilitzi nombres en base 2 i la clàssica utilitzi lletres, els xifratges encara es basen en els antics principis de substitució i transposició. Qualsevol xifra, per molt complexa que sigui, pot ser separada en aquestes dues operacions.

Imaginem que volem encriptar el missatge “Espia!” amb una versió informàtica d’una xifra de transposició. Una de les maneres de xifratge més senzilles seria intercanviar el primer dígit amb el segon, el tercer amb el quart, etc. així:

Text pla = 1000101 1110011 1110000 1101001 1100001 0100001

Text xifrat = 0100011 1110011 1101001 0010110 1100000 1010010

En aquest cas, a més, l’algorisme per xifrar és el mateix que per desxifrar.

Ara imaginem que volem xifrar el mateix missatge amb la versió informàtica d’una xifra de substitució. Abans de xifrar, Alice i Bob[11] han de pactar una clau: per exemple, “Pedres”, la qual ha de ser codificada en ASCII abans que s’utilitzi. Un cop fet això, se sumen el text pla i la clau. La suma de bits segueix dos senzilles normes: si els dos elements de la suma són iguals, el resultat és 0; en canvi, si els sumands són diferents, és 1. En aquest cas:

Text pla = 1000101 1110011 1110000 1101001 1100001 0100001

Clau = 1010000 1100111 1100100 1110010 1100111 1110011

Text xifrat = 0010101 0010100 0010100 0011011 0000110 1010010

Un cop Bob rep el text xifrat, només fa falta que li sumi la clau per poder obtenir el text pla i llegir el missatge d’advertència d’Alice.

La informàtica neix a Bletchey Park, on, a més a més de l’Enigma, s’intentaven desxifrar els missatges de la màquina Lorenz, utilitzada per a les comunicacions d’alt

[11] Mirar l’apartat “Conceptes Clau”.

nivell a Alemanya, com ara entre Hitler i els seus generals. Aquesta màquina es va aconseguir desxifrar amb el que serien els primers ordinadors: els *Colossus*, ideats per Max Newman i Tommy Flowers. Lamentablement, les operacions a Bletchey Park es van guardar en secret durant molts anys des de la fi de la Segona Guerra Mundial, i les màquines *Colossus* van ser destruïdes. Això va significar que el títol de "mare dels ordinadors" fos atorgat a un altre aparell de disseny similar, l'ENIAC (sigles en anglès de "Computador i Integrador Numèric Electrònic") dissenyat a la Universitat de Pennsilvània i consistent de 12 vegades més vàlvules electròniques que els *Colossus* i capaç de realitzar 5000 operacions per segon. L'ENIAC va passar llavors a la propietat del Laboratori d'Investigació Balística de l'Exèrcit dels EUA.

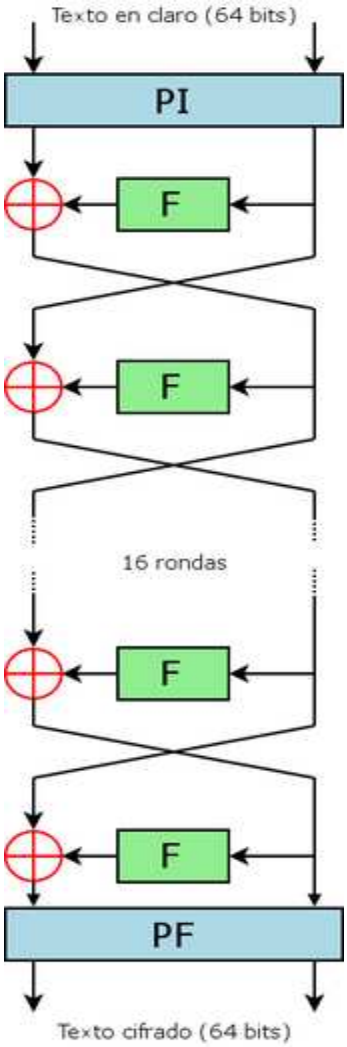
Tommy Flowers. Font: *Google*

Amb el temps, els ordinadors van anar canviant. L'any 1947 els laboratoris AT&T de Bell van inventar el transistor, una alternativa més barata a les vàlvules electròniques. A partir del 1951, les computadores van deixar de ser d'ús exclusius dels organismes governamentals i militars, i les grans empreses ja començaven a tenir ordinadors per a enregistrar les seves activitats comercials. La gegant de la informàtica IBM llança el 1953 el seu primer ordinador, i quatre anys més tard inventa Fortran, un llenguatge de programació que va permetre que la gent escrigués els seus propis programes. La invenció del circuit integrat o *chip* el 1959 va iniciar una nova era en les ciències de la computació.

Durant els anys 60, els ordinadors cada vegada eren més potents i més barats. Per això, també eren més usats en els negocis, i s'utilitzaven per encriptar afers importants, com transferències de diners o negocis delicats. No obstant això, mentre

cada vegada més i més negocis adquirien ordinadors, els criptògrafs es van trobar amb nous problemes i dificultats que no existien quan la criptografia era competència exclusiva dels governs i exèrcits. Una de les principals qüestions era l'estandardització. Una empresa podia utilitzar una xifra particular per assegurar les comunicacions internes, però no podia enviar un missatge secret a una organització externa si el destinatari no usava la mateixa xifra. Finalment, el 15 de maig del 1973, l'Oficina Nacional d'Estàndards nord-americana va decidir solucionar el problema, i va demanar propostes per a una xifra estàndard que permetria "parlar" secretament entre empreses i negocis diferents.

4.3. A la recerca d'un estàndard. DES



Esquema de funcionament del DES. Font: *Wikipedia*

Un dels algorismes de xifrat més estesos, i un dels candidats més sòlids per a l'estàndard, era un producte d'IBM conegut com a Lucifer. Havia estat desenvolupat per Horst Feistel, un immigrant alemany que havia arribat als EUA el 1934. Va tenir problemes diverses vegades amb l'Agència de Seguretat Nacional nord-americana (NSA), l'organització responsable de la seguretat de les comunicacions militars i governamentals, a causa del seu interès en la criptografia. Finalment, Feistel va acabar treballant en un laboratori d'IBM a Nova York, on va poder conduir la seva recerca sense ser perseguit. Va ser durant els inicis dels anys 70 quan va crear la xifra Lucifer.

Aquesta xifra encripta de la següent manera. Primer, el missatge es tradueix en una llarga cadena de bits. Segon, la cadena se separa en blocs de 64 dígits, i el procés

d'encriptació es fa separadament a cada bloc. Tercer, centrant-nos en només un bloc, els 64 bits es barregen amb la funció PI (Permutació Inicial), i se separen en dos semiblocs de 32 bits, anomenats $Dreta^0$ i $Esquerra^0$. Els dígits de $Dreta^0$ s'introdueixen en una funció "barrejadora" F, i se suma a $Esquerra^0$ per crear un nou semibloc anomenat $Dreta^1$. L'original $Dreta^0$ passa a ser ara $Esquerra^1$. Aquest seguit d'operacions s'anomena "ronda". Tot aquest procés es repeteix en una segona ronda, però començant amb $Dreta^1$ i $Esquerra^1$, i acabant amb els nous semiblocs $Dreta^2$ i $Esquerra^2$. El procés es va repetint fins a les 16 rondes. Finalment, els dos semiblocs finals, $Dreta^{16}$ i $Esquerra^{16}$, s'ajunten i es permuten amb la funció PF, inversa de PI (PF desfà el procés de PI).

Els detalls de la funció F poden canviar, i es determinen per una clau numèrica acordada prèviament entre l'emissor i el receptor. Per tant, per encriptar només fa falta que Alice introdueixi el missatge i la clau a Lucifer, que emet el text xifrat. Llavors Bob ha d'introduir el text xifrat i la clau a Lucifer, que emet el missatge original.

La seguretat de Lucifer i la seva difusió va fer que semblés inevitable la seva tria com a estàndard. Malauradament, la NSA va interferir un cop més en la feina de Feistel. Lucifer era tant forta que probablement estava més enllà de les seves possibilitats de trencar-la. Per això, la agència governamental va disminuir el nombre de possibles claus a poc més de 10^{17} (tècnicament ens referim a 56 bits, perquè aquest nombre consisteix de 56 dígits quan s'escriu en binari). Sembla que la NSA va pensar que aquest nombre de claus seria suficientment segur per a la comunitat civil, ja que cap organització civil tenia un ordinador prou poderós que comprovés cada una de les claus en una quantitat de

Horst Feistel. Font: *Google*

temps raonable. No obstant, la pròpia NSA podria tenir accés als missatges i transferències d'arreu del món. A la fi, la versió de 56 bits de Lucifer va ser adoptada oficialment el 23 de novembre del 1976, i va ser reanomenada **DES** (*Data Encryption Standard* – Estàndard per a l'Encriptació de Dades). Actualment, la seguretat del DES és baixa, i per això s'utilitzen el **Triple DES**, una forma més complexa del DES, que és l'estàndard que s'utilitza a les targetes de crèdit; i l'**AES** (*Advanced Encryption Standard* – Estàndard Avançat de Xifratge), un xifratge de blocs amb un algorisme molt complex.

4.4. Diffie-Hellman-Merkle o transmissió de claus

D'esquerra a dreta: R. Merkle, M. Hellman i W. Diffie. Font: *Google*

L'adopció del DES va solucionar el problema de la estandardització, però encara s'havia de solucionar un problema major: la distribució de claus. Des dels inicis de la criptografia la distribució de claus entre els usuaris ha sigut un problema. Tot i així, mentre la criptografia era només competència de governs i exèrcits, aquests podien encarar els costs monetaris i materials que això suposava per tal de garantir el bon funcionament d'una xifra. Malauradament, en la criptografia civil del món dels negocis, l'enviament de claus en mà a clients d'arreu del globus resulta un sobre cost prohibitiu.

Afortunadament, a la meitat dels anys 70 Whitfield Diffie, Martin Hellman i Ralph Merkle van idear un sistema per a transmetre una clau sense haver de veure's en

persona ni haver de confiar en terceres persones, sinó utilitzant un sistema de comunicació convencional, capaç de ser observat per qualsevol espia. Aquest mètode es coneix actualment com a **Diffie-Hellman-Merkle**.

Aquest mètode es basa en utilitzar funcions irreversibles o d'un sol sentit, amb les quals encara que sapiguem el resultat de la funció i quin és l'algorisme de la funció, no podem trobar el valor inicial que s'ha introduït a la funció. Per exemple, la funció $F(x) = 7 \cdot x$ és una funció reversible, ja que sabent per exemple que el resultat és 84, podem deduir ràpidament que $x = 12$. En canvi, l'aritmètica modular és una àrea de la matemàtica que conté funcions d'un sol sentit. La funció $F(x) = 7 \cdot x \pmod{11}$, per exemple, és irreversible, ja que si ens diuen que $F(x) = 4$, x llavors pot prendre una gran quantitat de valors, com ara 10, 21...

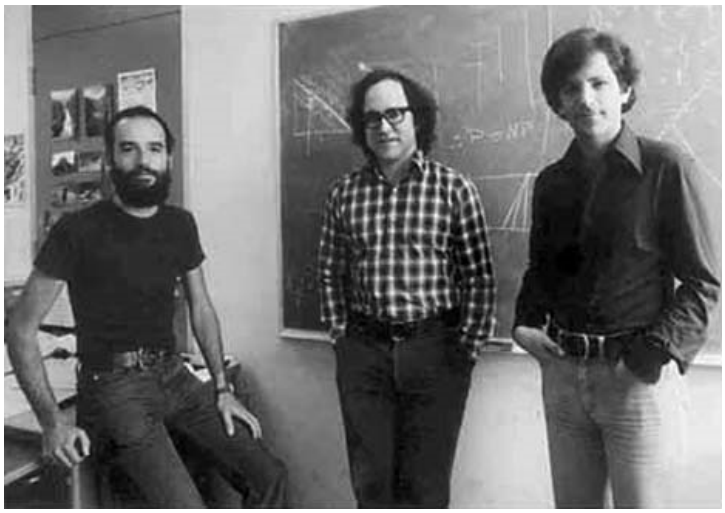
El protocol de la funció ideada per Diffie, Hellman i Merkle consisteix en els següents passos:

1- Alice i Bob acorden una funció $F(x)$ del tipus $Y^x \pmod{P}$, on P i Y són nombres enters positius, com per exemple $F(x) = 7^x \pmod{9}$. L'acord es pot realitzar per qualsevol medi convencional capaç de ser atacat per Eve.
2- Alice i Bob escullen un nombre cadascun (α, β) i el mantenen en secret, per exemple 5 i 9, respectivament.
3- Cada un d'ells per separat introdueix el nombre secret a la funció F, que n'emet un altre (A, B). En l'exemple, Alice fa $F(5) = 7^5 \pmod{9} = 16807 \pmod{9} = 4 = A$, i Bob, $F(9) = 7^9 \pmod{9} = 1 = B$.
4- Alice i Bob intercanvien els nombres A i B, i els introdueixen a la funció que els donarà la clau: Alice realitza la operació $B^\alpha \pmod{P}$ i Bob, la operació $A^\beta \pmod{P}$. En l'exemple: $1^5 \pmod{9} = 1$ i $4^9 \pmod{9} = 1$. El nombre resultant, que serà el mateix per a tots dos, conformarà la clau del sistema. Encara que Eve hagi

pogut espiar la transferència d'*A* i *B*, com que la funció *F* és d'una sola direcció no podrà esbrinar la clau.

Podríem fer una analogia del sistema Diffie-Hellman-Merkle amb pots de pintura. Imagineu-vos que tant Alice com Bob tenen un cubell de tres litres, i que els omplen d'un litre de pintura groga cadascun. Llavors cada un d'ells per separat hi afegeix un litre d'una pintura d'un color determinat, que serà secret, per exemple blau per l'Alice i vermell per Bob. A continuació s'envien els pots de pintura l'un a l'altre, i omplen el litre que falta al cubell amb la seva pintura secreta. Així, cada un d'ells tindrà un cubell amb un litre de pintura groga, un de pintura blava i un de vermella, que conformarà la clau. Per molt que Eve hagi tingut accés als pots de pintura mentre s'enviaven, no podrà separar les pintures originals que els conformen.

4.5. La criptografia de clau pública. RSA



D'esquerra a dreta: A. Shamir, R. Rivest i L. Adleman.
Font: *Google*

Encara que el protocol d'intercanvi de claus Diffie-Hellman-Merkle va ser un pas de gegant endavant en la criptografia, no era perfecte perquè tenia un problema inherent. Imagineu que Alice viu a Nova Zelanda i vol enviar-li un missatge xifrat a Bob, que viu a Bilbao. Vol fer servir el protocol Diffie-Hellman-Merkle, així que li envia la funció *F* i el seu resultat per e-mail. Per tenir una resposta, Alice haurà d'esperar 12 hores fins que Bob es desperti. Com que llavors el més probable és que ella estigui dormint, s'haurà d'esperar 12 hores més fins que ja estigui desperta i obri el correu per

trobar-se amb el missatge de Bob. Si, a més a més, Bob no ha pogut respondre a l'e-mail, s'haurà d'esperar fins que aquest comprovi els seus correus per a poder enviar-li finalment el missatge xifrat.

Com veieu, la distribució de claus planteja el problema que s'ha d'esperar fins a que els dos interlocutors s'han posat en contacte. Per això, els matemàtics i informàtics Ronald Rivest, Adi Shamir i Leonard Adleman van crear el 1977 el sistema **RSA**, el primer de *clau asimètrica*[12], on les claus utilitzades per xifrar i desxifrar són diferents. Val a dir, però, que la criptografia asimètrica ja havia sigut ideada per Whitfield Diffie, encara que mai se li va acudir com es podria crear un algorisme que utilitzés aquesta propietat. Tot i així, els investigadors del MIT van ser capaços de trobar-ne un que complís els requisits.

Podríem imaginar-nos l'RSA com a un cadenat. Si qualsevol persona vol enviar-li un missatge a Alice, només ha d'anar a una botiga a comprar un "cadenat Alice" (simbolitza la clau pública) i posar-lo a la capsa on hi hagi el missatge. Un cop tancat el cadenat, ningú no podrà obrir-lo excepte Alice amb la seva clau personal (simbolitza la clau privada). Evidentment, l'algorisme de xifratge de l'RSA és una mica més complicat:

1- Alice escull dos nombres primers gegants p i q. En la pràctica aquests tenen més de 150 xifres, però per simplificar-ho utilitzaré $p = 13$ i $q = 19$. Alice manté aquests nombres en secret absolut.

2- Alice multiplica p i q per obtenir un altre nombre, N. En aquest cas, $N = 247$. Tot seguit calcula $\varphi(N)$, operant $(p-1)\cdot(q-1)$. Per tant, $\varphi(247) = (13-1)\cdot(19-1) = 216$.

[12] Veure l'apartat de "Conceptes Clau"

També escull un altre nombre, *e*, tal que sigui coprimer[13] amb *φ(N)*, i escull en aquest cas *e = 5*.

3- Ara Alice pot publicar les seves claus públiques, *e* i *N*, en qualsevol lloc a la vista de tothom, com en un llistin telefònic. Ara, qualsevol que vulgui enviar-li un missatge a Alice, només haurà d'anar a mirar-ho al llistin.

4- Per a poder encriptar el missatge, primer s'ha de convertir en un nombre, *M*. Per exemple, qualsevol paraula pot ser transformada a ASCII, i qualsevol nombre binari pot ser canviat a base decimal. Llavors, *M* s'encripta per donar el text xifrat, *C*, amb la fórmula $C = M^e \ (mod\ N)$. Imaginem que Bob vol enviar a Alice la lletra *X*. En codi ASCII, la *X* es representa com a 1011000, que equival al nombre decimal *88*. Com que *M = 88*, llavors opera $C = 88^5 \ (mod\ 247) = 160$. Ara Bob envia *C* a Alice.

5- Perquè Alice pugui desxifrar el missatge, necessita la clau privada *d*. Aquesta es pot calcular amb la fórmula $d = e^{-1} \ (mod\ φ(N))$. Això es calcula buscant el primer nombre *d* tal que $d \cdot e = 1 \ (mod\ φ(N))$. En l'exemple, $5 \cdot 173 = 1 \ (mod\ φ(N))$. Llavors *d = 173*.

6- Per desencriptar el missatge, Alice només ha d'utilitzar la fórmula $M = C^d \ (mod\ N)$. En aquest cas, $M = 160^{173} \ (mod\ 247) = 88 = X$ en ASCII.

El mètode RSA i la criptografia de clau pública ha sigut considerat per molts com el major avenç en criptografia des de la invenció dels xifratges monoalfabètics. Per primera vegada no era necessària cap distribució segura de claus, sinó que si

---

[13] Dos nombres són coprimers quan el màxim comú divisor (mcd) entre tots dos és 1. Per exemple, 25 i 24 són coprimers.

La funció ϕ (*phi d'Euler*) és una peça clau de la xifra RSA. Consisteix en calcular la quantitat de nombres enters menors que un altre nombre que siguin coprimers amb ell. És una funció molt complicada de calcular si no se saben els factors del nombre. Si el nombre és producte de dos nombres primers *p* i *q*, com és en aquest cas *N*, la funció phi d'Euler es pot calcular amb l'expressió *(p-1)·(q-1).*

qualsevol persona havia d'enviar un missatge xifrat a una altra, només havia de buscar la seva clau pública en una llista.

Clifford Cocks. Font: *Google*

Un fet curiós són els descobriments fets pels investigadors del GCHQ (l'anàleg de la NSA al Regne Unit) James Ellis, Clifford Cocks i Malcolm Williamson. Aquests van inventar, abans que Diffie, Hellman, Merkle, Rivest, Shamir i Adleman ho fessin, el protocol Diffie-Hellman-Merkle i la xifra RSA, però com que treballaven per una agència governamental no ho van poder fer públic. Això, tot i així, no resta mèrit als investigadors nord-americans, ja que ells van inventar-ho partint del no res, sense saber que tres treballadors de la intel·ligència britànica ja ho havien fet tres anys abans.

4.6. Criptografia segura a l'abast de tothom. PGP. Signatura digital

Malgrat tot, el sistema RSA és un sistema lent, i per això s'utilitza normalment com a manera d'enviar les claus per a un sistema de clau simètrica, com el DES, AES, o Blowfish, un altre xifratge de bloc semblant al DES. El sistema més conegut que utilitza aquest procediment és el **PGP** (*Pretty Good Privacy* – Privacitat Bastant Bona) de Phil Zimmermann, que combina l'RSA i un mètode de clau privada anomenat IDEA. La seguretat del PGP és tan alta que Zimmermann va tenir problemes amb l'FBI per haver-lo exportat. A més a més, el PGP porta implementat un sistema de *signatura digital*.

La signatura digital respon a un altre dels problemes de la criptografia, l'*autentificació*.

Imagineu-vos que la malvada Eve envia un e-mail a Bob i escriu el nom d'Alice al final. Com es pot assegurar Bob que ha estat escrit realment per ella? De la mateixa manera, imagineu-vos que un banc rep un correu d'un client dient que traspassin tots els seus fons a un compte de les Illes Caiman. Com poden estar segurs sobre la identitat del seu client sense una firma manuscrita? La criptografia de clau pública ens dóna una solució a tots aquests problemes.

Hem vist que quan s'utilitza aquest tipus de criptografia la clau pública s'utilitza per xifrar i la privada per desxifrar. Què passaria si ho féssim al revés, que la clau privada s'utilitzés per xifrar i la pública per desxifrar? Llavors el missatge no oferiria cap seguretat, ja que tothom podria desxifrar-lo. Però quan la gent ho desxifrés, sabria amb tota seguretat qui ha escrit aquell missatge. Si Alice envia un missatge a Bob i Bob pot desxifrar-lo utilitzant la clau pública d'Alice, llavors sap amb absoluta seguretat que aquell missatge l'ha escrit ella.

La signatura digital s'utilitza de la següent manera: Alice escriu un missatge a Bob i l'encripta primer amb la seva pròpia clau privada, llavors ho fa amb la clau pública de Bob i li ho envia tot; quan ell rep el missatge, el desxifra primer amb la seva clau privada i llavors amb la clau pública d'Alice. Un procés garanteix la privacitat i l'altre l'autenticitat.

Phil Zimmerman. Font: *Google*

4.7. Epíleg

Tot i l'alta seguretat que proporcionen actualment els sistemes de criptografia moderna, aquesta es basa sobretot en la potència i velocitat de càlcul dels ordinadors convencionals. Però existeixen un tipus d'ordinadors, que actualment només són

teòrics, que podrien trencar un sistema RSA en un període de temps raonable. Es tracta dels *ordinadors quàntics* que basen el seu funcionament en la física quàntica, en comptes de la física clàssica com els ordinadors convencionals. Va ser a partir de la ideació d'aquests ordinadors que va néixer el concepte d'un tipus de criptografia absolutament irrompible, la criptografia quàntica.

5. CRIPTOGRAFIA QUÀNTICA

5.1. Introducció a la mecànica quàntica

Thomas Young. Font: *Google*

Abans de començar amb la computació quàntica i les seves aplicacions criptogràfiques, he de fer una petita introducció a la mecànica quàntica o física quàntica. L'any 1799, l'erudit anglès Thomas Young, que va poder desxifrar els jeroglífics egipcis amb l'ajuda de la pedra de Roseta, va publicar *The Undolatory Theory of Light*, on explicava que la llum es comportava com una ona. Actualment sabem que la llum es comporta com una ona i com una partícula, i la considerem d'una manera o d'una altra depenent de les circumstàncies. La partícula de llum, anomenada *fotó*, és la pedra angular de la mecànica quàntica.

Com va dir un dels pares de la física quàntica, el danès Niels Bohr, "Qualsevol que pugui observar la mecànica quàntica sense marejar-se, és que no l'ha entesa". I no li falta raó, ja que aquesta se sustenta en unes idees molt estranyes. Una de les característiques del món quàntic, és a dir, el de les partícules fonamentals com els fotons o els electrons, és la característica de ser en dos llocs i estats diferents al mateix temps.

Com s'explica això? Hi ha bàsicament dues teories oposades. La primera és la de la *superposició*. Imaginem-nos un túnel, al final del qual hi ha una bifurcació, i una pantalla on desemboquen tots dos camins. Si llancem un fotó a través del túnel, l'únic que sabem és que hem llançat un fotó que ha arribat a la pantalla, i, en canvi, no sabem per quin dels dos camins ha passat. La teoria de la superposició diu que, com que no ho sabem, assumim llavors que ha passat pels dos camins al mateix moment.

És a dir, que en arribar a la bifurcació, el fotó s'ha separat en dos fotons "fantasma" que s'han tornat a unir quan han sortit del túnel.

Hi ha una altra teoria que explica aquest estrany comportament. Malauradament, és igual d'estrambòtica. És la *interpretació dels diversos mons* o *teoria del multivers*. Aquesta teoria ens diu que quan el fotó arriba a la bifurcació, aquell punt es divideix en dos universos, i en un d'ells el fotó passa per un camí i en l'altre, per l'altre camí. Quan s'acaba el túnel, els dos universos interactuen entre ells i es tornen a unir. En definitiva, la teoria ens diu que si quan una partícula té l'oportunitat de triar entre diversos possibles estats, l'univers es divideix la mateixa quantitat d'universos, i en cada un d'ells la partícula tria un estat diferent.

Malgrat que aquestes teories siguin molt estranyes, només la teoria quàntica pot predir les conseqüències de les interaccions nuclears a les centrals; només la teoria quàntica explica com brilla el Sol; només la teoria quàntica pot ser emprada per dissenyar els làsers que llegeixen els CD en un equip estèreo. Ho vulguem o no, vivim en un món quàntic.

5.2. A la recerca del computador quàntic

David Deutsch. Font: *Google*

De totes les conseqüències de la teoria quàntica, la tecnològicament més important és sens dubte la computació quàntica. El primer en idear una computació d'aquest tipus va ser el físic britànic David Deutsch. Quan assistia a una conferència sobre la teoria de la informació, va adonar-se d'una cosa: s'estava pressuposant que els ordinadors havien de funcionar amb les lleis de la física clàssica. Deutsch estava convençut que els ordinadors haurien de poder obeir les lleis de la física quàntica, ja

que són lleis més fonamentals. En una publicació del 1985, descriu la seva visió d'un ordinador quàntic utilitzant les lleis de la física quàntica.

Imaginem que hem de fer dues operacions. Per fer-les amb un ordinador convencional, primer hem d'introduir la primera operació, esperar la resposta, i llavors introduir la segona operació. En canvi, si l'ordinador seguís les lleis de la física quàntica podria realitzar les dues operacions al mateix moment, degut a la característica dels dos estats simultanis.

Per tal que ens en puguem fer una idea més clara, comparem el que passaria amb cada tipus d'ordinador si busquem la solució a un problema concret. Per exemple, busquem quin és el nombre el quadrat i cub del qual utilitzen totes les xifres de l'1 al 9 només una vegada. Si provem amb el 19, trobem que $19^2 = 361$ i que $19^3 = 6859$. Per tant, el número 19 no compleix els requeriments, ja que només hi apareixen les xifres 1, 3, 5, 6, 6, 8, 9; hi manquen els nombres 0, 2, 4 i 7 i el nombre 6 es repeteix.

Per solucionar el problema amb un ordinador convencional, s'anirien provant tots els nombres un a un fins a trobar la solució: primer l'1, i es troba que no ho compleix; després el 2, i es troba que tampoc ho fa; i així successivament. Finalment, l'ordinador trobaria que la resposta és 69, ja que $69^2 = 4761$ i $69^3 = 328509$. Si tardés un segon a fer cada operació, hauria tardat 69 segons. En comparació, un ordinador quàntic hagués tardat només un segon.

Per tal de poder operar amb un ordinador quàntic, primer s'han de representar els nombres de tal manera que els pugui comprendre. Una de les maneres seria utilitzar l'*spin*, que determina la direcció en la que rota una partícula fonamental. Així, quan giri en sentit horari representarà un 1 i quan giri en sentit antihorari representarà un 0. D'aquesta manera, qualsevol nombre serà representat de forma binària.

Amb un ordinador quàntic, es podrien representar molts nombres a la vegada degut a la característica dels dos estats simultanis. Aconseguir la superposició d'estats (o d'universos) es faria de la forma següent. Imaginem que tenim una partícula rotant en sentit horari. Per fer-la canviar de direcció, només li hem d'aplicar un pols d'energia suficientment fort. Si li apliquem un pols d'energia més dèbil, llavors podria ser que canviés de direcció, i podria ser que no. Si la partícula hagués estat a la vista, hauríem seguit tot el procés. En canvi, si hagués estat tancada en una capsa i li haguéssim aplicat un pols d'energia dèbil, llavors no tindríem cap manera de saber si ha canviat de sentit o no. Seguint les lleis de la mecànica quàntica, la partícula estaria rotant cap a totes dues direccions alhora.

Si llavors agaféssim set partícules (capaces de representar del 0 al 127), les tanquéssim en una capsa i els apliquéssim set polsos d'energia dèbils, les set partícules estarien en superposició i s'estarien representant 128 estats diferents a la vegada. Per tant, un ordinador quàntic podria comprovar tots els nombres a la vegada i resoldre el problema en tan sols un segon.

Mentre que els zeros i uns que utilitzen els ordinadors convencionals són anomenats bits, els zeros i uns en superposició que utilitzarien els ordinadors quàntics s'anomenen *qubits* (acrònim de ***qu****antum* ***bits***). Els avantatges dels qubits respecte dels bits són més clars si n'utilitzem molts. Amb 250 qubits seríem capaços de representar simultàniament gairebé 10^{75} combinacions diferents, un nombre més gran que la quantitat d'àtoms a l'univers.

Tot i així, els ordinadors quàntics tenen diversos problemes. El primer de tot, i el més complicat de solucionar, és la seva construcció, ja que no s'ha trobat cap manera de mantenir la superposició i a la mateixa vegada mesurar l'spin de les partícules. Un sol àtom entrant amb contacte amb elles faria que desaparegués la superposició.

Un altre problema era que no se sabia com poder programar un ordinador quàntic. Tot i així, el 1994, Peter Shor, dels Laboratoris AT&T Bell de Nova Jersey, va definir amb èxit un programa útil per un ordinador quàntic. Va ser una notícia remarcable pels criptoanalistes, ja que el programa de Shor definia una sèrie de passos que podia seguir un ordinador quàntic per factoritzar nombres gegantins, exactament el que feia falta per trencar l'RSA. Dos anys després, Lov Grober, dels mateixos laboratoris, va crear un altre programa poderós. Aquest programa és una manera de buscar en una llista a grans velocitats, cosa que podria no semblar interessant si no ens fixem que és exactament el que es requereix per trencar el DES i d'altres programes similars.

Segons Serge Haroche, de la Universitat de Paris VI, l'arribada dels ordinadors quàntics serà en un futur proper. Com que els criptògrafs ja se'n van adonar, van saber que s'havien de crear nous mètodes criptogràfics per fer front als computadors quàntics, que deixaran tots els sistemes de criptografia informàtica obsolets.

5.3. Criptografia realment segura. *One-Time Pad*

Gilbert Vernam.
Font: *Google*

L'any 1917, Gilbert Vernam, dels laboratoris AT&T, i Joseph Mauborgne, capità a l'exèrcit dels EUA, van inventar la Xifra de Vernam, una variant de la Xifra Vigenère on la clau és una seqüència completament aleatòria i de la mateixa longitud que el text. La variant d'aquesta xifra on la clau mai pot ser repetida ni total ni parcialment es coneix com a **One-Time Pad**, o *Llibreta d'un sol ús*.

Claude Shannon va demostrar durant els anys 40 que la xifra One-Time Pad és absolutament impossible de trencar, sempre que se segueixin una sèrie de condicions, com que la clau sigui realment aleatòria, tan llarga com el text, que no es reutilitzi total o parcialment i que es mantingui en absolut secret.

Per mostrar la seguretat del mètode posaré un exemple. Imagineu que Alice vol enviar a Bob el missatge “HOLA” d'aquesta manera, i produeix la clau aleatòria “XMCK”. Si ara usem el quadre de substitució de la Xifra Vigenere (en realitat els bits d'“HOLA” se sumarien amb els de “XMCK”), el missatge es transforma en “FBNK”. Com que Bob ja ha rebut abans la clau d'Alice per un canal segur, serà capaç d'entendre el missatge. Eve, en canvi, no sap la clau. D'aquesta manera, encara que tingui una potència computacional infinita que li permetés comprovar totes les claus possibles, trobaria una clau amb la que el missatge “FBNK” seria “HOLA”, però també una altra amb la que seria “DEMA” o “ADEU”. Així, si la clau compleix tots els requeriments One-Time Pad és absolutament segur.

Tot i que no ha tingut difusió en el món civil i empresarial ja que és poc pràctica, la xifra One-Time Pad ha sigut emprada en diverses ocasions durant l’últim segle per part dels serveis d'intel·ligència de diversos països. Justament és això, la seva poca rendibilitat, el que intenta canviar la criptografia quàntica.

C. H. Bennett i G. Brassard. Font: *Google*

La criptografia quàntica no és realment un mètode criptogràfic en si mateix com DES, RSA o el propi One-Time Pad, sinó que és un mètode per a poder enviar una clau aleatòria, que posteriorment serà utilitzada amb One-Time Pad, d'una forma completament segura. Això és així perquè es pot saber si Eve ha estat observant el canal gràcies a la mecànica quàntica. Actualment existeixen dos mètodes d'aconseguir-ho, i és molt probable que un d'ells es converteixi en l'estàndard d'encriptació en un futur proper. Són el BB84 i l'E91.

5.3.1. BB84

El **BB84** va ser inventat el 1984 per Charles Benett, empleat d'IBM, i Giles Brassard, canadenc. Per utilitzar aquest sistema primer s'han de representar els zeros i uns amb fotons de certes polaritzacions[14]. En aquest cas, es representen de diferent manera depenent de l'esquema o base que utilitzem: l'esquema *rectilini* o +, i l'esquema *diagonal* o ×. En el primer, ↑ (vertical, V) representa 1 i → (horitzontal, H) representa 0; i en el segon, ↘ (-45) representa 1 i ↗ (+45) representa 0. Per enviar un missatge, s'escullen els esquemes de forma aleatòria. Així, la seqüència de bits 100110110110 es codifica de la següent manera:

Text pla: 1 0 0 1 1 0 1 1 0 1 1 0

Esquemes: × × + × + + + × × + × +

Text xifrat: ↘ ↗→↘ ↑→ ↑ ↘↗ ↑ ↘→

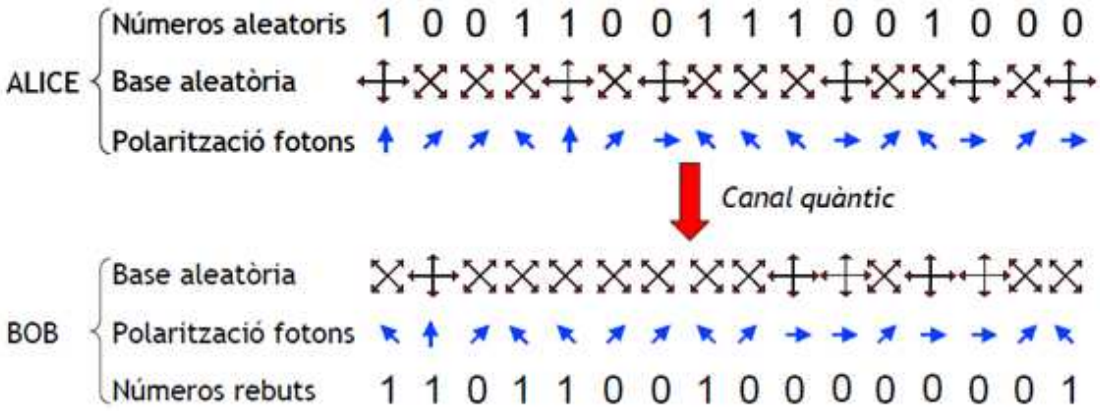
Llavors només s'han d'enviar els fotons polaritzats en la direcció desitjada i enviar-los a través d'algun sistema òptic com l'aire o la fibra òptica. Aquests fotons prèviament s'han escollit amb l'ajuda d'un Separador de Fotons segons Polarització o *Polarization Beam Splitter.*

El procés de funcionament del BB84 és el següent:

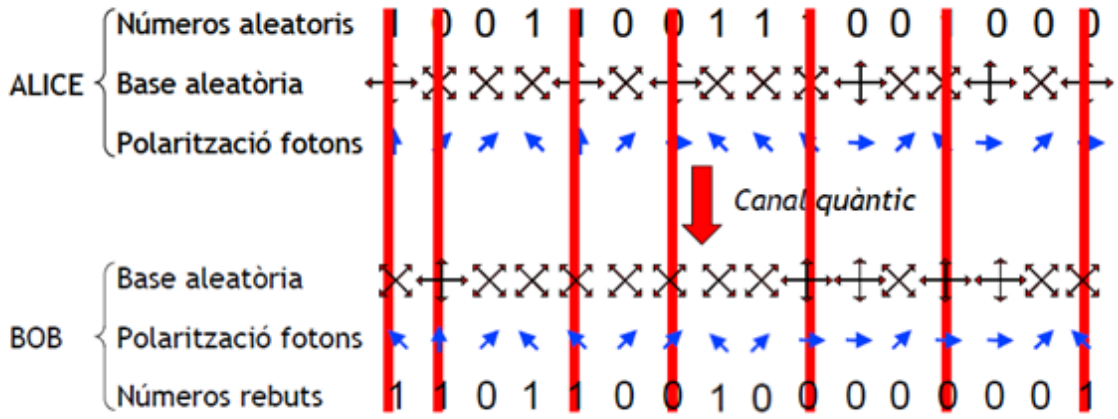
1- Alice genera una seqüència aleatòria de bits (recordem que aquest protocol serveix per enviar la clau de One-Time Pad, que ha de ser aleatòria) molt llarga, molt més que el text amb el que s'ha d'usar. Aquesta seqüència es transforma en una altra seqüència de fotons polaritzats segons una sèrie aleatòria d'esquemes × i + i s'envien a Bob per un canal quàntic.

[14] La polarització és la direcció en la que vibra el camp elèctric d'un fotó. En realitat, el camp pot vibrar en qualsevol direcció, però per simplificar es diu que només por vibrar en 4 direccions.

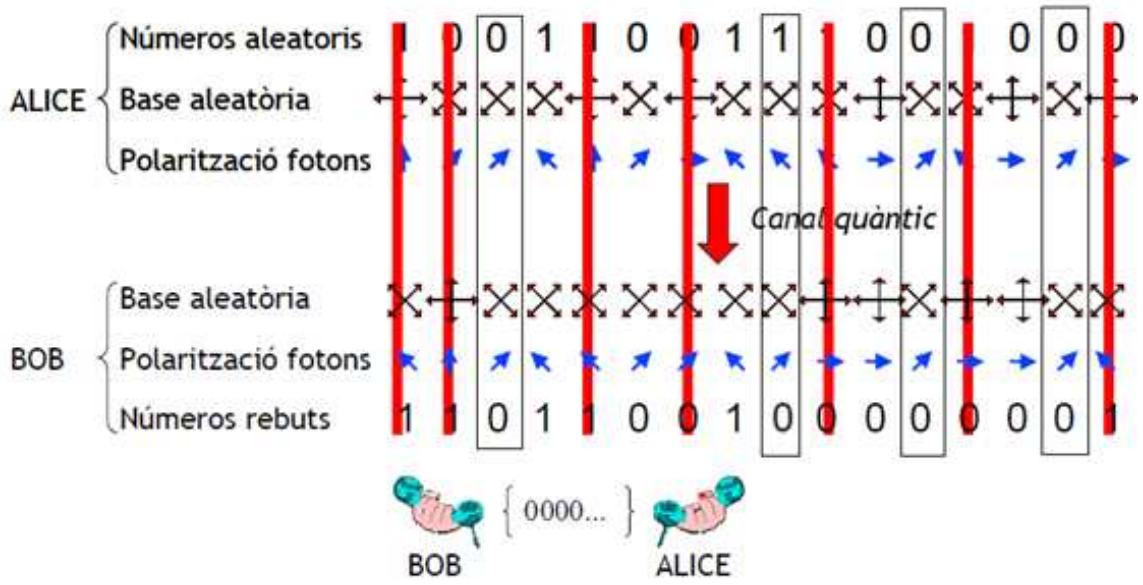
2- Bob analitza els fotons rebuts amb una sèrie aleatòria pròpia d'esquemes i els transforma en uns i zeros. Si mesura el fotó amb el mateix esquema que ha usat Alice, la polarització del fotó rebut serà la mateixa. Si, en canvi, s'equivoca d'esquema, la polarització del fotó li pot sortir en qualsevol direcció. Per exemple, si Alice envia un fotó amb polarització → i Bob ho mesura amb l'esquema rectilini +, Bob rebrà que el fotó era →. En canvi, si ho mesura amb l'esquema diagonal ×, tant pot ser que rebi que era ↗ com ↘.



3- Bob comunica a Alice les bases que ha utilitzat. Llavors Alice li diu a Bob quan han utilitzat el mateix esquema i tots dos eliminen el subconjunt de dades on han utilitzat bases diferents (*basis reconcilliation*). El conjunt de dades que queda s'anomena clau esporgada (*shifted key*).



4- Bob envia a través d'un canal públic una fracció de la clau esporgada a Alice per comprovar la correlació de les dades. En un sistema ideal i sense cap espia la correlació és del 100%.



5- Alice analitza la taxa d'errors en la correlació (QBER[15]) per saber si Eve ha estat espiant. Quan Eve rebés un fotó d'Alice, hauria utilitzat una base a l'atzar i, per tant, hauria utilitzat la base correcta en el 50% dels casos. En aquests casos, només el 50% de les vegades Bob utilitzaria la mateixa base que Alice. Per tant, el QBER típic en un sistema ideal on hi hagi un espia és del 25%. En el quadre esquemàtic, podem veure com el QBER seria del 25%.

Podríem pensar en el BB84 utilitzant una analogia amb un joc de cartes. Les bases o esquemes per escollir en aquest cas són "pal" i "nombre". Imaginem doncs que Alice treu una carta a l'atzar de la baralla i n'apunta només el nombre, 7. Quan Bob rep la carta, escull aleatòriament la base "pal" i apunta llavors "bastos". Quan ho han repetit suficients vegades, llavors s'envien per un canal públic en quin moment han utilitzat la base "pal" i quan la base "nombre" i descarten les vegades que no han usat la mateixa.

[15] De *Quantum Bit Error Rate*, Taxa d'Error dels Bits Quàntics.

Malgrat tot, un sistema real de transmissió de fotons, com la fibra òptica, produeix errors: pèrdua de fotons, canvi de polarització, etc. Tot i així, el QBER típic d'un sistema real no arriba al 10%.

Si el QBER estimat és de més de l'11%, la clau es descarta. Si és inferior a aquest valor, s'efectua el següent procediment per tal d'eliminar els errors: Bob i Alice sumen per separat dos bits que es trobin en les mateixes posicions i comparen el resultat; si és igual, llavors es queden amb un bit i descarten l'altre; si obtenen un resultat diferent es descarten tots dos bits. L'operació es repeteix progressivament fins que ja s'ha realitzat amb tots els bits. Llavors es torna a calcular el QBER amb una fracció de les dades, i si aquest no és perfecte, es repeteix la operació de sumar bits. Un cop el QBER és nul, es descarten les dades que sobrin i ja s'obté la clau.

5.3.2. E91

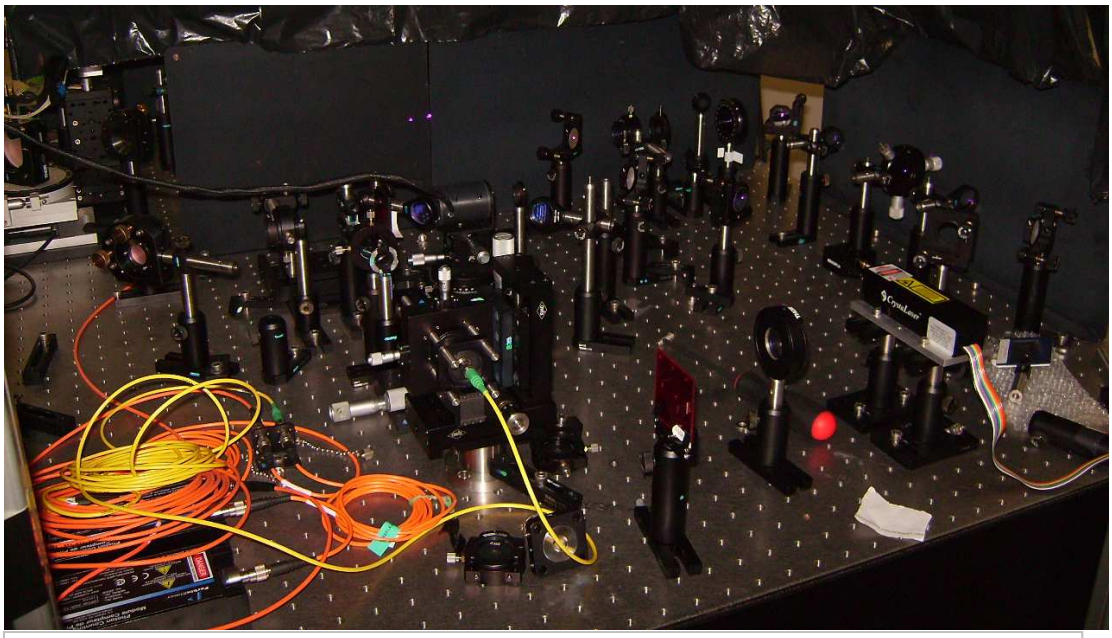
Artur Ekert. Font: *Wikipedia*

Malauradament, el BB84 té desavantatges. Si l'emissor de fotons que utilitza Alice no emet només fotons individuals, és a dir, que a vegades emet dos o més fotons a la vegada, el sistema no és segur. Si s'emeten dos fotons a la vegada, tots aquests tindran la mateixa polarització. Quan Eve intercepti els fotons, pot analitzar-ne un i deixar passar l'altre. D'aquesta manera, ni Bob ni Alice se n'adonaran de la presència d'Eve.

Per això, el 1991 Atur Ekert va idear el sistema **E91**, que es basa en les propietats de l'entrellaçament quàntic o de fotons. Es diu que dos fotons estan entrellaçats quan, si sabem una característica determinada d'un d'ells, podem deduir la de l'altre. Per exemple, si tenim dos fotons entrellaçats i l'*spin* d'un va en sentit horari, llavors el de l'altre anirà en sentit antihorari. Això mateix es pot aplicar a la resta de característiques

quàntiques, com ara la polarització, la direcció i sentit del moviment, la longitud d'ona, etc.

Per aconseguir l'entrellaçament quàntic dels fotons es procedeix de la següent manera. Un feix làser, prèviament condicionat amb les característiques desitjades (forma, radi del feix, intensitat...) , es dirigeix a un cristall especial. Com que la matèria està pràcticament buida, es necessita un feix amb una gran quantitat de fotons perquè tan sols un o dos aconsegueixin impactar contra els àtoms del cristall. Quan un fotó aconsegueix impactar contra un d'ells, l'àtom s'excita[16], i, quan torna a l'estat original, emet dos fotons que estan entrellaçats.



Feix làser condicionat i dirigit cap a un cristall que emet llavors dos fotons entrellaçats.
Font: Fotografia feta durant la visita a l'ICFO.

Un cop s'obtenen els dos fotons entrellaçats, Alice es queda amb un d'ells i envia l'altre a Bob. En aquest cas, poden utilitzar qualsevol característica dels fotons per transmetre la clau, no solament la polarització. Amb aquest sistema, és molt fàcil

[16] Es diu que un àtom està excitat quan un dels seus electrons « puja » de nivell atòmic. Perquè un àtom s'exciti necessita rebre energia, i quan es desexcita emet energia en forma de fotons.

esbrinar quan Eve ha interferit en la transmissió dels fotons, ja que l'entrellaçament entre els fotons desapareix quan algú altera el sistema, encara que sigui tan sols observant-lo. Malauradament, qualsevol petita alteració en el sistema provoca que els fotons deixin d'estar entrellaçats. Per tant, mantenir-los en aquest estat el temps suficient per fer la transferència és molt complicat.

5.4. Epíleg. Futur de la criptografia

La criptografia quàntica encara és un camp per explorar del qual se'n coneix molt poc. L'E91 encara no ha sortit mai del món teòric a causa de la dificultat de transmetre fotons entrellaçats, i el BB84 tan sols s'ha provat en un grapat d'experiments. Malgrat tot, això correspon només a l'àmbit públic, la informació del qual és a disposició de tothom; per això, és possible que actualment ja hi hagi una xarxa que connecti el Pentàgon i la Casa Blanca funcionant amb criptografia quàntica.

Tot i així, el futur de la criptografia és incert. Phil Zimmerman, creador del PGP, afirma que vivim en una edat daurada de la criptografia, ja que actualment la balança de l'eterna batalla entre criptoanalistes i criptògrafs es decanta cap a aquests últims. Malgrat tot, l'arribada dels ordinadors quàntics abans que la criptografia quàntica estigui ben conformada provocaria un espai de temps on no hi hauria seguretat ni privacitat a l'hora de transmetre missatges.

Fa ben poc, el dia 27 de desembre del 2009, un grup noruec, *Quantum Hacking Group*, conjuntament amb el *Centre for Quantum Technologies* de Singapur, han obtingut una manera de poder interceptar el 100% dels fotons transmesos en el BB84 sense que Bob i Alice ho notin. Aquest descobriment podria causar que el BB84 deixés de ser un sistema segur; cosa que provocaria que la criptografia quàntica estigués més lluny de poder ser portada a la pràctica mentre l'E91 no deixi de ser bàsicament teòric.

PART PRÀCTICA

6. ANÀLISI DEL DESXIFRAT DE TEXTOS

Tal i com he explicat a la introducció la primera idea que vaig tenir per fer una part pràctica va ser xifrar un text amb un sistema dèbil, fàcilment desxifrable, i passar-lo a un grup d'alumnes de 1r de Batxillerat que es van oferir voluntaris. Quan el desxifressin els passaria un qüestionari demanant-los com ho havien fet.

Vaig xifrar el conte "L'eufòria dels troians" de Quim Monzó, del llibre "El Perquè de tot plegat" publicat per Quaderns crema l'any 1993, dividit en 21 parts. Vaig escollir aquest conte perquè no hi ha diàlegs.

Vaig utilitzar un xifratge de substitució monoalfabètic amb un alfabet de xifratge determinat, amb el qual vaig xifrar el primer text. Als següents textos vaig córrer cada cop un lloc l'ordre de les lletres de l'alfabet de xifratge. La frase que vaig utilitzar per crear l'alfabet és la següent:

ENGANYAR I VOLER FER CREURE QUE NO HA ESTAT AIXÍ

L'ordre de les lletres en l'alfabet era el següent:

ENGAYRIVOLFCUQHSTXZBÇDJKMPW

Aquest és el text que presentava els missatges xifrats que eren entregats als alumnes de Batxillerat:

> He interceptat un text xifrat.
> Sé que l'original està escrit en català i que l'enemic ha utilitzat l'alfabet habitual A-Z (de 27 caràcters, amb la ç) mantenint els espais en blanc però sense signes de puntuació. Ignoro totalment quina clau ha utilitzat l'enemic per xifrar el text, encara que, probablement, es tracti d'algun mètode de xifratge per substitució, que es pot trencar amb **l'anàlisi de freqüències**.
> AJUT: http://bibliotecnica.upc.es/cambranegra/crackingsubstitution.html
> http://www.xtec.cat/~jjareno/activitats/criptologia/idees.htm
>
> Necessito que m'ajudis a desxifrar-lo. Et passo una part del text xifrat numerada. Així, quan tingui totes les parts desxifrades, podrem llegir el missatge complet.

Si vols confirmar el valor d'alguna lletra o tens algun dubte o necessites una pista o bé si ja tens la solució, pots contactar amb mi a l'adreça: rzuloagageli@gmail.com
Si necessites una còpia via e-mail del text xifrat, escriu-me i te l'enviaré (no oblidis indicar de quin fragment es tracta).

Un cop em contestaven, els enviava el següent qüestionari realitzat amb *Google Docs*:

Has començat fent un recompte de freqüències de les lletres? (si/no)

Si has contestat SI : Manual o utilitzant la web?
Si has contestat NO: Com has començat?

Quina estratègia has utilitzat per determinar la A i la E quan has sabut quines eren les dues lletres més freqüents al text xifrat?
- He vist una d'aquestes lletres sola i he determinat que no podia ser la E (havia de ser la A)
- He analitzat els trios que més es repetien al text xifrat i he determinat quin corresponia a la paraula QUE (amb això he trobat la Q, la U, la E i la A)
- He analitzat les paraules de dues lletres que més es repetien al text xifrat i que podien correspondre a AL, EN, EL, ES, LA, etc.
- Un altre mètode: (especifica'l)

Quines lletres has determinat en segon lloc? Quina estratègia has utilitzat?
- He buscat dígrafs (dues lletres iguals) que havien de ser SS, LL, MM, o RR
- He buscat lletres soles que només podien ser I, O, D', L', S', N', M' i T'
- He analitzat els trios del text xifrat que podien correspondre a ELS, LES, UNS, ... ja que acabaven amb la mateixa lletra que la paraula següent (i que podia ser la S)
- Altres mètodes: (especifica'ls)

Com has continuat?

Has anat substituint les lletres a mà o amb la web?

Quant de temps has tardat?

Només he rebut 3 respostes fins al dia d'avui, i amb tan poques mostres és impossible fer un estudi.

7. THE CIPHER CHALLENGE

Com a treball de camp m'he proposat desxifrar tres dels missatges proposats per Simon Singh al llibre THE CODE BOOK a l'apartat "The Cipher Challenge" (el repte de les xifres), un desafiament de deu missatges xifrats, cada un més difícil que l'anterior, on s'atorgaven 15.000 $ al primer que ho aconseguís. Els deu missatges es van poder desxifrar l'any 2000, un any després de la publicació del llibre. L'idioma dels missatges són l'anglès, el llatí i el francès, respectivament.

Utilitzaré diversos programes on-line per ajudar-me a fer els anàlisis de freqüències, les substitucions, etc.[17]

7.1. Xifratge de substitució monoalfabètic

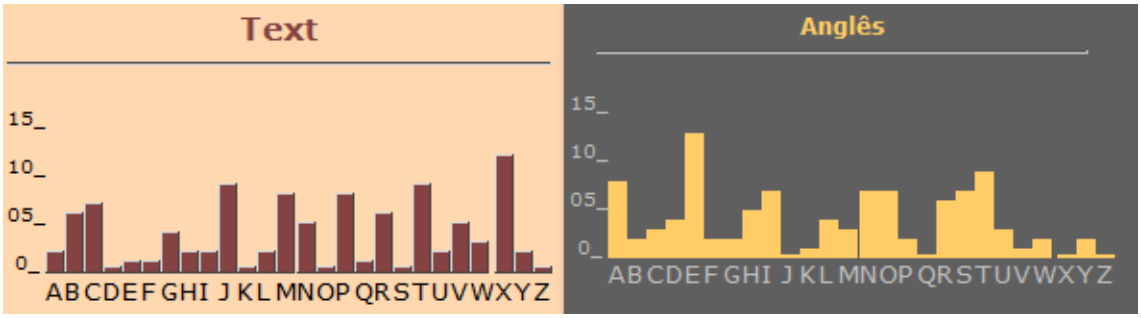
El primer de tots està xifrat amb un mètode de substitució monoalfabètic. És el següent:

> BT JPX RMLX PCUV AMLX ICVJP IBTWXVR CI M LMT'R PMTN, MTN YVCJX CDXV MWMBTRJ JPX AMTNGXRJBAH UQCT JPX QGMRJXV CI JPX YMGG CI JPX HBTW'R QMGMAX; MTN JPX HBTW RMY JPX QMVJ CI JPX PMTN JPMJ YVCJX. JPXT JPX HBTW'R ACUTJXTMTAX YMR APMTWXN, MTN PBR JPCUWPJR JVCUFGXN PBL, RC JPMJ JPX SCBTJR CI PBR GCBTR YXVX GCCRXN, MTN PBR HTXXR RLCJX CTX MWMBTRJ MTCJPXV. JPX HBTW AVBXN MGCUN JC FVBTW BT JPX MRJVCGCWXVR, JPX APMGNXMTR, MTN JPX RCCJPRMEXVR. MTN JPX HBTW RQMHX, MTN RMBN JC JPX YBRX LXT CI FMFEGCT, YPCRCXDXV RPMGG VXMN JPBR YVBJBTW, MTN RPCY LX JPX BTJXVQVXJMJBCT JPXVXCI, RPMGG FX AGCJPXN YBJP RAMVGXJ, MTN PMDX M APMBT CI WCGN MFCUJ PBR TXAH, MTN RPMGG FX JPX JPBVN VUGXV BT JPX HBTWNCL. JPXT AMLX BT MGG JPX HBTW'R YBRX LXT; FUJ JPXE ACUGN TCJ VXMN JPX YVBJBTW, TCV LMHX HTCYT JC JPX HBTW JPX BTJXVQVXJMJBCT JPXVXCI. JPXT YMR HBTW

[17] Els programes es troben a les següents pàgines web:
http://www.numaboa.com/criptografia/substituicoes/polialfabeticas/506-vigenere
http://www.numaboa.com/criptografia/criptoanalise/309-Ferramenta-de-frequencia
http://bibliotecnica.upc.es/cambranegra/frequencypuzzle.htm

FXGRPMOOMV WVXMJGE JVCUFGXN, MTN PBR ACUTJXTMTAX YMR APMTWXN BT PBL, MTN PBR GCVNR YXVX MRJCTBRPXN. TCY JPX KUXXT, FE VXMRCT CI JPX YCVNR CI JPX HBTW MTN PBR GCVNR, AMLX BTJC JPX FMTKUXJ PCURX; MTN JPX KUXXT RQMHX MTN RMBN, C HBTW, GBDX ICVXDXV; GXJ TCJ JPE JPCUWPJR JVCUFGX JPXX, TCV GXJ JPE ACUTJXTMTAX FX APMTWXN; JPXVX BR M LMT BT JPE HBTWNCL, BT YPCL BR JPX RQBVBJ CI JPX PCGE WCNR; MTN BT JPX NMER CI JPE IMJPXV GBWPJ MTN UTNXVRJMTNBTW MTN YBRNCL, GBHX JPX YBRNCL CI JPX WCNR, YMR ICUTN BT PBL; YPCL JPX HBTW TXFUAPMNTXOOMV JPE IMJPXV, JPX HBTW, B RME, JPE IMJPXV, LMNX LMRJXV CI JPX LMWBABMTR, MRJVCGCWXVR, APMGNXMTR, MTN RCCJPRMEXVR; ICVMRLUAP MR MT XZAXGGXTJ RQBVBJ, MTN HTCYGXNWX, MTN UTNXVRJMTNBTW, BTJXVQVXJBTW CI NVXMLR, MTN RPCYBTW CI PMVN RXTJXTAXR, MTN NBRRCGDBTW CI NCUFJR, YXVX ICUTN BT JPX RMLX NMTBXG, YPCL JPX HBTW TMLXN FXGJXRPMOOMV; TCY GXJ NMTBXG FX AMGGXN, MTN PX YBGG RPCY JPX BTJXVQVXJMJBCT. JPX IBVRJ ACNXYCVN BR CJPXGGC.

Començo fent un anàlisi de freqüències del text i buscant la freqüència de les lletres en l'anglès:



Sembla ben probable que la X en el text correspongui a la E real. A més a més, observo que el trio de lletres JPX apareix molt en el text. Com que la freqüència de la J en el text s'assembla molt a la T real, sembla molt probable que JPX sigui THE, el trio més comú de l'anglès. A més a més, la lletra M apareix sola unes quantes vegades. La única lletra que apareix sola en l'anglès és la A, així que ja tinc una altra lletra. El trio MTN ha de correspondre a ARE o AND, i com que ja hem trobat la E llavors correspon a AND. Al principi del missatge hi apareix la parella BT. Com que sabem que la T és la

N, BT pot ser ON o IN, ja que AN queda descartat perquè la à no és la B. M'arrisco i dic que és IN.

Sembla que l'he encertada, ja que m'apareix la paraula INTEvqvETATIcN, on les lletres majúscules són les lletres del text pla i les minúscules del text xifrat. Sembla llavors que aquesta paraula és INTERPRETATION; per tant, V correspon a R, Q a P i C a O. També hi trobo diverses vegades Oi, que segur que correspon a OF. Després dels apòstrofs hi trobo sempre la lletra R. Com que la T (de DON'T, ISN'T, etc) no pot ser perquè ja tenim la T, ha de ser per força la S. Ara hi trobo la paraula AwAINST, així que amb tota seguretat la W correspon a la G. També trobo yROTE, que ens indica que la Y correspon a la W. A més a més, l'aparició de hING diverses vegades em senyala que la H correspon a la K. La paraula KINGDOl em suggereix que la L correspon a la M.

Paraules com FOREdER o OdER em fa pensar que la D correspon a la V. uNDERSTANDING i uPON em fan veure que, curiosament, la U correspon a la U mateixa. Ara trobo al text kUEEN, que em fa creure que la K correspon a la Q. THE KING'S PAgAaE sembla "the king's palace". Per tant, la G correspon a la L i la A a la C. TROUfLED i fRING em diu que la F correspon a la B. HOLe, SAe i BABeLON em fa veure que la E correspon a la Y. Sé que la Z correspon a la X per la paraula EzXELLENT, i que la S correspon a la J per sOINTS. L'única parella que em queda és la O que correspon a la Z. Un cop fetes totes les parelles, podem crear la següent taula de correspondència:

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

El text pla, finalment, és aquest:

> In the same hour came forth fingers of a man's hand, and wrote over against the candlestick upon the plaster of the wall of the king's palace; and the king saw the part of the hand that wrote. Then the king's countenance was changed, and his thoughts troubled him, so that the joints of his loins were loosed, and his knees smote one against another. The king cried aloud to bring in the astrologers, the Chaldeans, and the soothsayers. And the king spake, and said to the wise men of Babylon, whosoever shall read this writing, and show me the interpretation thereof, shall be clothed with scarlet, and have a chain of gold about his neck, and shall be the third ruler in the kingdom. Then came in all the king's wise men; but they could not read the writing, nor make known to the king the interpretation thereof. Then was King Belshazzar greatly troubled, and his countenance was changed in him, and his lords were astonished. Now the queen, by reason of the words of the king and his lords, came into the banquet house; and the queen spake and said, o king, live forever; let not thy thoughts trouble thee, nor let thy countenance be changed; there is a man in thy kingdom, in whom is the spirit of the holy gods; and in the days of thy father light and understanding and wisdom, like the wisdom of the gods, was found in him; whom the King Nebuchadnezzar thy father, the king, I say, thy father, made master of the magicians, astrologers, Chaldeans, and soothsayers; forasmuch as an excellent spirit, and knowledge, and understanding, interpreting of dreams, and showing of hard sentences, and dissolving of doubts, were found in the same Daniel, whom the king named Belteshazzar; now let Daniel be called, and he will show the interpretation. The first codeword is Othello.

Els mots "spake" (en l'anglès actual "spoke") i "loosed" ("lost") i l'aparició de la forma personal "thou" (i el seu possessiu "thy") m'han fet veure que correspon a un text en anglès medieval, segurament un passatge de la Bíblia. Buscant per Internet, he trobat que es tracta del passatge de l'Antic Testament Daniel 5:5-12. La frase en color ha sigut afegida per Simon Singh i ens aporta una paraula clau.

7.2. Xifratge tipus Juli Cèsar

El següent text està xifrat amb un mètode de Juli Cèsar. Aquest és molt fàcil de desxifrar, ja que només hem de provar les 25 claus possibles. El text és el següent:

> MHILY LZA ZBHL XBPZXBL MVYABUHL HWWPBZ JSHBKPBZ JHLJBZ KPJABT HYJHUBT LZA ULBAYVU

Després d'unes quantes proves, descobreixo que la clau és 7, i el missatge original, en llatí, és:

> "Faber est suae quisque fortunae." Appius Claudius Caecus. Dictum arcanum est Neutron.

La cita d'Appius Claudius Caecus es pot traduir com a "Cadascú és el forjador de la seva fortuna/destí". També en aquest cas Singh ha aportat les paraules en color, les quals es poden traduir com a "La paraula clau és Neutron".

7.3. Xifratge Vigenère

L'últim text està xifrat amb Vigenère i el seu idioma és el francès:

> KQOWE FVJPU JUUNU KGLME KJINM WUXFQ MKJBG WRLFN FGHUD WUUMB SVLPS NCMUE KQCTE SWREE KOYSS IWCTU AXYOT APXPL WPNTC GOJBG FQHTD WXIZA YGFFN SXCSE YNCTS SPNTU JNYTG GWZGR WUUNE JUUQE APYME KQHUI DUXFP GUYTS MTFFS HNUOC ZGMRU WEYTR GKMEE DCTVR ECFBD JQCUS WVBPN LGOYL SKMTE FVJJT WWMFM WPNME MTMHR SPXFS SKFFS TNUOC ZGMDO EOYEE KCPJR GPMUR SKHFR SEIUE VGOYC WXIZA YGOSA ANYDO EOYJL WUNHA MEBFE LXYVL WNOJN SIOFR WUCCE SWKVI DGMUC GOCRU WGNMA AFFVN SIUDE KQHCE UCPFC MPVSU DGAVE MNYMA MVLFM AOYFN TQCUA FVFJN XKLNE IWCWO DCCUL WRIFT WGMUS WOVMA TNYBU HTCOC WFYTN MGYTQ MKBBN LGFBT WOJFT WGNTE JKNEE DCLDH WTVBU VGFBI JGYYI DGMVR DGMPL SWGJL AGOEE KJOFE KNYNO LRIVR WVUHE IWUUR WGMUT JCDBN KGMBI DGMEE YGUOT DGGQE UJYOT VGGBR UJYS

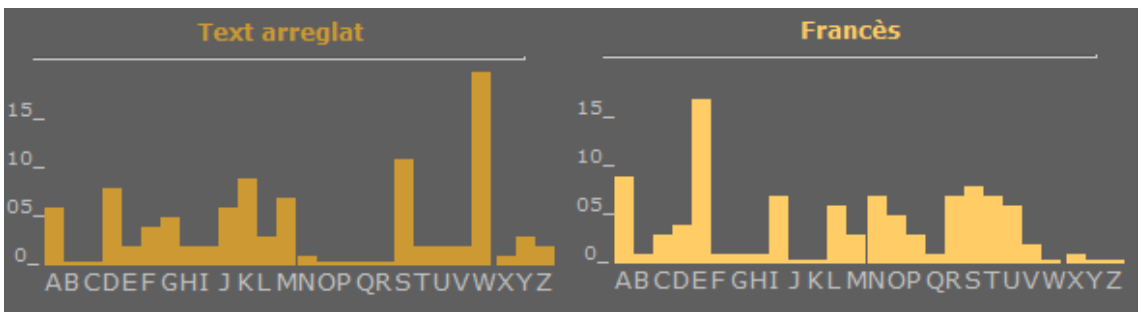
Començo l'Atac de Kasiski buscant repeticions de grups de lletres al text:

KQOWEFVJPUJUUNUKGLMEKJINMWUXFQMKJBGWRLFNFGHUDWU
UMBSVLPSNCMUEKQCTESWREEKOYSSIWCTUAXYOTAPXPLWPNTC
GOJBGFQHTDWXIZAYGFFNSXCSEYNCTSSPNTUJNYTGGWZGRWUU
NEJUUQEAPYMEKQHUIDUXFPGUYTSMTFFSHNUOCZGMRUWEYTR
GKMEEDCTVRECFBDJQCUSWVBPNLGOYLSKMTEFVJJTWWMFMWP
NMEMTMHRSPXFSSKFFSTNUOCZGMDOEOYEEKCPJRGPMURSKHFR
SEIUEVGOYCWXIZAYGOSAANYDOEOYJLWUNHAMEBFELXYVLWN
OJNSIOFRWUCCESWKVIDGMUCGOCRUWGNMAAFFVNSIUDEKQHC
EUCPFCMPVSUDGAVEMNYMAMVLFMAOYFNTQCUAFVFJNXKLNEI
WCWODCCULWRIFTWGMUSWOVMATNYBUHTCOCWFYTNMGYTQ
MKBBNLGFBTWOJFTWGNTEJKNEEDCLDHWTVBUVGFBIJGYYIDGM
VRDGMPLSWGJLAGOEEKJOFEKNYNOLRIVRWVUHEIWUURWGMUT
JCDBNKGMBIDGMEEYGUOTDGGQEUJYOTVGGBRUJYS

Les distàncies entre aquests grups de paraules repetides són de: 5, 55, 165, 80, 190, 220, etc. Podem veure clarament que el m.c.d. de tots aquests nombres és el 5. Per tant, la longitud de la clau és 5. Ara separem el text agrupant les lletres en cinc grups. Al primer grup hi van les lletres de les posicions 1, 6, 11..., al segon grup les de les posicions 2, 7, 12..., i així successivament.

Ara he fet anàlisis de freqüències per separat a cada un dels grups i he determinat quina és la clau del mètode de Juli Cèsar que se'ls aplica. Faig un exemple amb el primer grup:

KFJKKWMWFWSNKSKIAAWGFWYSYSJGWJAKDGMHZWGDEJWLSF
WWMSSTZEKGSSVWYAEWMLWSWSDGWASKUMDMMATFXIDWWW
THWMMLWWJDWVJDDSAKKLWIWJKDYDUVU



D'aquest gràfic podem deduir que el desplaçament realitzat a aquest primer grup és de 18, és a dir, la lletra S, ja que és el valor que li correspon segons la taula de la pàgina 16. He fet el mateix amb la resta de grups i he arribat a la conclusió que la clau és SCUBA, i que el text pla és aquest:

> SOUVE NTPOU RSAMU SERLE SHOMM ESDEQ UIPAG EPREN NENTD ESALB ATROS VASTE SOISE AUXDE SMERS QUISU IVENT INDOL ENTSC OMPAG NONSD EVOYA GELEN AVIRE GLISS ANTSU RLESG OUFFR ESAME RSAPE INELE SONTI LSDEP OSESS URLES PLANC HESQU ECESR OISDE LAZUR MALAD ROITS ETHON TEUXL AISSE NTPIT EUSEM ENTLE URSGR ANDES AILES BLANC HESCO MMEDE SAVIR ONSTR AINER ACOTE DEUXC EVOYA GEURA ILECO MMEIL ESTGA UCHEE TVEUL ELUIN AGUER ESIBE AUQUI LESTC OMIQU EETLA IDLUN AGACE SONBE CAVEC UNBRU LEGUE ULELA UTREM IMEEN BOITA NTLIN FIRME QUIVO LAITL EPOET EESTS EMBLA BLEAU PRINC EDESN UEESQ UIHAN TELAT EMPET EETSE RITDE LARCH ERBAU DELAI REEXI LESUR LESOL AUMIL IEUDE SHUEE SLEMO TPOUR ETAGE QUATR EESTT RAJAN SESAI LESDE GEANT LEMPE CHENT DEMAR CHER

Si l'arreglem, surt aquest missatge:

> Souvent pour s'amuser les hommes d'équipage prennent des albatros vastes oiseaux des mers qui suivent indolents compagnons de voyage le navire glissant sur les gouffres amers à peine les ont ils déposés sur les planches que ces rois de l'azur maladroits et honteux laissent piteusement leurs grandes ailes blanches comme des avirons trainer a cote d'eux ce voyageur aile comme il est gauche et veule lui naguère si beau qu'il est comique et laid l'un agace son bec avec un brule gueule l'autre mime en boitant l'infirme qui volait le poète est semblable au prince des nuées qui hante la tempête et se rit de l'archer Baudelaire exile sur le sol au milieu des huées le mot pour étage quatre est Trajan ses ailes de géant l'empêchent de marcher

La paraula “Baudelaire” m’ha donat una pista. Quan he buscat a *Google* “Baudelaire albatros” he trobat un poema de l’artista francès titulat *L’Albatros* (*Les fleurs du mal*, 1859), la lletra del qual coincideix amb el missatge xifrat per Singh, exceptuant els mots de color al paràgraf anterior, on ens indica que la clau és “Trajan”. El poema original és aquest:

***L'Albatros* de Charles Baudelaire (Les fleurs du mal, 1859)**

Souvent pour s'amuser, les hommes d'équipage
Prennent des albatros, vastes oiseaux des mers,
Qui suivent, indolents compagnons de voyage,
Le navire glissant sur les gouffres amers.
À peine les ont-ils déposés sur les planches,
Que ces rois de l'azur, maladroits et honteux,
Laissent piteusement leurs grandes ailes blanches
Comme des avirons traîner à côté d'eux.
Ce voyageur ailé, comme il est gauche et veule !
Lui, naguère si beau, qu'il est comique et laid !
L'un agace son bec avec un brûle-gueule,
L'autre mime, en boitant, l'infirme qui volait !
Le poète est semblable au prince des nuées
Qui hante la tempête et se rit de l'archer;
Exilé sur le sol au milieu des huées,
Ses ailes de géant l'empêchent de marcher.

8. CONCLUSIONS

Els dos objectius que em vaig plantejar a l'inici del treball han quedat plenament assolits. Tot seguit exposo les conclusions que he extret de la meva investigació:

- **El rol de la criptografia en l'actualitat**

Quan la gent em preguntava de què feia el Treball de Recerca i jo responia "de criptografia", la majoria em posaven cara de no saber de què els estava parlant. Els altres tenien la mateixa visió de la criptografia que tenia jo abans de fer el treball, la visió que ens aporten les pel·lícules i novel·les d'intriga: missatges xifrats de forma estranya que revelaven la ubicació d'un lloc secret o una conspiració contra algú. Si bé és cert que la criptografia pot fer aquesta funció, he vist que la majoria desconeix la seva aplicació en el món actual. Sense criptografia, el món digital i telemàtic actual -on comprar per Internet o pagar amb la targeta de crèdit són el pa de cada dia- no podria existir.

En els seus inicis, la criptografia només s'usava en els àmbits polític i militar, i el seu ús ha repercutit fortament en la història mundial. El desxiframent de l'ENIGMA només n'és un exemple. Però en els últims seixanta anys, amb l'aparició de la informàtica, la criptografia ha hagut d'estendre's al món civil, per tal de protegir la privacitat de les persones, físiques i jurídiques.

La invenció del protocol d'intercanvi de claus Diffie-Hellman-Merkle, en un principi, i del sistema RSA, més tard, ha revolucionat el panorama de la criptografia. Ja no cal contactar amb algú personalment abans de comunicar-s'hi amb algun mètode criptogràfic, malgastant diners i recursos en el procés. La criptografia quàntica, que s'imposarà en un futur, és un pas més en l'evolució de la criptografia.

- **L'existència d'un criptosistema completament segur**

Al llarg de la història, diversos mètodes per xifrar missatges han sigut considerat segurs: la Xifra Vigenère (que va guanyar el sobrenom de "la xifra indesxifrable"), la màquina ENIGMA... Aquests sistemes han sigut finalment trencats, destruint el seu mite d'invulnerabilitat.

La Xifra de Vernam també ha sigut catalogada d'"indesxifrable", sempre que es garanteixin unes condicions, i podríem caure en l'error de dir que només seguirà així fins que algú trobi una manera de trencar-la. No obstant, s'ha provat matemàticament que aquesta Xifra és realment indesxifrable.

El *quid* de la qüestió és trobar un mètode segur per enviar la clau d'amagat d'un espia. La criptografia quàntica, que podria ser confosa amb un seguit de xifres que utilitzen propietats de la mecànica quàntica, es dedica justament a trobar maneres de poder realitzar aquesta tasca. El BB84 i l'E91 són de moment els únic mètodes ideats, però podem esperar que en un futur s'inventin mètodes més segurs o més pràctics.

Tot i així, el que avui en dia és indesxifrable demà pot no ser-ho. L'aparició d'una conferència a finals de desembre on s'explica que s'ha trobat una manera de trencar el protocol BB84 només n'és l'exemple més recent.

Per acabar, val a dir que per molt que un mètode sigui indesxifrable, sempre es pot aconseguir la informació desitjada d'altres maneres. Per exemple, si Alice envia a Bob un missatge xifrat amb One-Time Pad i Eve vol saber què diu, pot anar a buscar a Bob i obligar-lo a que li digui la clau o directament el contingut del missatge.

- **Què més he extret en la realització d'aquest treball?**

El contacte amb el meu tutor extern de la UAB, Jordi Mompart, m'ha descobert el món de la criptografia quàntica, de la qual jo no en tenia ni la més remota idea. Gràcies a la

visita a l'Institut de Ciències Fotòniques de Castelldefels i a les explicacions de Noelia González i Gabriel Molina he vist com és i com es treballa en un laboratori d'investigació quàntica.

La part teòrica del treball m'ha permès practicat el xifratge de cada un dels sistemes esmentats, ja que jo mateix he xifrat tots els exemples que hi apareixen. També m'ha permès trobar *applets* que em permetessin fer operacions vàries (xifrar, desxifrar, fer anàlisis de freqüències, etc.). La part pràctica del treball m'ha servit per poder aplicar els meus coneixements teòrics del desxiframent de missatges a informació xifrada real.

He gaudit molt fent aquest Treball de Recerca. A part dels amplis coneixements de criptografia que m'ha proporcionat, m'ha ajudat a saber com es fa un treball i en quin ordre s'han de fer les coses; així com a buscar informació arreu i contrastar-la amb altres fonts. A més, també ha servit per poder practicar el meu anglès amb la lectura del llibre de Simon Singh.

9. BIBLIOGRAFIA

Pàgines web

- <http://www.xtec.net/~jjareno/activitats/criptologia/intro.htm>

Web interactiva on es pot practicar amb diversos mètodes de xifratge.

- <http://enigmaco.de/enigma/enigma.swf>

Simulador de la màquina ENIGMA.

- <www.xtec.net/~dobrador/cripto/index.htm>

Explicació de l'RSA on es pot interactuar amb la calculadora WIRIS.

- <http://events.ccc.de/congress/2009/Fahrplan/events/3576.en.html>

Pàgina web del congrés realitzat el 27/12/09 on es revelava que es pot atacar al sistema BB84.

- <http://www.simonsingh.net/The_Ciphertexts.html>

Web on es troben els missatges per desxifrar que Simon Singh proposa a "The Cipher Challenge"

Llibres

- *L'art de la comunicació secreta*. JUHER BARROT, David. 2004 Barcelona: Llibres de l'índex.
- *Introducció a la criptografia*. JUHER BARROT, David. 2000 Girona: Universitat de Girona.
- *The Code Book*. SINGH, Simon. 2000 Nova York: Anchor Books.

Altres

- Visita a l'Institut de Ciències Fotòniques (ICFO), Castelldefels. [1-12-2009]
- Arxius PDF sobre criptografia quàntica, de Jordi Mompart. [19-2-2009]

ANNEXOS

DEMOSTRACIÓ DE LES LIMITACIONS DELS CRIPTOSISTEMES AFINS

La limitació dels possibles valors de *m* en les funcions dels criptosistemes afins *f(x) = mx + n (mod p)* ve determinat per la possibilitat de crear una funció inversa. Només les funcions injectives, on a cada imatge *y* li correspon només una antiimatge *x*, poden tenir inversa. En un criptosistema afí només ens interessen les funcions injectives, ja que és necessari que a cada lletra del text xifrat li'n correspongui només una del text pla, perquè sinó l'operació desxifradora seria impossible.

D'aquesta manera el problema es trasllada a trobar els valors que poden prendre *m* i *n* perquè existeixi $f(x)^{-1}$. Llavors, per a una funció xifradora *f(x):*

$$f(x)= y = mx + n \ (mod\ p) \rightarrow \quad f^{-1}(y)= x = m^{-}1\cdot y - m^{-1}\cdot n \ (mod\ p).$$

Existeix un teorema que diu: m^{-1} *(mod p) existeix si, i només si, mcd(m,p) = 1*. Per tant, *m* no pot ser un divisor de *p*. Per això en un alfabet de 26 lletres, és a dir, *p = 26*, *m* només pot prendre els valors senars de l'1 al 25 exceptuant el 13, ja que els divisors de 26 són 2 i 13. De la mateixa manera, en un alfabet de 27 lletres, com el català o el castellà, *m* pot prendre qualsevol valor exceptuant els múltiples de 3, ja que l'únic divisor primer de 27 és 3, perquè $27 = 3^3$.

A partir d'aquí podríem començar la recerca del valor de m^{-1}, però per fer-ho necessitarem abans uns coneixements previs. La identitat de Bézout[18] diu:

$$Si\ a,b\in Z \quad i \quad d=mcd(a,b) \quad \Rightarrow \quad \exists\, r,s\in Z \quad tal\ que \quad d=a\cdot r+b\cdot s$$

[18] La identitat de Bézout és una equació diofàntica (que només admet solucions enteres) de la forma ax+by=c. Aquesta equació només té solució si i només si el mcd(a,b) és un divisor de c.

Si utilitzem la identitat de Bézout als criptosistemes afins amb *m* i *p*, podem veure que

$$1 = m \cdot r + p \cdot s \ (mod\ p) = m \cdot r \ (mod\ p) \rightarrow m^{-1} = r \ (mod\ p).$$

Com trobem ara *r*? Utilitzant l'algorisme d'Euclides ampliat[19] amb els nombres *m* i *p*, que ens donarà el valor del *mcd(m,p)* i de les constants *r* i *s* de la identitat de Bézout.

Abans de tot, explicaré el mètode a seguir amb dos nombres qualssevol *a* i *b*. Per exemple, utilitzem l'algorisme d'Euclides amb *a = 256* i *b = 90*.

- Considerem $a = R_{-2}$ i $b = R_{-1}$:
- R_i és el residu de la divisió entera de R_{i-2} entre R_{i-1} i Q_i n'és el quocient.
- En cada iteració calculem els valors $A_i = Q_i \cdot A_{i-1} + A_{i-2}$ i $B_i = Q_i \cdot B_{i-1} + B_{i-2}$ (amb $A_{i-2}=0$, $A_{i-1}=1$, $B_{i-2}=1$ i $B_{i-1}=0$)
- Quan $R_k=0$ acabem

	i = - 2	i = - 1	i = 0	i = 1	i = 2	i = 3	i = 4
B_i	1	0	1	1	6	13	-
A_i	0	1	2	3	17	37	-
Q_i			2	1	5	2	3
R_i	256	90	76	14	6	2	0

A partir d'aquesta taula podem trobar el màxim comú divisor de 256 i 90, així com els valors de *r* i *s* de la identitat de Bézout.

El mcd (a, b) es troba a la casella R_{k-1}, on $R_k = 0$. En aquest cas, *k = 4* i $R_3 = 2$ = mcd (256, 90).

Els valors de *r* i *s* són els següents:

[19] L'algorisme d'Euclides ampliat és una millora de l'algorisme d'Euclides de càlcul del màxim comú divisor de dos nombres enters, que dóna, a més del màxim comú divisor dels dos nombres, els coeficients de cadascun d'aquests dos nombres a la identitat de Bézout.

- $r = (-1)^{k-1}\cdot(-A_{k-1}) \rightarrow r = (-1)^3\cdot(-37) = 37$.
- $s = (-1)^{k-1}\cdot B_{k-1} \rightarrow s = (-1)^3\cdot 13 = -13$.

Podem comprovar que es compleix la identitat de Bézout:

$$1 = 37\cdot 90 + (-13)\cdot 256 = 3330 - 3328 = 2.$$

Fem-ho ara amb un criptosistema afí real, per exemple: $f(x) = 14\cdot x + 5 \ (mod\ 27)$, on, en l'alfabet català, C, de valor numèric 2, pren el valor de 6, és a dir, la lletra G. Per trobar la funció inversa utilitzem l'algorisme d'Euclides amb $p = 27$ i $m = 14$ per trobar el valor de r:

	i = - 2	i = - 1	i = 0	i = 1	i = 2
B_i	1	0	1	1	-
A_i	0	1	1	2	-
Q_i			1	1	1
R_i	27	14	13	1	0

Ara k pren el valor de 2, $r = 2$ i $s = -1$. Ho comprovem: $1 = 2\cdot 14 + (-1)\cdot 27 = 28 - 27 = 1$. Com que $m^{-1} = r \ (mod\ p)$, $14^{-1} = 2 \ (mod\ 27)$.

Abans hem arribat a la conclusió que $f(x)^{-1} = m^{-1}\cdot x - m^{-1}\cdot n \ (mod\ p)$. Si ho apliquem a aquest criptosistema afí en concret, trobem que

$$f(x)^{-1} = 14^{-1}\cdot x - 14^{-1}\cdot 5 \ (mod\ 27) = 2\cdot x - 2\cdot 5 \ (mod\ 27) = 2\cdot x - 10 \ (mod\ 27).$$

Si ara ho comprovem amb la lletra G, de valor numèric 6, veurem que

$f(6)^{-1} = 2\cdot 6 - 10 \ (mod\ 27) = 12 - 10 \ (mod\ 27) = 2 \ (mod\ 27) = 2$, és a dir, la lletra C, com hem vist en un principi.

MILLORES DE SEGURETAT DELS CRIPTOSISTEMES AFINS

Una de les formes més senzilles de millorar els criptosistemes afins és usant dígrafs, és a dir, grups de dues lletres juntes. Abans de tot, però, hem de donar un valor numèric a cada dígraf. En un alfabet de 27 lletres un dígraf de la forma AB, on *x* i *y* són els valors numèrics d'A i B, respectivament, pren el valor $27 \cdot x + y$. Per exemple, el dígraf MP pren el valor de $27 \cdot 13 + 16 = 367$.

Un cop tenim el valor numèric del dígraf li apliquem una funció xifradora $f(x) = m \cdot x + n \pmod{p^2}$, on *p* és el nombre de lletres de l'alfabet i *m* por prendre qualsevol valor menys el d'un múltiple d'un factor primer[20] de *p*, és a dir, el *mcd (m,p)* ha de ser 1. Per exemple, $f(x) = 17 \cdot x + 9 \pmod{27^2} = 17 \cdot x + 9 \pmod{729}$. En el cas del dígraf MP, si l'introduíssim a la funció anterior quedaria:

$$f(367) = 17 \cdot 367 + 9 \pmod{729} = 6239 + 9 \pmod{729} = 6248 \pmod{729} = 416$$

Ara hem de transformar el número obtingut de manera que en tinguem dos per tal de formar un altre dígraf, que és el que apareixerà al text xifrat. Els dos nombres seran el quocient i el residu de la divisió entre el nombre obtingut i *p*. En l'exemple, $416 = 27 \cdot 15 + 11$, és a dir, les lletres del nou dígraf prendran els valors de 15 i 11, per tant, les lletres O i K. Així, el dígraf MP es xifra com a OK.

Un cop aquí podem buscar la funció inversa desxifradora $f(x)^{-1}$. El procediment per trobar-la és el mateix que es descriu en l'Annex A. Per tant, utilitzem l'algorisme d'Euclides ampliat amb *m* i p^2.

[20] Tot això es troba demostrat més àmpliament a l'Annex A.

	i = - 2	i = - 1	i = 0	i = 1	i = 2	i = 3
B_i	1	0	1	1	8	-
A_i	0	1	42	43	343	-
Q_i			42	1	7	2
R_i	729	17	15	2	1	0

Calculem *r*, és a dir, el valor de $m^{-1} \pmod{p^2}$:

$$r = (-1)^{k-1} \cdot (-A_{k-1}) = (-1)^2 \cdot (-343) = -343 = 386 \pmod{729}$$

Un cop hem trobat el valor de m^{-1} podem trobar el valor de $f(x)^{-1}$:

$$f(x)^{-1} = m^{-1} \cdot x - m^{-1} \cdot n \pmod{p^2} = 386 \cdot x - (-343) \cdot 9 \pmod{729} = 386 \cdot x + 171 \pmod{729}$$

Si ara inserim 416, el valor numèric del dígraf OK, a la funció inversa, trobem que:

$$f(416)^{-1} = 386 \cdot 416 + 171 \pmod{729} = 160576 + 171 \pmod{729} = 160747 \pmod{729} = 367 = 27 \cdot 13 + 16$$

, nombres que corresponen a les lletres del dígraf MP.

* * *

Una altra manera de xifrar dígrafs és utilitzant matrius, amb el què es coneix com a **Xifra de Hill**. Aquesta xifra utilitza una funció matricial del tipus $f(x_1, x_2) = A \cdot X + B \pmod{p}$, on $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ i $B = \begin{pmatrix} e \\ f \end{pmatrix}$. Els valors de x_1 i x_2 són el valor numèric de cada una de les lletres del dígraf. Per exemple, en el cas del dígraf MP, la seva matriu associada és $\begin{pmatrix} 13 \\ 16 \end{pmatrix}$.

La única restricció en el valor de A és que sigui regular ($|A| \neq 0$) i que $mcd(|A|, p) = 1$.

Posem per exemple que la funció matricial *f* és:

$$f(x_1, x_2) = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} 9 \\ 2 \end{pmatrix} (\text{mod } 27)$$

Si ara hi introduïm el dígraf MP, llavors

$$f(13,16) = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 13 \\ 16 \end{pmatrix} + \begin{pmatrix} 9 \\ 2 \end{pmatrix} (\text{mod } 27) = \begin{pmatrix} 10 \\ 3 \end{pmatrix} + \begin{pmatrix} 9 \\ 2 \end{pmatrix} (\text{mod } 27) = \begin{pmatrix} 19 \\ 5 \end{pmatrix} (\text{mod } 27) = \begin{pmatrix} 19 \\ 5 \end{pmatrix}$$

que correspon al dígraf SE, en l'alfabet català.

Quan busquem la funció inversa, és a dir, la funció desxifradora, trobarem que $Y = A \cdot X + B \rightarrow A \cdot X = Y - B \rightarrow X = A^{-1} \cdot Y - A^{-1} \cdot B \rightarrow f(x_1, x_2)^{-1} = A^{-1} \cdot X - A^{-1} \cdot B \ (mod\ p)$.

Si ara busquem la funció inversa de la funció xifradora anterior, veurem que:

$$f(x_1, x_2)^{-1} = A^{-1} \cdot X - A^{-1} \cdot B \ (mod\ 27) = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} - \begin{pmatrix} 2 & 0 \\ -1 & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 9 \\ 2 \end{pmatrix} (\text{mod } 27) =$$

$$= \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} - \begin{pmatrix} 11 \\ 13 \end{pmatrix} (\text{mod } 27)$$

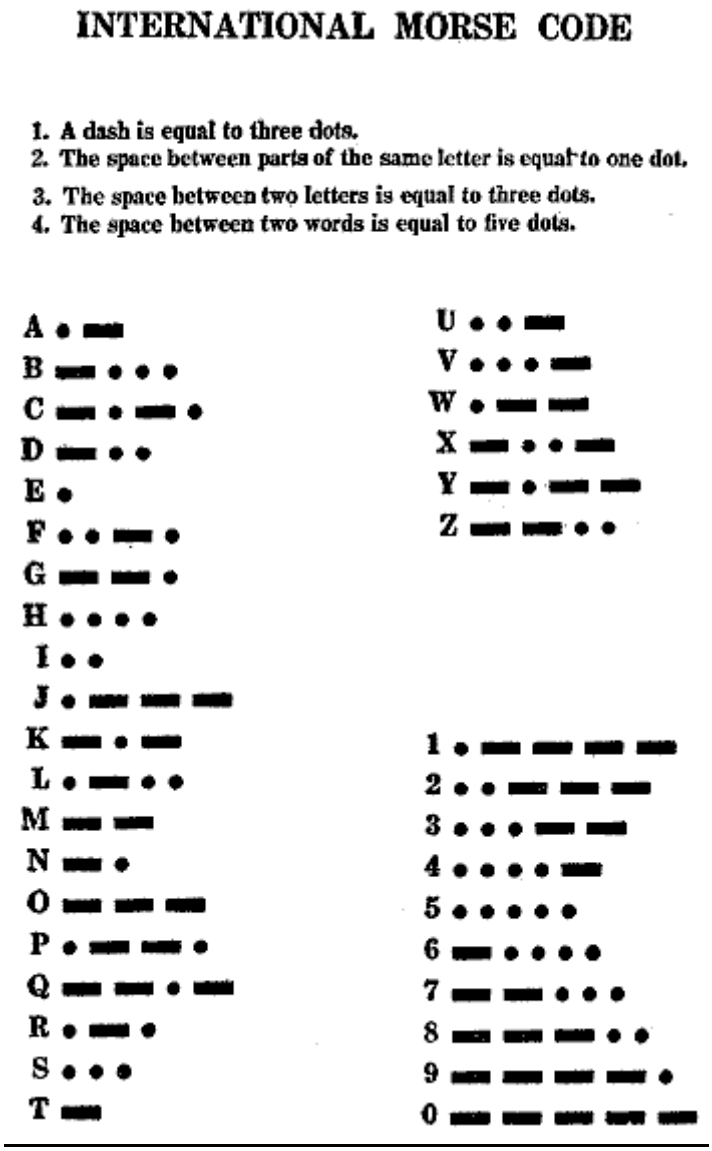
Comprovem-ho amb el dígraf SE:

$$f(19,5) = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 19 \\ 5 \end{pmatrix} - \begin{pmatrix} 11 \\ 13 \end{pmatrix} (\text{mod } 27) = \begin{pmatrix} 24 \\ 29 \end{pmatrix} - \begin{pmatrix} 11 \\ 13 \end{pmatrix} (\text{mod } 27) = \begin{pmatrix} 13 \\ 16 \end{pmatrix} (\text{mod } 27) = \begin{pmatrix} 13 \\ 16 \end{pmatrix},$$

que correspon al dígraf originari MP.

CODIS USATS EN EL MÓN PÚBLIC

CODI MORSE



INTERNATIONAL MORSE CODE

1. A dash is equal to three dots.
2. The space between parts of the same letter is equal to one dot.
3. The space between two letters is equal to three dots.
4. The space between two words is equal to five dots.

A	·−	U	··−
B	−···	V	···−
C	−·−·	W	·−−
D	−··	X	−··−
E	·	Y	−·−−
F	··−·	Z	−−··
G	−−·		
H	····		
I	··		
J	·−−−		
K	−·−	1	·−−−−
L	·−··	2	··−−−
M	−−	3	···−−
N	−·	4	····−
O	−−−	5	·····
P	·−−·	6	−····
Q	−−·−	7	−−···
R	·−·	8	−−−··
S	···	9	−−−−·
T	−	0	−−−−−

Traducció:

1. La durada d'una línia és igual a la de tres punts

2. L'espai entre dues parts d'una mateixa lletra dura el mateix que un punt.

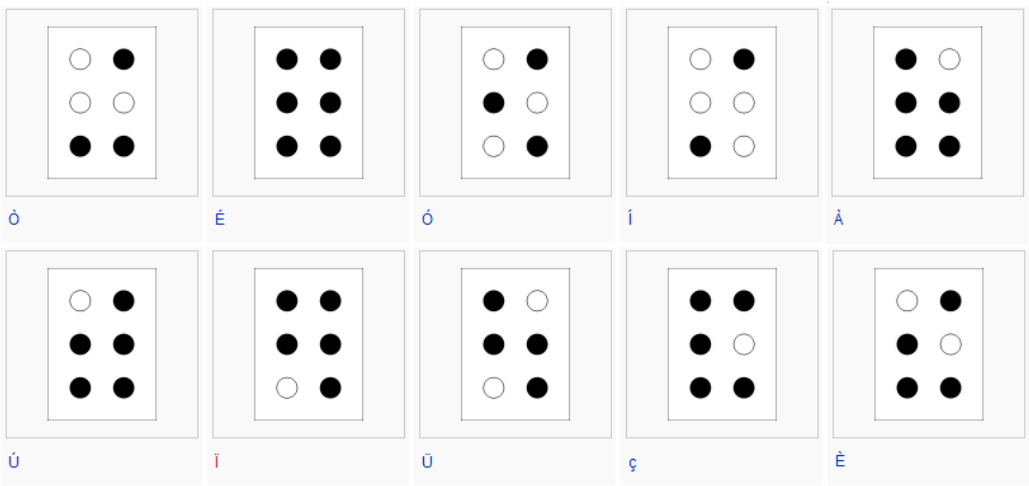
3. L'espai entre dues lletres dura igual que tres punts.

4. L'espai entre dues

ALFABET BRAILLE

Braille	significado	- Braille	significado	- Braille	significado
⠁	a , 1	⠞	t	⠷	á
⠃	b , 2	⠥	u	⠮	é
⠉	c , 3	⠧	v	⠌	í
⠙	d , 4	⠺	w	⠬	ó
⠑	e , 5	⠭	x	⠾	ú
⠋	f , 6	⠽	y	⠳	ü
⠛	g , 7	⠵	z		
⠓	h , 8	⠠	Signo de mayúsculas		
⠊	i , 9	⠼	Signo de número		
⠚	j , 0	⠲	Punto (.) *(punto 3)*		
⠅	k	⠂	Coma (,) *(punto 2)*		
⠇	l				
⠿	ll	⠦	Signos de interrogación (¿?)		
⠍	m	⠆	Punto y coma (;)		
⠝	n	⠖	Signos de exclamación (¡ !)		
⠻	ñ	⠒	Dos puntos (:)		
⠕	o	⠶	Comillas (de cualquier tipo)		
⠏	p	⠣	Abrir paréntesis "("		
⠟	q	⠜	Cerrar paréntesis ")"		
⠗	r	⠤	Guión (-)		
⠎	s		espacio *(ningún punto)*		

Aquesta és la versió de l'alfabet Braille en castellà. Per al català, només hi ha petits canvis i afegiments:

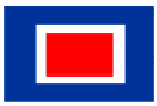


ALFABET FONÈTIC DE L'OTAN

Aquest és l'alfabet per paraules més utilitzat. S'empra tant en les comunicacions de tipus civil (policia, control aeri, etc.) com militar quan s'han de lletrejar sigles o noms. A cada lletra de l'alfabet li correspon una paraula en anglès que comenci per la mateixa lletra, i quan hi ha un caràcter que es repeteix la seva multiplicitat s'esmenta amb els prefixes "DOUBLE", "TRIPLE", etc. Quan s'han de lletrejar nombres amb decimals, per a indicar el punt es diu "DECIMAL".

Lletra	**Paraula**	**Lletra**	**Paraula**	**Lletra**	**Paraula**
A	Alfa	M	Mike	Y	Yankee
B	Bravo	N	November	Z	Zulu
C	Charlie	O	Oscar	1	One
D	Delta	P	Papa	2	Two
E	Eco	Q	Quebec	3	Three
F	Foxtrot	R	Romeo	4	Four
G	Golf	S	Sierra	5	Five
H	Hotel	T	Tango	6	Six
I	India	U	Uniform	7	Seven
J	Juliet	V	Victor	8	Eight
K	Kilo	W	Whisky	9	Nine
L	Lima	X	X-Ray	0	Zero

BANDERES DE SIGNES

	**A**	Tinc un bus sota aigua. Mantingui's allunyat i redueixi la velocitat.		**N**	Negatiu.
	**B**	Estic carregant, descarregant o transportant mercaderies perilloses.		**O**	Home a l'aigua.
	**C**	Afirmatiu.		**P**	*Al port:* Tothom a bord. El vaixell llença amarres.
	**D**	Maniobro amb dificultat. Mantingui's allunyat.		**Q**	El vaixell està "sa". Sol·licito lliure navegació.
	**E**	Estic virant cap a estribord.		**R**	Rebut.
	**F**	Tinc una averia. Comuniqui's amb mi.		**S**	Estic fent marxa enrere.
	**G**	Necessito un pràctic.		**T**	*Vaixells de pesca:* Estic pescant amb arrossegament en parella. Mantingui's allunyat.
	**H**	Tinc un pràctic a bord.		**U**	S'està dirigint vostè cap a un perill.
	**I**	Estic virant cap a babord.		**V**	Necessito auxili.
	**J**	Tinc un incendi i transporto mercaderies perilloses. Mantingui's allunyat.		**W**	Necessito assistència mèdica.
	**K**	Desitjo comunicar-me amb vostè.		**X**	Suspengui les maniobres y presti atenció als meus senyals.
	**L**	Detingui el vaixell immediatament.		**Y**	Estic maniobrant cap enrere par a fixar l'àncora.
	**M**	El meu vaixell està parat i no s'engega.		**Z**	Necessito un remolcador.