1. PRESENTACIÓ

Els motius pels quals vaig escollir fer el treball sobre criptografia van ser diversos: en primer lloc, en David Obrador em va proposar fer aquest treball, vaig buscar informació sobre el tema i em va semblar molt interessant. A més, la criptografia és una assignatura optativa dins la carrera de Telecomunicacions que possiblement estudiaré l'any vinent. Els objectius que em vaig proposar van ser els següents: conèixer els mètodes criptogràfics tot valorant la seva importància al llarg de la història, fer una recerca d'exemples de criptografia en el nostre entorn, aprendre a desxifrar codis de diferents dificultats, trobar les eines més adients per un desxiframent ràpid i arribar a conèixer si existeix algun mètode indesxifrable. A més volia seleccionar les fonts d'informació adequades tot comparant-les per tal d'assegurar-me que les informacions eren certes, sintetitzar sense entrar en qüestions matemàtiques de gran dificultat i estructurar la informació de manera coherent.

A l'estiu vaig començar el procès d'elaboració del treball de recerca amb la lectura del llibre *Los códigos secretos* d'en Simon Singh, un bon didacte en criptografia . El llibre em va proporcionar informació acurada sobre la criptografia i els principals mètodes criptogràfics i vaig fer un resum de tot el llibre que he utilitzat de guia i consulta per desenvolupar el treball. El segon pas va ser començar a desxifrar codis. Vull parar atenció en aquest punt ja que per mi ha estat el més difícil perquè un desxiframent requereix perseverança, paciència i sobretot molt de temps. Ara bé, un cop desxifrat he sentit molta satisfacció. Les fonts d'informació que he fet servir han estat llibres (faig especial esment a un llibre molt didàctic: *L'art de la comunicació secreta* del David Juher, professor de matemàtiques) i pàgines web de criptografia. Una eina molt útil que m'ha ajudat a desxifrar codis ha estat el CD-ROM del Simon Singh. A més he utilitzat diferents programes com l'Excel, el Word i el Paint per elaborar gràfics, taules, modificar les imatges i donar format al document.

Els continguts d'aquest treball de recerca sobre criptografia s'estructuren en diferents apartats els quals donen a conèixer els mètodes criptogràfics més importants de la història. Aquests estan ordenats segons la seva antiguitat (de més vells i elementals als actuals i complexos). Així, començo amb una introducció de la criptografia tot donant una definició d'aquesta i situant-la en un context; a l'apartat 3 explico la base d'un mètode criptogràfic els classifico de manera general segons la forma amb què s'han encriptat; el següent punt tracta el mètode que utilitzava l'emperador Cèsar per xifrar els seus missatges i he fet l'explicació matemàtica d'aquesta xifra; en l'apartat 5 exposo la tècnica de l'anàlisi de freqüència la qual utilitzo per trobar la solució a un missatge que una amiga em va xifrar. He afegit gràfics de barres per explicar el trencament del codi; el següent punt tracta la xifra Vigenère amb què es

va voler superar l'anàlisi de freqüència. Aquest apartat també inclou el desxiframent d'un missatge que vaig trobar proposat a Internet per un dels professors de criptografia de la UAB; deixant d'una banda els mètodes criptogràfics, a l'apartat 7 relaciono la criptografia amb l'esteganografia, una altra tècnica d'amagar missatges, i l'escriptura jeroglífica; el següent punt és una recerca de curiositats criptogràfiques i de missatges secrets amagats al nostre voltant; els apartats 9, 10 i 11 són una introducció a la criptografia actual, centrada en el món de la informàtica. El mètode RSA és, actualment, indesxifrable; l'ús de la criptografia en la nostra societat amb tècniques tant potents com RSA es debateixen al punt 12 del treball.

Per una altra banda, he inclòs un annex on aclareixo alguns apartats o amplio les informacions que no són imprescindibles per fer una lectura del treball. No obstant és útil per tal d'entendre amb més profunditat qüestions matemàtiques o d'altres relacionades amb allò que s'està explicant. També he elaborat un glossari ja que apareixen força tecnicismes els quals he decidit marcar amb negreta per aclarir el lector.

Al llarg del treball m'he trobat amb diferents dificultats. Per exemple he tingut problemes a l'hora de redactar alguns punts del treball de manera entenedora sense entrar en detalls de matemática superior. Això no ha estat fàcil si tenim en compte que els llibres utilitzen de deu a cinquanta pàgines per explicar un sol mètode criptogràfic. Per tant, el meu objectiu ha estat explicar la "filosofia" de cada mètode de la manera més senzilla i didàctica possible per veure així el gran salt realitzat en els últims anys.Tot i així, per fer aquesta síntesi he hagut de fer un estudi previ més detallat sobre els diferents temes.

També vull deixar justificat el diferent ús de les persones gramaticals. Malgrat que la major part de les vegades he fet una visió més distant i objectiva del treball (amb la tercera persona del singular) no em sentia a gust en alguns moments com per exemple quan s'han de seguir els passos d'un mètode, en aquestes situacions he fet una alusió directa al lector amb la segona persona del singular o bé amb la primera del plural.

Per últim vull agrair a tots els qui m'han ajudat amb el treball: al meu tutor David Obrador per engrescar-me amb el treball, per tot el temps dedicat i pels materials aportats. Al Raül per la seva paciència, la lectura del treball i per l'ajuda en alguns punts concrets. A la meva mare per llegir-se tot el treball de manera crítica i per aportar-me informació sobre les lleis que regulen la signatura digital. Al Víctor, que també fa el Treball de Recerca de criptografia, per la informació proporcionada i a la Bidea per elaborar-me codis per desxifrar.

2. INTRODUCCIÓ

Imagina que vols comunicar un missatge secret a una altra persona amb la qual no tens accés directe i per tant l'hi has de transmetre per Internet. Per Internet qualsevol missatge que circuli pot ser interceptat per una tercera persona (per explicar com s'aconsegueix això caldria un altre Treball de Recerca). Si vols que ningú de la xarxa intercepti i conegui el missatge, has d'utilitzar els mètodes existents per manipular la informació que conté el teu missatge amb la intenció que no sigui descobert per cap altra persona més que per aquella a qui vols que li arribi. O imagina't en una guerra on l'enemic pot obtenir informació secreta i pot acabar amb la teva vida. L'ésser humà té la necessitat de privacitat. Per tal d'ocultar la informació necessitaràs l'ajut de la criptografia.

La criptografia és l'art i la ciència de modificar i amagar (del grec κρψπτοζ (kryptos), "ocult" i γραπτοζ (graphos), "escrit") un missatge per tal que tingui una aparença nova irreconexible pel públic no autoritzat a conèixer el missatge original.

El desig de les nacions per mantenir secrets ha provocat, al llarg dels anys, que aquestes hagin format departaments encarregats de crear **codis**, **desxifrar**-los i posar en pràctica les diferents formes d'**encriptació** tot utilitzant les matemàtiques, la lingüística, la teoria de la informació i la teoria quàntica. Exemples d'aquests departaments són les Cambres Secretes de Bletchley Park de l'Anglaterra del 1939 per desxifrar la màquina Enigma dels nazis i la NSA (National Security Agency) a USA actualment on es controla la comunicació dels Estats Units i part del món.

Per escollir el **mètode criptogràfic** més adient cal tenir en compte les teves necessitats i sobretot les eines a l'abast. Per una altra banda, l'emissió d'un missatge xifrat pot aixecar sospites. La **criptoanàlisi** s'encarrega d'interceptar aquests missatges. Ara bé, si no ets cap traficant de drogues ni cap mafiós els **serveis d'intel·ligència** dels diferents països no tindran cap interés en allò que vols comunicar, i aquests són gairebé els únics que tenen els medis necessaris per trencar els mètodes més segurs (o algun *hacker* per la xarxa...).

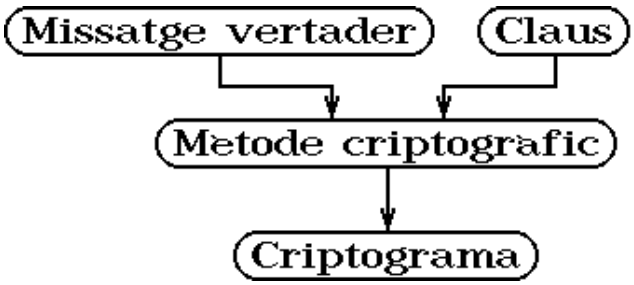
La criptografia és una ciència molt útil actualment en el món de les comunicacions ja que permet una gran seguretat i confidencialitat. L'efectivitat dels mètodes emprats creix espectacularment i els governs d'algunes nacions ja estan prenent mesures legislatives per tal de controlar les comunicacions.

3. BASE D'UN MÈTODE CRIPTOGRÀFIC

Els mètodes criptogràfics són els mètodes que es fan servir per encriptar (transformar i modificar) dades. Val a dir que no tots els mètodes són igual de fiables.

Els elements característics dels mètodes criptogràfics són els següents:

- un missatge que es vol xifrar
- unes **claus** que permetin xifrar i desxifrar el missatge, sovint aquestes claus són numèriques i involucren operacions matemàtiques més o menys complexes.



Esquema de la base d'un criptograma

El principal problema dels mètodes més potents és que es basen a fer operacions que requereixen molt temps de càlcul per a l'ésser humà, com ara la **factorització** de nombres, però amb la introducció dels ordinadors aquesta tasca és molt més ràpida. Aquest fet fa que cada vegada les claus numèriques hagin de ser més llargues per ser més segures. Però la llargària de la clau no serveix si no es millora el mètode.

Els mètodes criptogràfics es poden classificar segons la manera de xifrar. La criptografia es divideix en dues branques conegudes com **transposició** i **substitució**. En la transposició, les lletres del missatge es col·loquen en un altre ordre, generant així un **anagrama**. Per a missatges molt curts aquest mètode és insegur perquè les diferents posicions serien escasses per garantir la seguretat. Per tal que la transposició sigui efectiva, la combinació de lletres ha de seguir un **sistema** senzill que hagi estat acordat per l'emissor i pel receptor. Un exemple és la "transposició de riel" que era molt utilitzada pels estudiants anglesos:

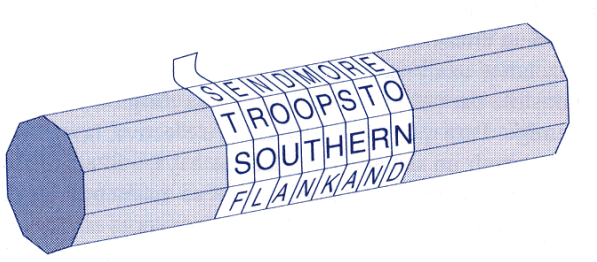
Text en clar: *Quedem a la cabana del llac a mitjanit*

Q E E A A A A A E L A A I J N T

U D M L C B N D L L C M T A I

Text xifrat: QEEAAAAAELAAIJNTUDMLCBNDLLCMTAI

Una altra forma de transposició és la produïda per l'*escital* espartà, al segle V a.C. Aquest va ser el primer aparell criptogràfic. L'escital és una vara de fusta que té una tira de cuir. Quan la tira es desenrosca de l'escital de l'emissor sembla que hi hagi lletres a l'atzar però quan el receptor torna a enroscar la tira al voltant d'un escital igual al de l'emissor les lletres donen a conèixer el missatge. La imatge següent conté un text ocult: "Send more troops to southern flank and..." que traduït vol dir "Envieu més tropes del costat sud i…"



Escital espartà

L'alternativa a la transposició és la substitució. En la trasposició cada lletra manté la seva identitat però canvia la seva posició, mentre que en la substitució cada lletra canvia la seva identitat però manté la seva posició. En sentit estricte, la substitució es divideix en codis i **xifres**. Els codis consiteixen a reemplaçar una paraula per una altra com "hola" per "Júpiter" i en canvi, les xifres substitueixen una lletra per una altra.

4. LA XIFRA DE CÈSAR

El primer ús documentat de la xifra de substitució monoalfabètica, és a dir, utilitzant només un alfabet, va ser la *Xifra del Cèsar*. L'emperador substituïa cada lletra del missatge amb la lletra que es troba tres llocs davant de l'alfabet per protegir les seves comunicacions.

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

Taula de canvi d'alfabets de Juli Cèsar

Per exemple, si apliquem el mètode de Cèsar al famós lament d'Obèlix "Estan bojos, aquests romans", obtindrem "HVWDQERMRVDTXHVWURPDQV". Fixem-nos que s'eliminen els espais en blanc.

Les posicions de l'alfabet poden variar. Tenim només 26 possibilitats diferents utilitzant la taula de canvi d'alfabets de Cèsar perquè l'alfabet que utilitzem (a diferència de l'utilitzat a l'apartat següent) no té la *ç*. Per treballar millor amb aquesta xifra he elaborat una roda d'alfabets que es troba a la tapa del darrera del treball i que té un funcionament elemental: la roda interior presenta l'abecedari sense xifrar i a mesura que la movem les posicions desitjades, la roda amb radi més gran mostra les lletres xifrades segons el mètode Cèsar.

Com hem fet, la xifra de Cèsar pot ser interpretada com una taula de canvi d'alfabets però també es pot veure com una expressió en llenguatge matemàtic. Si assignem nombres enters a cadascuna de les 26 lletres de l'alfabet tenim:

alfab. clar	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
alfab. xifrat	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

Valor numèric de les lletres de l'alfabet A-Z

Ara, el mètode Cèsar és una fórmula matemàtica que transforma el valor numèric d'una lletra sumant-li 3. És a dir, $f(x) = x + 3$ (on x representa una variable que pot prendre qualssevol dels valors numèrics entre 0 i 25). Per exemple, si x=6 tenim la lletra *g*. Si apliquem la fórmula $f(6) = 6 + 3 = 9$, totes les lletres *g* equivalen a les lletres $f(x) = f(6) = f(g) = J$. Aquesta formulació té un problema quan per exemple x=24. Si s'aplica textualment la fórmula anterior $f(24) = 24 + 3 = 27$. Però 27 no correspon a cap número del nostre alfabet ja que tots estan compresos entre 0 i 25. La fórmula s'ha de corregir utilitzant l'aritmètica modular (mireu l'explicació matemàtica a l'annex). Així la fórmula totalment correcta seria $f(x) = x + 3 (\mathrm{mod}\, 26)$. Totes les *y* es convertiran en B.

5. ANÀLISI DE FREQÜÈNCIA

L'anàlisi de freqüència s'atribueix als àrabs. Aquests van ser els primers criptoanalistes. Els criptoanalistes, en lloc de proposar nous mètodes de codificació, més potents i segurs, es dediquen a estudiar com es poden trencar els que ja existeixen. L'anàlisi de freqüència consisteix a desxifrar la substitució monoalfabètica sense conèixer la clau.

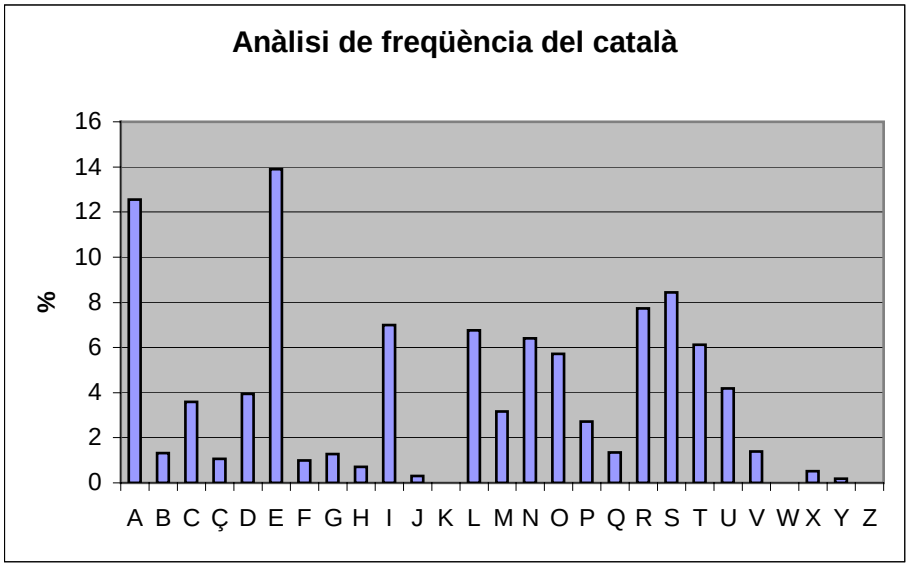
Per explicar en què consisteix i quan es pot aplicar aquest mètode utilitzaré un exemple personal. A l'estiu, quan estava preparant el treball de recerca, vaig demanar ajuda a una amiga (la Bidea, citada als agraïments) per fer pràctica de desxifrar codis. Vaig explicar-li ràpidament en què consistia la criptografia i vaig demanar-li que em preparés un text xifrat sense espais entre paraules. Al dia següent me'l va portar. Jo sabia que ella no havia llegit res sobre criptografia i per tant segur que no havia pensat a utilitzar ni una clau ni cap mètode amb una base sòlida. Així tenia dos possibilitats: o havia fet servir la transposició i havia mogut les lletres del text o havia fet una substitució canviant cada lletra de l'alfabet per una altra. El text xifrat és el següent:

LYPUFHADLLUADLLOHLFUTEFEBLYTEIFGFOWLHFEHWJFHDOFXLT
OFTFSHLOBHLDOWXTPTYTOWLOEHFHLOLUKWOBLUYZHFOYGTDH
LFUKWOBLBLJWTFOFHYLYJEDFOEFULYSLHFBDOFWSWHEDOTEFES
LHLMLHPTHFHFIFFKJEWELYULYSWYYTJTUTEFEYBDOFBDUEUFYL
GFTHHLBDPETJULGWPFPTWBLKFUGFEADLYRFGTFBLSWYYFHLOKF
HMFFUFSHTKLHFWPFYTWADLLYSHLYLOELYBLKWKLOESLHPWKL
OÇFHYRFGTFRFZDEBLPWOXWHKFHFKJUWXLHEFBLUYLDWOPULB
LEHLJFUUFHFUEFUULHBLUYLKJFUFEZLYTGFSFYYFHULYETDLOEH
LPFHEWOYXDYELYTSFSLHYFSHLOLOTPWKLYXFJHTPFGLOLUYLOG
FYWYBLMTUSHWBDPELY

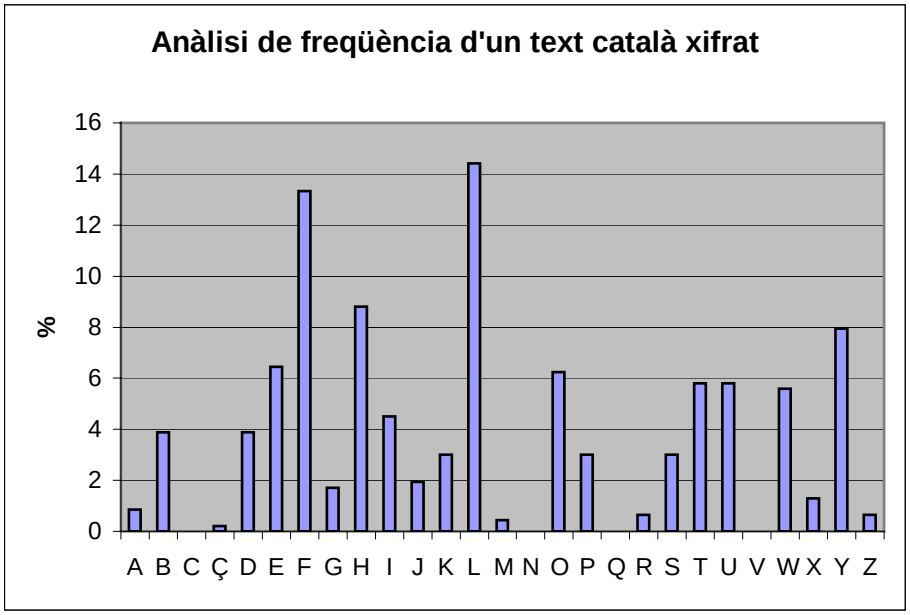
De les dues possibilitats que em vaig plantejar, vaig descartar automàticament la transposició ja que el text xifrat conté moltes *W, F, H...* lletres que en català no són massa freqüents, per tant no havia canviat la posició de les lletres. Directament vaig pensar que un anàlisi de freqüència seria el millor en aquest cas. L'anàlisi de freqüència és un mètode molt potent basat en un anàlisi estadístic. El podrem aplicar sempre i quan sapiguem la llengua en què s'ha escrit. L'anàlisi estadístic consisteix a trobar un **text en clar** diferent, escrit en la mateixa llengua, i que sigui suficientment llarg per omplir un full. Després s'ha de fer una feina molt cansada: comptar quants cops apareix una mateixa lletra fins a completar totes les lletres de l'abecedari i fer uns percentatges dels resultats obtinguts. S'ha de repetir el mateix procés en el text xifrat i posteriorment cal fer una comparació dels resultats obtinguts en els dos casos i tractar d'emparellar les lletres del text en clar amb les del text xifrat.

Al llibre *L'art de la comunicació secreta* d'en David Juher hi ha una taula elaborada per *l'Institut d'Estudis Catalans* a partir d'un recompte de més de 100.000 lletres extretes de textos periodístics i literaris en català, la distribució estadística de les lletres de l'alfabet és, en ordre decreixent: E (13'89%), A (12'55%), S (8'43%), R (7'74%), I (6'99%), L (6'76%), N (6'40%),T (6'11%), O (5'71%), U (4'18%), D (3'94%), C (3'60%), M (3'16%), P (2,72%), V (1'40%), Q (1'35%), B (1'32%), G (1'28%), Ç (1'06%), F (1%), H (0'72%), X (0,52%), J (0,30%), Y (1'18%), Z (0'006%), K (0'004%), W (0'001%).

L'alfabet català que utilitzo ara és de 27 lletres perquè s'inclou la "ç". El gràfic de barres amb aquests percentatges ens ajudarà a tenir una imatge visual del recompte:



Un cop analitzat el text en clar, procedim amb el text xifrat. Les dades de l'anàlisi estan a l'annex ja que m'interessa expossar els resultats directament. Així, el gràfic amb la freqüència de les lletres del text xifrat és el següent:



Per poder fer el primer parell de lletres fem coincidir per exemple la *e* (del text en clar) amb la *L* (del text xifrat) que són les lletres amb més freqüència. La següent lletra amb més freqüència en català és la A que sembla coincidir amb la F del text xifrat. Fent aquestes comparacions podem arribar a saber totes les lletres de l'alfabet xifrat. Aquest mètode no ofereix exactitut sinó aproximació.

La relació de substitució de lletres que es va establir per xifrar el text va ser la següent:

Lletra de l'alfabet	Correspondència text xifrat	Lletra de l'alfabet	Correspondència text xifrat	Lletra de l'alfabet	Correspondència text xifrat
a	F	**i**	T	**r**	H
b	J	**j**	I	**s**	Y
c	P	**k**	C	**t**	E
ç	Ç	**l**	U	**u**	D
d	B	**m**	K	**v**	G
e	L	**n**	O	**w**	Q
f	X	**o**	W	**x**	M
g	Z	**p**	S	**y**	V
h	R	**q**	A	**z**	N

Val a dir que moltes lletres es poden desxifrar per intuició com per exemple els dígrafs "*qu,gu,rr,ss,ny,sc,ll"* que apareixen al català. Per exemple a la primera línia del text xifrat tenim la següent cadena de lletres: LYPUFHADLLUADL. Suposem que és una paraula catalana amb tres lletres que es repeteix molt sovint ("els, que, són, qui..."). Els gràfics mostren clarament que la lletra *L* del text xifrat correspon a la *e* de l'alfabet en clar. Per tant, ja es poden descartar moltes paraules de tres lletres. Sembla que la paraula buscada sigui "que". Per desxifrar la lletra *A* mirem la frequència en què apareix en el text xifrat (a l'annex) i el resultat és d'un 0'86%, la divuitena lletra amb més freqüència. Segons *l'Institut d'Estudis Catalans*, la lletra *q* és la setzena més freqüent en el nostre llenguatge. Les dues dades són molt properes i tenen sentit dins del que estem buscant. Si la *A* equival a la *q*, l'única possibilitat és que la *D* substitueixi la *u*.

Tenint en compte els gràfics de freqüències i les deduccions, el text en clar (que després vaig saber que és del llibre *Silvestre Malasang*, d'Antoni Dalmases) és el següent:

> És clar que el que en realitat desitjava no era trobar una feina i aprendre un ofici, sinó entrar en el món dels grans, viure al món de debò i anar-se situant, a l'espera d'una oportunitat per exercir, ara ja amb totes les possibilitats d'un adult, la seva irreductible vocació de malvat, que s'havia de possar en marxa a la primera ocasió que es presentés. De moment, per començar, s'havia hagut de conformar amb l'oferta del seu oncle, de treballar al taller dels embalatges. I va passar l'estiu entre cartrons, fustes i papers, aprenent com es fabricaven els envasos de mil productes.

6. LA XIFRA DE VIGENÈRE

El següent text s'ha xifrat mitjançant la xifra Vigenère. Abans de començar el treball, el vaig trobar a la *web* personal del David Juher http://ima.udg.es/~juher/pro2006.html i vaig decidir que seria el primer text que desxifraria. No obstant, em vaig adonar que era un missatge molt difícil ja que no sabia quin mètode s'havia fet servir, no hi ha espais entre paraules i era força llarg. Vaig començar provant el mètode Cèsar i no va funcionar, per sort només tenia 27 possibilitats per provar. Després vaig fer un anàlisi de freqüència del text que no va ser inútil però vaig descartar la possibilitat d'una xifra monoalfabètica perquè el recompte de lletres era uniforme. El següent pas era la xifra Vigenère.

KMEHRJVFOGIRBCDMZEAWGWVGRVBFLIZXVBQWNURVHNDMJXRFVGDIZ
CYAVEHRPBAZMIFDRKAMEPOEAKUEISAWTEQHFFVMXQBBRKBUVYOCD
MZMGIQVMXEFHEWVAGGIEFQDVNRVSDMYAOYDCYFYOAICURBGNIQTR
BRLZMZNDRJTMJVBRKBDEQSYSKMQOFNWTEFNFEGBEQRHNDTUGFHNDT
MZRBRDNQMKZHEQZMPEHWMETECWWKFEIODMIPVVQHDIFEYRNECZXQI
AYZGTQSDMIFVRCOBMOXRGQWAPIYOYLZMFNBQSLQPNDBJBMYAGBJWX
PFCEVQOSZDNKAMXDIRLIZXCCQAIBVBJRFQDHHBRKAMRQOYAMEHRGCS
ZFGBAQWTRVRQQMVMXHBVUIAYAVNTQFIFRRKXXEPOISXQPCOFKIPMFS
YEWZNBFRTCFNNRRFBDEQOYSPUTBHRKQPYAORPXQVVSAUQMSAWEAK
MMIOPGVEMQSESZCYRZNDTQYTSESNXEVFRVMOIEOPJMYEQORJIGRVBQ
AKUVNQVGVMPCFBMAAPVRFWAAFESCGAMMQSPALUUHSAGUQWYWSW
QMTBFRDLUEOZRAYGINZQAUARVBBDQOEYSAWABIYARKWNVVRBFKEIY
TBJZQPYOGAAAVGWNDKAVESQGZGRSZBICQXYIZAVUGBGPATXEAHFSTX
YAMNNIOECOYWABVBTHFLUXNHFVMXTNGFSLUWVRRKIBEESVPQMTRZ
GGUNEAHVFAFEAHCJMOMFSAICQIYXBULAQOFRQOSAHESTXYZGISXQVZ
SGJMXMESPGVQMKSEWTDSFHEWLQPCCELIPSE

La xifra Vigenère utilitza dos o més alfabets per xifrar un missatge i així despistar els criptoanalistes. Cal un text més o menys llarg per utilitzar aquest mètode, aquest text té 828 lletres.

La xifra Vigenère rep el nom del seu inventor, un criptògraf francès de principis del segle XIX. Aquest va estudiar les idees d'Alberti, Trithemius i Porta (tots tres del segle XV els quals van començar a treballar amb xifres polialfabètiques) i va crear una xifra coherent i poderosa. La força de la xifra Vigenère radica en què utilitza 26 alfabets xifrats. La línia 1 representa un alfabet xifrat amb un canvi del Cèsar d'una posició. Per desxifrar el missatge el receptor necesita saber quina línia del quadre de Vigenère ha estat utilitzada per codificar cada lletra.

Llano	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	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
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	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

Quadre de Vigenère

Aquest és un exemple aïllat per entendre com s'utilitza aquesta taula. Sabem que la clau del text és EQUACIÓ i que el text xifrat és WUGPTMSRIKUGLOVQJATQG. Volem saber quin és el missatge en clar.

clau	E	Q	U	A	C	I	O	E	Q	U	A	C	I	O	E	Q	U	A	C	I	O
en clar	s	e	m	p	r	e	e	n	s	q	u	e	d	a	r	a	p	a	r	i	s
xifrat	W	U	G	P	T	M	S	R	I	K	U	G	L	O	V	Q	J	A	T	Q	G

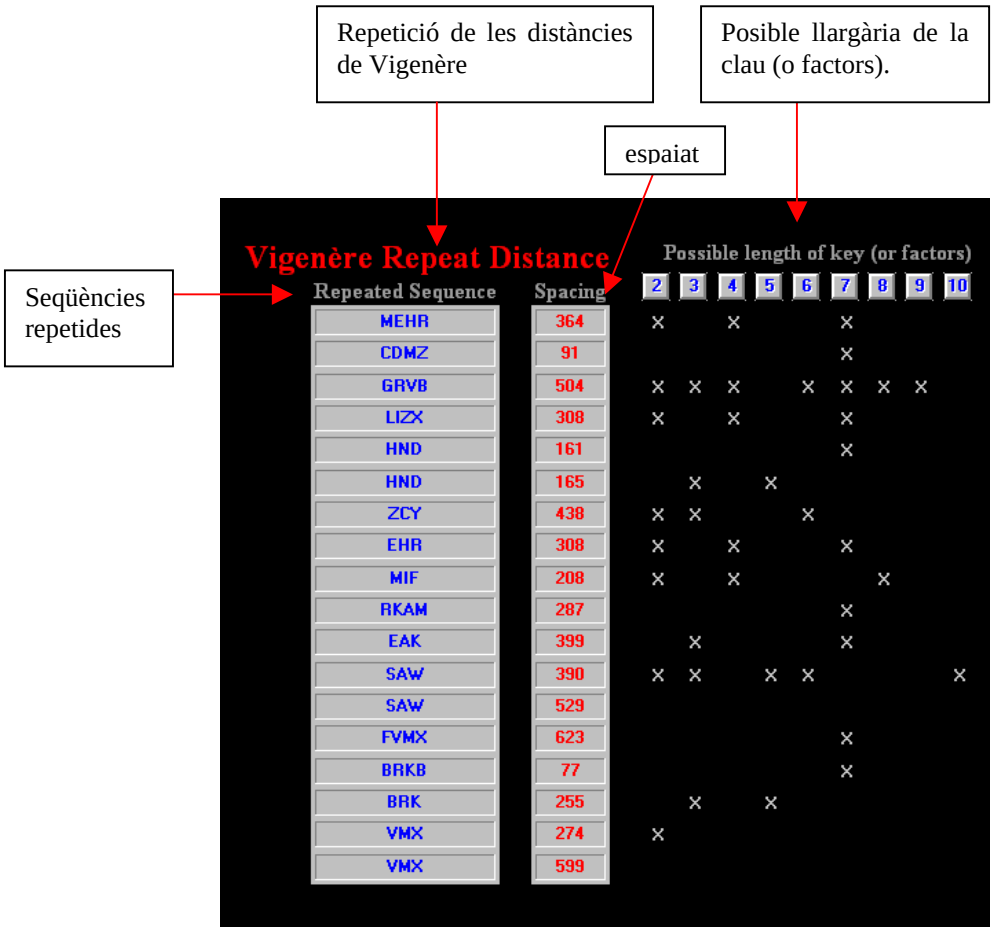
La primera lletra de la clau és *E*, per tant ens situem a la fila 4 on està la *E*. Ens desplacem per aquesta línia fins trobar la *W* que és la lletra xifrada amb la *E* de la clau. Un cop situats en fila 4- lletra *W* pugem per aquesta columna fins arribar a les lletres en minúscula que indiquen el text en clar. D'aquesta manera veiem que *W* es correspon amb la *s* del text en clar. Aquest procediment es repeteix per totes les lletres del text xifrat per trobar el missatge original.

Per saber quina línia s'utilitza per codificar cada lletra s'utilitza una clau que es lletreja sobre el missatge, repetint-la els cops que faci falta fins que cada lletra del missatge quedi associada amb una lletra de la clau.

L'avantatge de la xifra Vigenère és que no es pot sotmetre a l'anàlisi de freqüència, ja que una mateixa lletra del text xifrat pot representar lletres diferents en el text en clar.

Com ja he dit abans, el primer problema que ens trobem en decantar-nos per la xifra Vigenère és que no tenim la clau del missatge. En el meu cas calia saber almenys quantes lletres tenia la clau per aconseguir-la. Per això, s'ha d'examinar el text xifrat i detectar possibles repeticions entre lletres. La rigidesa del llenguatge serà el que ens determinarà la longitud de la clau. Les hores que trigariem en adonar-nos d'aquestes repeticions serien una pèrdua de temps ja que tenim programes informàtics que ens faciliten aquesta feina. Així vaig fer servir el programa de *Los códigos secretos* d'en Simon Singh i em va detectar la longitud de la clau de la següent manera:

En primer lloc, el programa analitza el text instantaniament i ens estalvia una feina molt pesada. Mostro unes imatges del seu funcionament. Val a dir que està en anglès i el fons és negre perquè el programa vol imitar les Cambres Negres de Bletchey Park on molts criptoanalistes, matemàtics i lògics treballaven sense descans per desxifrar la màquina Enigma dels nazis. La columna de l'esquerra mostra les seqüències de lletres repetides i al costat d'elles l'espai de lletres que hi ha fins que es repeteix la mateixa successió. Aquí entren en lloc les matemàtiques ja que els divisors dels espaiats estan indicats amb les creus. Si un divisor és comú en molts espaiats, serà probablement la longitud de la clau. En el nostre cas és normal sospitar que la clau té set lletres (el factor més repetit).



Captura de pantalla dels espaiats de les seqüències repetides del text xifrat de la pàgina 10.

Aclaració: en la columna de “seqüències repetides” hi ha conjunts de lletres repetides tipus HND i SAW. Això vol dir que aquestes lletres xifrades s’han de tornar a repetir amb diferents espaiats. Per exemple entre un HND i un altre hi ha 161 espais i per tant és múltiple de 7. En canvi una altra seqüència HND està separada per 165 espais (múltiples de 3 i de 5).

Aquesta eina també fa un gràfic de barres per cada alfabet corresponent a cada lletra de la clau. Els diferents gràfics es poden comparar amb un gràfic de la freqüència de les lletres en català (mireu el gràfic en l’apartat d’anàlisi de freqüència). Per trobar la solució del text xifrat amb captures de pantalla aneu a l’annex.

Aquest primer exemple l’hem resolt mitjançant un programa informàtic per estalviar temps, no obstant això diré que vaig trigar 4 hores en desxifrar el codi.

7. ESTEGANOGRAFIA I JEROGLÍFICS

Sovint la criptografia es confon amb una altra ciència: l'esteganografia. L'esteganografia consisteix en l'ocultació física (del grec στεγανοζ "cobert" en el sentit d'ocult i γραπτοζ "escrit") d'un missatge o informació. Per una altra banda, tal com es diu a la introducció del treball, la criptografia és la transformació d'un missatge per tal que sigui irreconeixible a qualsevol persona que no conegui el sistema de desxiframent.

No obstant, la criptografia i l'esteganografia sempre han estat molt lligades. Una ciència no exclou l'altra. D'aquesta manera amb la criptografia clàssica al mateix temps que es xifrava un missatge també s'utilitzava l'esteganografia per amargar-lo. Hi ha exemples esteganogràfics molt antics: a l'antiga Xina s'escrivien missatges sobre seda fina, que s'aplastava fins a formar una boleta diminuta que es recobria amb cera. El missatger s'empassava la bola de cera i ja us podeu imaginar com es podia recuperar el missatge per tal de llegir-lo. Un mètode més curiós va ser ideat pel científic Giovanni Porta al segle XV. Aquest va descriure com amagar un missatge dins d'un ou dur: s'escriu el missatge damunt la clova de l'ou dur utilitzant una barreja de vinagre i pols d'alumini. El text preparat amb aquesta barreja travessa la clova i desapareix. Només cal pelar-lo per llegir el missatge perquè aquest queda plasmat en la superfície de l'ou. La forma més coneguda d'esteganografia és l'ús de la tinta invisible que es pot llegir acostant el missatge a la calor. Algunes substàncies que s'utilitzen com a tinta invisible són: la saba d'alguns arbustos, el suc de llimona, la llet, el vinagre i l'orina.

Si no es tenia pressa per fer arribar el missatge s'afeitava el cap d'un home, s'escrivia el missatge i s'esperava que tornés a créixer el cabell per transportar la informació.

Sobre la comunicació secreta durant la Segona Guerra Mundial es podria fer tot un Treball de Recerca de criptografia i esteganografia. Sense oblidar el complex funcionament de la màquina Enigma i tots els esforços dels criptoanalistes per tal de desxifrar-la, a la Segona Guerra Mundial també es va fer ús de l'esteganografia: el text que es volia protegir es reduïa a un micropunt de la mida d'un mil·límetre i funcionava com a punt de la lletra "i", calia saber on localitzar el punt i mirar-lo pel miscroscopi.

Deixant de costat l'esteganografia, també hi ha gent que associa els jeroglífics egipcis amb la criptografia quan estrictament no és així ja que els jeroglífics no s'utilitzaven amb l'objectiu d'amagar i transformar informació sinó que era l'escriptura de l'època. Els jeroglífics es troben des del 3000 a.C fins al s.IV d.C. No obstant, molt criptògrafs van estudiar-los per saber els seus significats. Va ser al 1799 quan uns acadèmics francesos entre els quals estava Champollion (qui va estudiar la pedra) van trobar la pedra Rossetta. Al 1822

Young aprofita el treball de Champollion i desxifra la pedra la qual conté tres escriptures diferents: la grega, demòtica i jeroglífica. Després de molts prejudicis i de molts anàlisis comparant l'escriptura jeroglífica amb les llegües grega i egípcia es va arribar al descobriment que els jeroglífics a part de representar semagrames, és a dir, idees senceres, representen sobretot sons fonètics. Aquest descobriment va sorprendre a tothom ja que l'ús de sons en l'escriptura era molt avançat per aquella època.

8. RECERCA D'EXEMPLES CURIOSOS DE LA CRIPTOGRAFIA I L'ESTEGANOGRAFIA EN EL NOSTRE ENTORN

En aquest apartat he triat diversos exemples curiosos en l'ús de l'esteganografia i la criptografia en la música i literatura. Diferents anècdotes consisteixen en jocs de paraules i números per ocultar informació i gairebé sempre passen desapercebuts als ulls del receptor. Les persones que analitzen els diferents textos moltes vegades treuen conclusions massa precipitades que després són rebutjades però altres semblen tenir lògica quan són explicades.

A mitjan segle XIX Giuseppe Verdi era un compositor famós. Les seves estrenes d'òpera eren tot un esdeveniment social. Les melodies corals de Verdi van esdevenir himnes de llibertat pels nacionalistes del Risorgimento (moviment italià de mitjan segle XIX que pretenia la unificació política dels seus estats per millorar l'economia) . A l'endemà d'una estrena, els carrers que envoltaven el teatre apareixien amb pintades que clamaven "Viva Verdi!". En realitat, aquestes manifestacions ocultaven un missatge: "Viva V.E.R.D.I", és a dir, "Viva Vittorio Emmanuelle, Re d'Italia". Eren, doncs, aclamacions de suport al príncep de Savoia. En aquest cas es fa ús dels **acrònims**, és a dir, sigles que formen un substantiu. El contrari d'un acrònim és un **acròstic**: el missatge que realment es vol transmetre s'aconsegueix juntant les inicials de certes paraules extretes d'un missatge. El 1970 es va publicar un dels darrers discos dels Beatles, el *Sargent Pepper's Lonely Hearts Club Band*, que conté la cançó *Lucy in the sky with diamonds*. De seguida, algunes persones van interpretar que el títol de la cançó ocultava la paraula LSD, el psicofàrmac al·lucinogen de moda als anys 60: ***L**ucy in the **S**ky with **D**iamonds*. John Lennon va explicar que tot era causalitat però hi ha fragments de la cançó que no l'ajuden en la seva argumentació: "Cellophane flowers of yellow and green towering over your head [...] Everyone smiles as you drift past the flowers that grow so incredibly high...". La traducció en català seria " flors grogues i verdes de celofan s'alcen sobre el meu cap [...] Tothom somriu quan tu sures per sobre les flors que creixen tan increiblement alt..."

A vegades el mecanisme per amagar el missatge és més complex. Per exemple, el poema *An enigma*, d'Edgar Allan Poe, conté el nom de la seva estimada, Sarah Anna Lewis, si es pren la primera lletra del primer vers, la segona del segon i així successivament:

Seldom we find, says Solomon Don Dunce
H**a**lf an idea in the profoundest sonnet.
Th**r**ough all the flimsy things we see at once
As e**a**sily as through a Naples bonnet
- Tras**h** of all trash!- [...]".

També hi ha autors que han demostrat que es pot anar en contra l'anàlisi de freqüència. Així, l'escriptor Georges Perec va publicar la novel·la policíaca *La disparition* (*La desaparició*) que va sorprendre molt als criptoanalistes. És una història de més de 300 pàgines en les quals no s'utilitza cap lletra "e", la lletra més freqüent del francès. Així el títol de l'obra no es refereix, com sembla, a la desaparició d'un cadàver, sinó a la desaparició de la lletra "e". Poc després, Perec va decidir publicar una altra novel·la univocàlica de 200 pàgines en honor a la lletra "e", el títol de la qual és *Les revenentes* i comença "Telles des chèvres en détresse, sept Mercédès-Benz vertes, les fenêtres crêpées de reps grège, descendent lentement West End Street et prennet sénestrement Temple Street vers les vertes venelles..." i acaba amb un "The end". Aquest fragment traduït vol dir "Com cabres en perill, set Mercedes-Benz verds, amb les finestres arrissades de reps cru, baixen lentament per West End Street i agafen a l'esquerra Temple Street cap als carrerons verds...".

Hi ha persones que s'han dedicat a estudiar les obres de Jules Verne i diferents treballs, com l'elaborat per Gilles Carpentier, mostren l'obsessió xifradora de Verne. Per exemple, en la novel·la *L'illa misteriosa*, Carpentier assegura que la descripció psicològica que Verne realiza del protagonista Gedeon Spilett correspon a la seva. De fet, si s'aplica el mètode de Cèsar a les inicials G.S., s'obté el sospitós J.V.

Existeixen molts jocs lingüístics en les novel·les de Verne, com ara el nom de l'ajudant del Doctor Ox, protagonista d'un relat **homònim**, que es diu Ygene, de forma que unint tots dos noms s'obté Oxygène, paraula molt relacionada amb l'argument de l'obra. Un altre exemple de l'ús de l'ocultació de Jules Verne és el nom de Michel Ardan, personatge de *De la Terra a la lluna*. Ardan llegit al revés és Nadar, pseudònim de Fèlix Tournachon, fotògraf molt famós de l'època i íntim amic de Verne.

Quant a anècdotes històriques, a finals del maig de 1944 a la ciutat de París ocupada per les tropes alemanyes, els murs d'alguns carrers van aparèixer coberts per uns cartells que

anunciaven l'actuació musical de Nico Taupin, a l'edifici del Casino. Tal com s'estilava en aquella època, l'anunci no informava sobre la data del concert, de fet mai es va arribar a celebrar. Nico era membre de la resistència francesa des de 1942 i pocs dies després de l'aparició dels cartells el van segrestar. El fet és que els pòsters musicals de París tenien escrits els noms dels músics que suposadament acompanyaven a Taupin "Utah", "Omaha", "Sword", "Juno" i "Gold". Aquests noms coincideixen amb els noms claus amb què els aliats es referien a les cinc platges on es produiria el desembarcament de Normandia per part dels soldats nord-americans. A l'annex hi ha una imatge del pòster.

9. CLAU PRIVADA I CLAU PÚBLICA

Els mètodes criptogràfics es classifiquen en dues grans famílies: els **sistemes de clau privada** i els de **clau pública**. Els de clau privada són aquells en els quals emissor i receptor han d'acordar una clau que han de mantenir en secret. Tots els mètodes explicats fins ara són de clau privada i, de fet, tota la comunicació secreta fins el 1970 pertany a aquest grup. L'altre grup, els de clau pública, han aconseguit desafiar tota lògica. En un sistema de clau pública, l'emissor i el receptor en cap moment comparteixen una clau, sinó que utilitzen claus diferents. En la història de la criptografia sempre s'ha plantejat el problema del repartiment de claus de manera segura i ràpida. A més s'havia d'afegir el problema de mantenir la clau en secret per tal que l'enemic no la robés i interceptés el missatge. Així al 1970 es va fer el salt més important de la criptografia, des de llavors els mètodes han canviat radicalment. Com és d'imaginar la criptografia actual es basa en els mètodes de clau pública i ja s'ha deixat de banda el llapis i paper per enviar missatges. Actualment Internet és el medi més utilitzat per les comunicacions i la criptografia del 2007 gira al voltant dels ordinadors, amb matemàtiques i **algorismes** molt complexos. No obstant, avui dia les claus han de continuar amb una llarga longitud per evitar l'atac per **força bruta**, és a dir, l'intent de provar totes les claus possibles fins a arribar a la correcta. Val a dir que no és un bon mètode ja que, amb els ordinadors més potents, pot comportar dies, mesos, anys o fins i tot que mai s'arribi a aconseguir, com és el cas d'una bona aplicació de la clau pública.

10. INTERCANVI SEGUR DE CLAUS

A la dècada de 1960 els pocs ordinadors que existien estaven en mans dels centres d'investigació, universitats, grans empreses, bancs i organitzacions governamentals. Aquests llocs exigien protecció en les seves comunicacions i tothom tenia clar que un dels axiomes de la criptografia és el fet que "qualsevol comunicació es pot intervenir". També s'acceptava que el moment crític de la seguretat del sistema és el moment en què l'emissor i el receptor realitzen l'intercanvi de claus. El 1976, al Congrés Nacional d'Informàtica dels Estats Units, dos matemàtics nord-americans, Diffie i Hellman, van presentar una idea: la **clau asimètrica** per la criptografia de clau pública. La clau asimètrica resol definitivament el problema de l'intercanvi de clau. A partir de llavors s'han creat diferents mètodes, com l'RSA, per xifrar utilitzant el seu descobriment.

La idea es fonamenta en l'ús de les **funcions d'una sola direcció**, és a dir, una operació matemàtica fàcil de calcular però difícil o impossible d'invertir. La clau és numèrica i s'obté del producte de dos **nombres primers**. La operació inversa del producte és la factorització, una operació que avui dia pot ser impossible de calcular, fins i tot amb els millors ordinadors, si es treballa amb xifres molt grans.

Un exemple molt didàctic, no matemàtic d'això que comento, pot ser imaginar dos pots de pintura que mesclem per obtenir un nou color. Aquesta operació és molt senzilla però fer el pas invers per tornar als colors originals és molt complicat.

11. SISTEMA RSA

Al 1997 Rivest, Shamir i Adleman van inventar el primer sistema de clau pública de la història, anomenat RSA (sigles dels seus noms). Només explicaré el funcionament genèric del sistema RSA, sense entrar en cap detall matemàtic ja que és un sistema molt complex dificilment a l'abast de qualsevol persona que no hagi estudiat carreres del tipus matemàtiques, telecomunicacions o informática. Així la meva intenció és plasmar la gran diferència entre la criptografia clàssica i l'actual.

La idea, com en el cas del protocol d'intercanvi de claus de Diffie-Hellman, torna a basar-se en l'ús de les funcions unidireccionals.

Per explicar la lògica de RSA farem servir els noms de dos personatges imaginaris que apareixen a tots els llibres de criptografia: Alícia i Benet. Alícia i Benet es volen comunicar però viuen en continents diferents. Alícia vol enviar un missatge molt important a Benet i l'introdueix en una caixa de ferro, la tanca i fica un candau. Envia la caixa tancada amb

candau i es queda amb la clau. Quan Benet rep la caixa no pot obrir-la perquè no té la clau. L'única solució sembla ser que Alícia i Benet es vegin per tal que Alícia li doni la clau de la caixa. Però amb RSA el que s'aconsegueix és que Benet, quan rebi la caixa d'Alícia, fiqui un altre candau al candau existent i es quedi amb la clau. Llavors, quan Benet enviï la caixa a Alícia, Alícia treurà el seu candau, tornarà a enviar la caixa amb el candau de Benet i aquest podrà obrir la caixa de ferro amb la seva clau i llegir el missatge. En termes criptogràfics, Alícia usa la seva propia clau per xifrar un missatge per Benet, el qual torna a xifrar-lo amb la seva propia clau i el retorna. Quan Alicia rep el missatge doblement xifrat, treu la seva pròpia codificació i li retorna a Benet que retirant la seva pròpia codificació podrà llegir el missatge.

En RSA, cada usuari tria dos nombres primers, *p i q*, molt grans. Aquest parell de nombres són la clau privada. Llavors es multipliquen *p* i *q* i s'obté *n* que és la clau pública de l'usuari. Un exemple real és:

p= 765453635474657464653452310983091829280384764655753838457
q= 918720925464512543092547364589875410928332746653839390286 1
n = *p* · *q*=703238272383452934818343379228800246389199968271559463196
818775039978537832794042319269833769756943816894594412547 7
Clau pública: *n*
Clau privada: *p, q*

Avui en dia no existeix cap ordinador que sigui capaç de calcular *p* i *q*, els dos **factors** que s'han utilitzat per obtenir *n*, amb menys de 4500 milions d'anys de càlculs. Dit d'una altra manera, ningú podrà deduir la clau privada a partir de la pública. Per fer servir RSA, la persona que vulgui enviar un missatge a algun usuari haurà de xifrar el codi amb la clau pública del receptor que es troba en el directori i el receptor utilitzarà la seva clau privada per desxifrar el missatge. Hem arribat a un punt en què la comunicació és segura perquè la clau privada no s'ha de compartir amb ningú. RSA està a l'abast de tothom amb la seva versió lliure PGP (Pretty Good Privacy) que es pot descarregar d'Internet gratuïtament a http://www.pgpi.com/, però només després de contestar un qüestionari detallat a partir del qual s'estableixen unes restriccions de descàrrega. Per exemple, no és possible tenir una còpia del PGP si la sol·licitud prové d'un ordinador de França, USA o els països islàmics ja que les lleis d'aquests països no ho permeten. El seu ús està dissenyat d'una manera molt sezilla per tal que tothom pugui utilitzar el sistema sense coneixements previs de criptografia. Qui va obtenir la patent de PGP va ser Phil Zimmermann i va tenir molts problemes amb les forces de seguretat dels Estats Units.

12. MARC LEGAL DE LA CRIPTOGRAFIA I L'ESTEGANOGRAFIA EN LA SOCIETAT ACTUAL

El gran debat actual de la comunitat relacionada amb seguretat i criptografia és si la criptografia i els mètodes tan segurs com RSA han d'estar a l'abast de tothom o bé han d'estar controlats pels serveis d'intel·ligència dels diferents països. Hi ha dues postures clares: els qui defensen la privacitat de la comunicació i estan a favor de la criptografia per tothom i els qui creuen que és més important la seguretat nacional i per tant aquests programes han d'estar sota control. S'ha de tenir en compte que la criptografia i l'esteganografia poden ser utilitzades per a fins il·legals. Un exemple és l'ús que grups de traficants de droga, o terroristes podrien fer per comunicar-se a través d'Internet amb seguretat. Però també és cert que l'Article 12 de la Declaració Universal dels Drets Humans reconeix el dret a la privacitat.

Com a possible solució d'aquesta problemàtica i partint de la criptografia de clau pública, alguns criptògrafs estan investigant els pros i els contres d'un pla conegut com a *dipòsit de claus* (*key escrow*). En termes criptogràfics, *dipòsit* significa que Alícia donaria una còpia de la seva clau privada a un agent de dipòsits (*escrow agent*), un intermediari independent i de fiar, que estigués autoritzat a entregar la clau privada a la polícia si en algun moment Alícia pogués estar involucrada en un delicte. Amb aquest pla es vol conservar el dret a la privacitat a més d'assegurar la seguretat nacional.

Alguns governs ja han començat a crear lleis per regular aquestes ciències, com és el cas dels Estats Units on RSA està prohibit i molts altres mètodes estan restringits a una longitud de clau determinada. A Espanya, no obstant, avui en dia, no hi ha cap llei que reguli la criptografia tret de la **signatura digital**. La llei 59/2003, del 19 de dessembre de 2003 és la que regula la signatura digital. Alguns punts d'aquesta llei són els següents:

- El reconeixement de la signatura amb l'objectiu de fomentar les noves tecnologies de seguretat de les comunicacions en àmbits d'empreses, ciutadans i Administracions públiques.
- Les dades de creació i verificació de la signatura són úniques, com codis o claus criptogràfiques privades, que el signant utilitza per crear la signatura electrònica.
- El Ministeri de Ciència i Tecnologia és l'encarregat de fer les inspeccions per garantir el bon funcionament de la signatura digital.
- Les sancions pel mal compliment de les lleis dictades al BOE núm.304 sobre signatura digital tindran un pes d'entre 6.000 i 600.000 euros de multa.

13. CONCLUSIONS

Les conclusions sobre criptografia que he extret al llarg del desenvolupament del treball de recerca són diverses: si ens fixem en els primers mètodes criptogràfics com la xifra de Cèsar veurem que són mètodes molt senzills, gairebé sense seguretat. Aquests mètodes que ara semblen jocs van tenir una gran importància a la seva època i no és d'extranyar que triguessin a ser descoberts ja que tampoc hi havia els medis ni les eines necessàries per desxifrar. Aquests primers usos documentats de la història de la criptografia donen a conèixer la necessitat de la privacitat des de temps antics. Al llarg dels segles, tal i com es reflexa al treball, l'ocultació de missatges ha estat imprescindible per tal d'evitar en molts casos la pròpia mort en temps de guerra o de repressió. Per una altra banda, el treball dels criptoanalistes és igual d'important ja que en molts casos la criptografia s'utilitza amb fins il·legals. Per tant, personalment penso que no hi ha ni bons ni dolents, és a dir, criptògrafs i criptoanalistes treballen junts per millorar la privacitat i en molts casos aquesta ha de ser violada per evitar grans incidents.

Com tot, la criptografia s'ha adaptat als temps actuals i ara s'estila la criptografia destinada als ordinadors, especialment a Internet. La clau pública és el millor descubriment fins ara ja que un bon ús proporciona una seguretat màxima, per tant un codi indesxifrable perquè els ordinadors actualment no són prou potents per realitzar una factorització complexa.

Si tenim en compte que Internet és el medi de comunicació més utilitzat i el més ràpid no és d'extranyar que hi hagi *hackers* i empreses que vulguin robar informació de la competència. Tothom qui vulgui enviar informació sense que sigui interceptada ha d'utilitzar la criptografia. Per una altra banda, si arriba un moment en què totes les comunicacions estan encriptades aquestes resultaran impossibles de controlar ja que la societat actual no està equipada per rebre un increment enorme en el seu ús. Cal veure, per tant, si la criptografia s'expandirà encara més del que ho està ara per poder preparar les infraestructures necessàries per tal de suportar-la.

El treball m'ha fet reflexionar sobre l'esforç que hi ha darrera dels codis, de la importància de les matemàtiques i la lingüística i la valoració de l'existència d'una ciència com la criptografia que faci possible la privacitat dins d'un món de corrupció en les comunicacions.

Quant a conclusions més específiques del treball faig referència a la importància de les definicions precises, l'abilitat de resumir i classificar la informació, la bona organització en capítols i annexos i ser clara i didàctica. També he estat conscient de les meves limitacions en la matèria ja que darrera de cada mètode hi ha molta meditació i matemàtiques sovint incomprensibles per a mi. Tot i això he pogut arribar als meus objectius inicials.

14. GLOSSARI

El glossari no segueix l'ordre alfabètic sinó que els termes estan ordenats segons l'ordre en què apareixen al treball.

1- **Codi**: Sistema de símbols, paraules o noms que substitueixen paraules senceres.
2- **Desxifrar**: posar en clar, arribar a solucionar un enigma o una xifra.
3- **Encriptació**: acció d'encriptar, és a dir, xifrar la informació per impedir que un missatge pugui ser llegit.
4- **Mètode criptogràfic**: conjunt de passos utilitzats per realitzar una xifra.
5- **Criptoanàlisi**: desxifrat de codis, l'art de tornar el text xifrat a la seva forma original sense disposar de la clau de xifrat.
6- **Serveis d'intel·ligència**: organismes que velen per la seguretat dels ciutadans.
7- **Clau**: el component d'un criptosistema que determina com serà mesclat el missatge. Aplicant una clau al missatge original s'obté el text xifrat; la mateixa el durà a la seva forma original. En el cas concret dels sistemes de clau pública, la seva clau secreta associada.
8- **Factorització**: operació matemàtica consistent a agafar un nombre generat per multiplicació de dos o més nombres més petits i trobar aquests nombres originals.
9- **Transposició**: acció i efecte de transposar, és a dir, invertir l'ordre en què està posada una cosa respecte d'altres.
10- **Substitució**: reemplaçar una lletra per una altra.
11- **Anagrama:** mot o frase formats per la transposició de les lletres d'un altre mot o una altra frase.
12- **Sistema**: conjunt d'elements relacionats entre ells.
13- **Xifra**: escriptura secreta.
14- **Text en clar**: el missatge abans de ser xifrat
15- **Acrònim**: sigla, especialment aquella que l'ús ha convertit en un substantiu. N'és un exemple TR per Treball de Recerca.
16- **Acròstic**: enigma consistent a insertar algun missatge secret que es pugui llegir verticalment a partir de les primeres lletres dels versos d'un poema (com l'exemple d'Edgar Allan Poe amb el missatge amagat de *Sarah*), o bé el nom antic per designar l'acrònim.
17- **Homònim**: allò que té el mateix nom.

18- **Sistemes de clau privada**: sistema basat en l'acord d'una clau entre emissor i receptor la qual s'ha de mantenir en secret.
19- **Sistemes de clau pública**: sistema basat en una clau pública (coneguda per tothom) formada a partir de dos nombres secrets que mai es podran conèixer.
20- **Algorisme**: Procediment de càlcul que consisteix a acomplir un seguit ordenat i finit d'instruccions que condueix, un cop epecificades les dades, a la solució que el problema genèric en qüestió té per a les dades considerades.
21- **Força bruta**: és un atac que consisteix a provar totes les claus possibles fins arribar a trobar la correcta. No és un bon mètode d'accés pel temps que pot implicar: dies, mesos, anys o fins i tot que mai s'arribi a aconseguir
22- **Clau asimétrica:** nom per dessignar la necessitat del conjunt de la clau privada i la clau pública per comunicar-se basat en l'existència d'una clau per xifrar i una altra clau diferent per desxifrar.
23- **Funcions d'una sola direcció**: funcions amb operacions fàcils de calcular però difícils o impossibles d'invertir.
24- **Nombres primers**: aquells que només són divisibles per si mateixos i per 1.
25- **Factors**: nombres que resulten del procés de factorització.
26- **Signatura digital**: conjunt de dades electròniques que poden ser utilitzades com a medi d'identificació del signant.

15. BIBLIOGRAFIA

LLIBRES

- Juher, David, *L'art de la comunicació secreta*; Ed. Llibres de l'índex, Barcelona, 2004
- Singh, Simon, *Los códigos secretos*; Ed. Debate, Madrid 2000
- V.V.A.A, *Técnicas criptográficas de protección de datos*; Ed. Ra-Ma, Madrid, 2005
- Enciclopèdia Catalana Bàsica, Barcelona, 1996

INTERNET

http://www.xtec.es/~dobrador/

Pàgina personal d'en David Obrador amb informacions sobre criptografia. En català.

http://www.xtec.es/~agonzal3/

Treball de criptografia i esteganografia de dos alumnes de l'IES Terra Roja. En català.

http://www.simonsingh.net/The_Black_Chamber/home.html

Pàgina en anglès d'en Simon Singh. Es pot descarregar el CD-ROM per desxifrar codis.

http://digital.el-esceptico.org/

Web en castellà amb articles diversos. Article del 2002: *De la clave del César a los algoritmos de encriptación*.

http://personal.telefonica.terra.es/web/jms32

Pàgina amb apunts sobre criptografia. A més està penjat tot el llibre de *Los códigos secretos* d'en Simon Singh. En castellà.

http://www.abcdatos.com/utiles/ascii.html

Taula del codi ASCII en castellà.

http://www.uv.es/metode/numero24/22-24.html

Pàgina en català que tracta els nombres primers i la seva importància en la criptografia.

http://www.kriptopolis.com/

Espai dedicat des de 1996 al debat i la opinió sobre criptografia, privacitat i seguretat. En castellà.

http://www6.gencat.net/stsi/dicctel/scripts/fitxa_terme_complet.asp

Web de la Generalitat de Catalunya on s'inclou un diccionari de telecomunicacions. En català.

http://www.fd.com.ar/manual7.html

Glossari en castellà d'informàtica i criptografia.

http://portal1.lacaixa.es/Channel/

Pàgina de “la Caixa” amb diccionari de seguretat. En castellà.

http://rinconquevedo.iespana.es/rinconquevedo/criptografia/anecdotas.htm

Web en castellà sobre criptografia general i anècdotes criptogràfiques.

http://www.dma.fi.upm.es/java/matematicadiscreta/Aritmeticamodular/criptografia.html

Breu història de la criptografia. Apartat de matemàtiques d’aritmètica modular i nombres primers. En castellà.

http://analisisdealgoritmos.galeon.com/

Web en castellà amb explicacions d’algoritmes i programes encriptadors.

http://es.wikipedia.org/

Encliclopèdia virtual.

http://www.bletchleypark.org.uk/

Web oficial de Bletchley Park on publiquen informacions esporàdiques dels seus desxiframents. En anglés.

http://emannuelle1.blogspot.com/2006/01/el-codigo-enigmahitler-y-los-nazis.html

Informació sobre la màquina Enigma, Hitler i els nazis. En castellà.

http://www.britishmuseum.org/

Pàgina oficial del British Museum. Informació sobre la pedra Rossetta que resideix al museu i els jeroglífics. En anglès.

http://www.dantealighieri.com.mx/historia/risorgimento.htm

Informació en castellà del Risorgimento. La vaig utilitzar per aclarir el context de l’exemple de Verdi.

http://www.partal.com/vademecum/cat/llibres/4.html

Web en català d’exemples de la criptografia en la literatura i la història.

http://ima.udg.es/~juher/pro2006.html

Pàgina on es proposa per desxifrar el missatge de l’apartat de la xifra Vigenère. En català.

http://www.eumed.net/cursecon/ecoinet/seguridad/sustitucion.htm

Pàgina en castellà amb explicacions de la substitució i la transposició.

ALTRES

- Butlletí Oficial de l’Estat, núm 304. Publicat el dissabte 20 de dessembre de 2003. *Lleis de regulació de la signatura digital.*
- CD-ROM per desxifrar d’en Simon Singh.

ÍNDEX

1. PRESENTACIÓ 1
2. INTRODUCCIÓ 3
3. BASE D'UN MÈTODE CRIPTOGRÀFIC 4
4. LA XIFRA DE CÈSAR 6
5. ANÀLISI DE FREQÜÈNCIA 7
6. LA XIFRA DE VIGENÈRE 10
7. ESTEGANOGRAFIA I JEROGLÍFICS 13
8. RECERCA D'EXEMPLES CURIOSOS DE LA CRIPTOGRAFIA I L'ESTEGANOGRAFIA EN EL NOSTRE ENTORN 14
9. CLAU PRIVADA I CLAU PÚBLICA 16
10. INTERCANVI SEGUR DE CLAUS 17
11. SISTEMA RSA 17
12. MARC LEGAL DE LA CRIPTOGRAFIA I L'ESTEGANOGRAFIA EN LA SOCIETAT ACTUAL 19
13. CONCLUSIONS 20
14. GLOSSARI 21
15. BIBLIOGRAFIA 23