CRIPTOQUÈ?

Pseudònim: Pumba

ÍNDEX:

1. INTRODUCCIÓ

El meu treball de recerca tracta sobre la Criptografia. I per què la Criptografia? Doncs perquè forma part de la branca de les matemàtiques, les quals a mi m'apassionen, i, al final, és com si estiguessis jugant amb elles.

Abans de fer aquest treball, quan sentia criptografia, pensava en els missatges de WhatsApp, que un bon dia el mòbil em va dir que anaven encriptats, però no m'havia parat mai a pensar què devia ser això de la criptografia, si era un invent d'ara dels WhatsApp, o si era quelcom que havia existit sempre, o com s'havia inventat... els més grans em deien que no, que no era un invent d'ara, sinó que es va inventar amb les guerres, que els alemanys ja tenien una màquina que encriptava els missatges perquè els seus enemics no sabessin què es deien... De fet, fins abans de plantejar-me el treball, no m'havia parat mai a pensar ben bé què era la criptografia. Per tant, l'objectiu del meu treball ha estat entendre què és la criptografia, com es va originar, d'on va sortir i entendre el perquè es va inventar.

I això és el que he fet en la part teòrica, estudiar els orígens de la criptografia, estudiar què és i perquè va sorgir, i com ha evolucionat fins al dia d'avui. També en la part teòrica he estudiat els diferents mètodes d'encriptació que hi ha hagut al llarg de la història (no tots, ja que n'hi ha molts més dels que em podia arribar a pensar), i he après a encriptar i desxifrar missatges encriptats.

Tot aquest treball teòric m'ha portat a plantejar-me una hipòtesi que és el que després he intentat verificar en la part pràctica. La hipòtesi que m'he plantejat és que ***la criptografia ha anat evolucionant amb mètodes cada cop més complexos a mesura que s'han anat trobant maneres de desencriptar-los, i que al final arriba un moment que si no tens ajudes (siguin màquines, ordinadors, pistes...) ja no pots desencriptar-los*.**

Per a verificar la hipòtesi, en la part pràctica el que he fet ha estat primer aplicar diferents mètodes d'encriptació per a encriptar un mateix text, començant per els més antics, i així veure en la realitat l'evolució i les diferències entre ells, veure la dificultat de cada mètode, i verificar que cada cop és més difícil i complicat... I després he agafat tres textos encriptats

amb diferents mètodes, i he intentat desxifrar-los manualment, per verificar la hipòtesi que arriba un moment que sense ajudes no te'n surts.

1.1 Motivació

El que m'ha mogut a fer aquest treball és la meva passió pels números i les matemàtiques. La criptografia és un camp desconegut per mi. Pel que el fet d'ampliar els meus coneixements és un repte.

1.2 Estructura del treball

El treball s'estructura en 3 parts diferenciades: Part teòrica, part pràctica i conclusions.

- En la part teòrica s'hi recull tota la informació necessària per comprendre la criptografia, les seves utilitats i el seu funcionament. Es relacionen els mètodes més importants utilitzats al llarg de la història, amb una explicació del seu funcionament. Finalment s'exposa la importància de la criptografia actual i es fa una incursió en el futur de la criptografia.

- La segona part és la que forma el marc pràctic, en el que s'utilitza la part teòrica apresa prèviament. Amb la finalitat de consolidar l'aprenentatge i veure quins mètodes eren o són més eficients i útils, quins són més fàcilment desxifrables o quins són quasi impossibles. La part pràctica es divideix en dues parts, la part de codificació, que és duta a terme durant la part teòrica per exemplificar els mètodes; i la segona part, la part de descodificació, on s'apliquen tres mètodes diferents en diversos textos codificats i el que es tracta és d'intentar desxifrar-los.

- Finalment, en la tercera i última part es recullen les conclusions a les quals s'ha arribat en finalitzar el treball.

1.3 Mitjans utilitzats per realitzar el treball

La meva principal eina de treball ha estat el meu ordinador, ja que m'ha permès utilitzar el Microsoft Word per redactar tot el treball i per fer la part pràctica. Per la pràctica, donat que es tractarà d'anar substituint lletres del text xifrat a l'original, s'ha utilitzat les funcions de buscar i reemplaçar, sense aquestes funcions la dificultat encara seria major.

La pàgina web: https://ca.worder.cat/buscarparaules, ha estat una magnífica eina a l'hora de desxifrar, ja que ha permès buscar paraules a partir de patrons. Per exemple: El patró era HA- i el resultat era HAVIA, HAN, HAS...

Il·lustració 1: cercador de paraules- https://ca.worder.cat/buscarparaules

En el procés de descodificació dels textos encriptats en la part pràctica s'ha utilitzat el programa Word, paper i llapis i moltes proves i versions a falta d'un ordinador potent, d'un programa descodificació i de coneixements informàtics que hauria facilitat la tasca de desencriptació.

2. METODOLOGIA

Per a realitzar la part teòrica del treball s'ha obtingut informació a través de:

- Accés a pàgines web d'internet, les dues principals serien aquestes, la resta la trobareu a la bibliografia del final:
    - *https://fme.upc.edu/ca/premi-poincare/arxius/criptografia_julia-alsina* Aquesta pàgina web m'ha fet molt de servei a l'hora de buscar informació sobre els mètodes criptogràfics de la història.
    - *https://www.genbeta.com/desarrollo/tipos-de-criptografia-simetrica-asimetrica-e-hibrida* És la principal pàgina web que he utilitzat per investigar sobre la criptografia asimètrica i simètrica.
- Assistència a conferències:
    - Vaig assistir a una conferència sobre criptografia que impartia el professor d'informàtica i matemàtica aplicada de la Universitat de Girona, David Juher adreçada a professors de batxillerat.
- Lectura de llibres:
    - El llibre que més m'ha ajudat i servit ha sigut "*L'art de la comunicació secreta*" de David Juher.
- Consultes a professors de matemàtiques:
    - David Juher, professor d'Informàtica i matemàtica aplicada de la Universitat de Girona
    - Jordi Herrera, professor agregat del departament d'Enginyeria de la Informació i les Comunicacions Escola d'Enginyeria a la Universitat Autònoma de Barcelona.

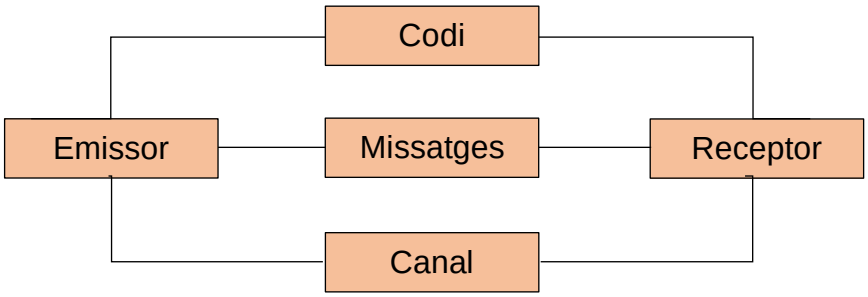
La part pràctica ha consistit en la desencriptació de 3 textos i la metodologia seguida ha estat la meva feina personal amb la utilització de l'ordinador, Word i Excel i paper i llapis.

3. TEORIA DE LA CRIPTOGRAFIA

3.1 Introducció a la comunicació

La comunicació és la transmissió d'informació codificada d'acord amb unes regles arbitràries i compartides per un grup. Qualsevol objecte, acció o fenomen que incorpori alguna informació i que pugui ser percebuda pels sentits pot considerar-se un element comunicatiu.

Els elements de la comunicació són els següents:



- Emissor: És la persona que envia el missatge. Aquesta és l'encarregada d'agafar informació i de fer-li arribar al destinatari.
- Receptor: És la persona que rep el missatge, llavors l'ha d'interpretar.
- Missatge: És la informació, el contingut, el que l'emissor envia al receptor.
- Codi: És la forma en què l'emissor codifica el missatge per tal d'enviar-lo al receptor. Per tal de tenir una comunicació satisfactòria, tant l'emissor com el receptor han de conèixer aquest codi.
- Canal: És l'espai pel qual s'envia el missatge. Com més sorolls, intervencions i distorsions, serà més complicat pel receptor interpretar correctament el missatge.

Val a dir que una regla important de la comunicació és que el responsable de la comunicació és l'emissor. L'emissor és qui s'ha d'assegurar que el receptor rep correctament el missatge, és a dir, que el missatge és clar, que utilitza un canal de comunicació al qual el receptor també té accés, i finalment que el codi que farà servir és conegut pel receptor.

Aquesta regla aplicada a la inversa és en part la responsable de l'aparició de la criptografia, és a dir, si volem passar un missatge per a només un sol receptor l'única manera és que o bé el canal o bé el codi siguin exclusius. Aconseguir un canal exclusiu és bastant difícil, podem intentar utilitzar una freqüència de ràdio exclusiva (com fa la policia, o els avions),

però tots veiem a les pel·lícules com és fàcilment interceptable, o podem intentar enviar missatges com feien en el passat amb coloms missatgers, però també moltes vegades eren interceptats. A final els canals són finits, i acaben essent els canals normals de transmissió (escrit, verbal, radio...). En canvi és més fàcil inventar-se un codi que només l'emissor i el receptor sàpiguen, el codi més senzill són els diferents idiomes, si parlem un idioma que només A i B coneixen llavors un tercer C encara que tingui accés al canal de comunicació no podrà entendre el missatge... podríem dir que l'idioma és la criptografia més bàsica... Com a regla general, per tant, el més fàcil és inventar-se un codi que només l'emissor sap, i que s'assegura que el receptor també sap. Si els dos saben el codi i només el saben ells dos llavors poden tenir una comunicació segura. Aquest codi és el que anomenem criptografia.

3.2 Introducció a la criptografia

La criptografia, del grec *kryptos-**κρυφή*** (amagat) i *graphein-**γράψτε*** (escriure) és l'estudi dels mètodes emprats per enviar missatges de manera encoberta per tal que només el receptor sigui capaç de llegir-los i entendre'ls. La criptografia és un branca de les matemàtiques, per tant, es tracta d'una disciplina purament científica, però que alhora toca arrels humanístiques de caràcter filosòfic, històric, lingüístic, religiós, etc.

L'objectiu principal de la criptografia era mantenir en secret un missatge, el dia d'avui ja no només s'utilitza per a la privacitat.

3.3 Utilitats de la criptografia

La principal utilitat de la criptografia és la privacitat, l'emissor només vol que la persona que ell autoritza pugui entendre el missatge i no altres persones alienes.

En un passat, la criptografia era utilitzada durant les guerres per enviar informació entre països aliats per tal que els enemics no entenguessin el contingut dels missatges. Una de les màquines de xifrat més famosa és la màquina Enigma, utilitzada pels nazis en la segona guerra mundial, però això ja ho veurem més endavant.

Avui en dia, amb tots els avenços tecnològics, la criptografia té moltes més utilitats que no pas tenia al passat, i també els codis poden ser molt més complexos o difícils de desxifrar.

La majoria de nosaltres quan sentim a parlar de criptografia ens imaginem a espies o agències com la NSA (*National Security Agency*), però la veritat és que és present a la nostra vida quotidiana. Tot el que sigui un mètode de pagament que no és a través de bitllets o monedes físiques utilitza criptografia, per exemple PayPal, Visa, Mastercard, ATM (*Automatic Teller Machine*), etc; quan ens connectem a internet, a qualsevol pàgina web que el seu link contingui HTTPS està utilitzant criptografia, ja que https es basa en uns algoritmes de xifrat de clau pública, els quals permeten una connexió segura; per comprar per internet o per entrar al correu electrònic també es fa ús de la criptografia, ja que estem establint una comunicació segura entre el nostre ordinador i els servidors de Google, Amazon, o el que estigui essent utilitzat; totes les converses que tenim a través del nostre telèfon, tota la seqüència de dades transmesa, també es mou de forma xifrada, per tal que cap persona no autoritzada pugui escoltar o interceptar la conversa.

En un futur, les utilitats de la criptografia podran o no haver canviat, les possibilitats de la computació que ens donen els ordinadors fa que es puguin fer codis extraordinàriament segurs, la dependència que tenim de les comunicacions per internet fa que necessitem aquests codis tant segurs, i fins i tot hi ha persones que diuen que la física quàntica haurà d'entrar en acció per poder distribuir claus per xifrar de manera segura en un món on la computació quàntica és relativament accessible; d'altres que creuen que la tecnologia quedarà estancada i que, per tant, la criptografia tindrà les mateixes utilitats d'ara, només que amb més complexitat. Però no hi ha res segur, no podem predir el futur, ens hem d'esperar i deixar que el temps flueixi.

3.4 Història de la criptografia

La criptografia coneguda com a tal, comença amb la criptografia clàssica, que es basa en mètodes de xifrat on s'utilitza paper i llapis. Però si ens remuntem al passat, no podríem dir que els jeroglífics utilitzats pels egipcis, per exemple, no eren ja criptografia? Aquí, com ja hem dit abans, es podria obrir un debat sobre si la primera criptografia no eren ja els mateixos idiomes o maneres d'escriure, i per tant, la criptografia es remunta a l'origen dels temps...

En qualsevol cas, és a partir del segle XIX, després de la invenció de la mecànica electromagnètica complexa, com la màquina de motors Enigma, que es van desenvolupar mètodes de xifrat més sofisticats i eficients. Finalment, la introducció de l'electrònica i la computació va permetre el desenvolupament de sistemes elaborats que, avui dia, continuen tenint una gran complexitat.

A l'inici del treball no pensava que hi hauria tants mètodes criptogràfics com els que he trobat, de fet, però, és normal, si volem transmetre un missatge amb un codi xifrat, el millor per assegurar que ningú altre coneix el codi és inventar-ne un de nou. He fet un recull dels més importants al llarg de la història, i em centraré en l'anàlisi d'uns quants d´ells que ens ajudaran a veure una mica l'evolució de la criptografia.

- Jeroglífics egipcis
- Escítala espartana- permutació
- Railfence- permutació
- Xifrat de Cèsar-Roda de Cèsar
- Xifrat de Kama-Sutra
- Xifrat de Pigpen
- Xifrat d'Atbash
- Xifrat Afí
- Xifrat mono alfabètic general
- Xifrat de vigènere
- Xifrat de Playfair
- Xifrat homofònic
- Xifrat del llibre
- Codi A D F G V K
- Xifrats 2a guerra mundial: Enigma
- Mètodes moderns (DES, AES...)

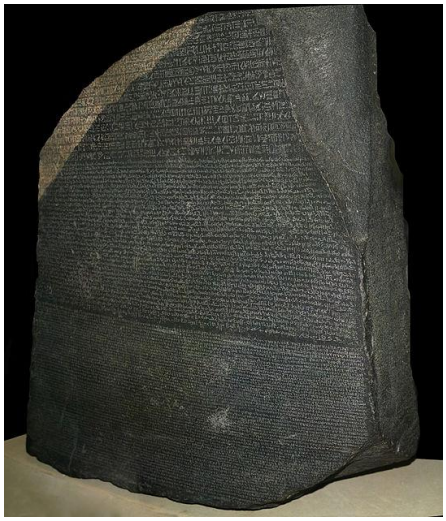
Si ens remuntem al passat, tal com hem dit abans, podríem dir que les diverses llengües i dialectes que hi ha arreu del món són la criptografia més bàsica i antiga.

3.4.1 Jeroglífics egipcis

Els jeroglífics egipcis van ser utilitzats pels egipcis entre el 3100 aC i 400 dC. És considerada l'escriptura més bella del món, ja que està formada per pictogrames que representen objectes naturals o artificials.

Els egipcis no utilitzaven paper i llapis per escriure, sinó que picaven pedres, és per això que avui dia encara es poden veure jeroglífics egipcis autèntics que es conserven en les parets de les piràmides d'Egipte. Com per exemple, un conjunt de jeroglífics d'uns 5.200 anys d'antiguitat que van descobrir el 2017 uns arqueòlegs de la Universitat de Yale i dels Museus Reials d'Art i Història de Brussel·les a Elkab, al sud de Luxor.[1]

Il·lustració 2: jeroglífic trobat a Elkab, al sud de Luxor. EL PERIÓDICO



Il·lustració 3: Pedra Rosseta exposada en el museu britànic.

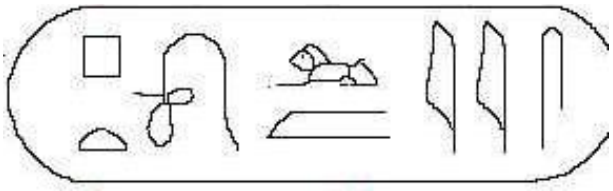
Aquesta escriptura es va mantenir incomprensible fins al segle XIX, quan Jean-François Champollion va desxifrar-la completament. Això va ser possible gràcies al descobriment de la pedra Rosseta, una pedra amb un mateix text escrit en dues llengües: grec i egipci, i tres escriptures: grec, jeroglífic i demòtic.

A l'hora de desxifrar es troben diverses hipòtesis que ajuden a aconseguir-ho:

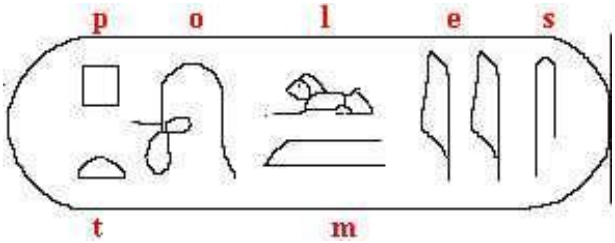
1. Se sap que els jeroglífics transcriuen la llengua copta.
2. Els cartutxos encerclen noms de Déus i faraons.
3. Els animals ens indiquen per on s'ha de llegir segons on estan mirant ells.

[1] Noticia extreta de National Geographic al 22.09.19
https://www.nationalgeographic.com.es/historia/actualidad/descubren-unos-los-jeroglificos-egipcios-mas-antiguos-5200-anos-antiguedad_11650/4

Un exemple de jeroglífic és aquest:



Aquest text està envoltat per un cartutx, per tant és el nom d'un Déu o faraó; el lleó del centre està mirant cap a l'esquerre, per tant, es comença a llegir per allà; i, a hores d'ara, sabem que en aquest jeroglífic hi posa: Ptolmes, més conegut com a Ptolemeu, el Salvador.



3.4.2 Escítala espartana

Un altre mètode criptogràfic antic és l'Escítala, utilitzada pels espartans. És considerada com la primera tècnica d'encriptació per transposició, és a dir, amagar el contingut del text alterant l'ordre lògic.

Il·lustració 4: Una escítala espartana amb un papir enrotllat.

L'Escítala consistia en un cilindre o un prisma de fusta on s'enrotllava un papir o una tira de cuir. Llavors, s'escrivia el missatge horitzontalment, d'aquesta manera, quan es desenrotllava les lletres quedaven desordenades. Per desxifrar-lo, només calia enrotllar el missatge en un cilindre del mateix diàmetre que l'utilitzat per xifrar el missatge.

Per exemple: hem agafat un cilindre de xcm de diàmetre on hi hem enrotllat un paper, llavors hi hem escrit en horitzontal el missatge "**demà menjaré macarrons amb formatge**".

Tot seguit, hem desenrotllat el paper i hem obtingut el missatge xifrat: "**dmaaraoteercomrgmneanbmeajmrsfa**"

Il·lustració 5: Un exemple d'escítala, un paper enrotllat amb un missatge escrit.

Il·lustració 6: El paper desenrotllat que ens revela el missatge encriptat.

3.4.3 Xifrat de Cèsar

El xifrat de Cèsar és un sistema d'encriptació de l'època de Juli Cèsar, d'aquí el nom del xifrat. Aquest és un dels xifrats de substitució més senzills, consisteix a desplaçar l'alfabet 3 llocs a la dreta, per exemple:

Original	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
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

Vist d'una forma més matemàtica, podem substituir les lletres per nombres: a-00, b-01, c-02,...,z-25. Llavors hi sumem la clau, que són els llocs que s'ha desplaçat l'alfabet, és a dir, codi=text+clau. En el xifrat de Cèsar és 3, a+clau=00+3=03=d, b+clau=01+3=04=e, etc. En les últimes xifres, el resultat de la suma és un nombre que no correspon a cap lletra, per exemple, y+clau=24+3=27. Aleshores, el que es fa és restar 26, el nombre de lletres totals a l'alfabet, per tal que obtinguem una lletra al codi. En aquest cas, a la lletra y li correspon la b.

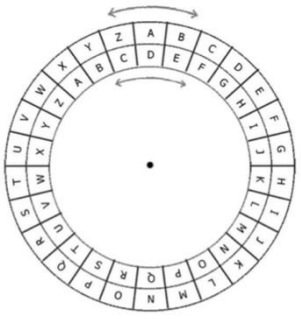
Matemàticament: f(x) = x + 3 (mod 26)

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

Si transformem la m:
f(m)= f(12)= 12+3 (mod 26)= 15= P
si transformem la y:
f(y)= f(24)= 24+3 (mod 26)= 27(mod26)= 1= P

Un exemple d'encriptació seria:
Missatge: "**Demà menjaré macarrons amb formatge**"
Missatge encriptat: "ghpd phqmduh pdfduurqv dpe irupdwjh" – si llavors traiem els espais, quedaria: "**ghpdphqmduhpdfduurqvdpeirupdwjh**"
Per poder desencriptar el missatge el receptor ha de saber la clau i invertir el procés i finalment, si el missatge està format per més d'una paraula, separar-les.

Més endavant hi va haver una millora en aquest xifrat anomenada RODA DE CÈSAR, un sistema d'encriptació formada per dues rodes de diferent mida i centrades en el mateix punt. Al voltant de cadascuna de les rodes hi ha escrites les lletres de l'alfabet. La roda gran conté les lletres del missatge original i la roda petita les del text codificat. El que es fa és, segons la clau, girar la roda petita per tal que les lletres del text sense xifrar i del xifrat coincideixin, si la clau és 3, la lletra *a* de la roda gran ha de coincidir amb la *d* de la roda petita, la *b* amb la *e*, etc.



Il·lustració 7: una roda de cèsar

El pas de xifratge que fa l'algorisme de Cèsar sovint forma part d'esquemes de codificació més complexos com el xifrat de Vigènere.1

3.4.4 Xifrat de Vigènere

Aquest xifrat és un xifrat emprat en la part pràctica, on tenim un missatge xifrat d'aquesta manera però en desconeixem la clau.

La invenció d'aquest xifrat es va atribuir a Blaise de Vigènere al segle XIX, d'aquí el nom. Però, va ser Giovan Batista Belas qui va descriure el mètode original en el seu llibre *La xifra del Sig Giovan Batista Belas* l'any 1553. Giovan es va basar en la taula de vigènere que havia inventat Johannes Trithemius l'any 1508, però va afegir una clau repetida per anar canviant de caràcter.

És un xifrat que sembla irresoluble, i per això, també se'l coneix com *El codi indesxifrable*. Tot i que ja veurem si ho és o no al final del treball, ja que intentaré desxifrar un text xifrat en vigènere, sense saber-ne la clau.

Aquest xifrat consisteix a substituir utilitzant un codi diferent depenent de la posició de la lletra. Per aquest mètode s'utilitza la taula següent, on les lletres de la primera fila, en negreta, corresponen al text original i les lletres de la primera columna, també en negreta, són les que corresponen amb la paraula clau. Com veurem a la taula de la pàgina següent:

a	b	c	ç	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
b	c	ç	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	ç	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
ç	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
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	ç
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	ç	d
f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	ç	d	e
g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	ç	d	e	f
h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	ç	d	e	f	g
i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	ç	d	e	f	g	h
j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	ç	d	e	f	g	h	i
k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	ç	d	e	f	g	h	i	j
l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	ç	d	e	f	g	h	i	j	k
m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	ç	d	e	f	g	h	i	j	k	l
n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	ç	d	e	f	g	h	i	j	k	l	m
o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	ç	d	e	f	g	h	i	j	k	l	m	n
p	q	r	s	t	u	v	w	x	y	z	a	b	c	ç	d	e	f	g	h	i	j	k	l	m	n	o
q	r	s	t	u	v	w	x	y	z	a	b	c	ç	d	e	f	g	h	i	j	k	l	m	n	o	p
r	s	t	u	v	w	x	y	z	a	b	c	ç	d	e	f	g	h	i	j	k	l	m	n	o	p	q
s	t	u	v	w	x	y	z	a	b	c	ç	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
t	u	v	w	x	y	z	a	b	c	ç	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
u	v	w	x	y	z	a	b	c	ç	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
v	w	x	y	z	a	b	c	ç	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
w	x	y	z	a	b	c	ç	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
x	y	z	a	b	c	ç	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
y	z	a	b	c	ç	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
z	a	b	c	ç	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

Taula 1: Taula de Vigènere amb ç

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

Taula 2: Taula de Vigènere sense ç

En aquest cas, utilitzarem la taula amb la ç.

Llavors, s'utilitza una paraula prèviament acordada que serveix de clau, per exemple "mates". En taronja hi ha marcats els diversos codis que s'utilitzaran d'acord amb la clau "mates".

Text	**a**	**b**	**c**	**ç**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	ç	d	e	f	g	h	i	j	k	l
A	a	b	c	ç	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
T	t	u	v	w	x	y	z	a	b	c	ç	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
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	ç	d
S	s	t	u	v	w	x	y	z	a	b	c	ç	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r

La primera lletra del missatge es codifica utilitzant el codi on la primera lletra és la "m", la segona lletra amb la fila que comença amb la lletra "a", i així successivament. Quan s'ha acabat la paraula clau, es torna a començar fins a obtenir tot el missatge xifrat.

Com que a la clau hi ha la lletra "a", quan toqui xifrar amb aquest codi, la lletra del missatge encriptat serà la mateixa que la del missatge original.

Per exemple, si es vol encriptar el missatge "**demà menjaré macarrons amb formatge**":
d (codi "m") – q
e (codi "a") – e
m (codi "t") – f
etc.
Missatge xifrat: "qefe ernçejq mtvejdogx szb ztjzamlx", i traiem els espais: "**qefeernçejqmtveidogxszbztjzamlx"**
El receptor, si sap la clau del missatge, podrà desxifrar el missatge fàcilment invertint el procés. En cas de desconèixer la clau, aquest xifrat no es pot atacar utilitzant l'anàlisi de freqüències, ja que no sabem la llargada de la paraula clau, i cada lletra utilitza un codi diferent. És per això que és un dels mètodes més segurs i complicats de desxifrar. No va ser fins al s.XIX, que el mètode Kasiski va aconseguir resoldre el xifratge.

3.4.5 Mètode Kasiski

És un mètode de criptoanàlisi (un atac criptogràfic) publicat l'any 1863 per Friedrich Kasiski.

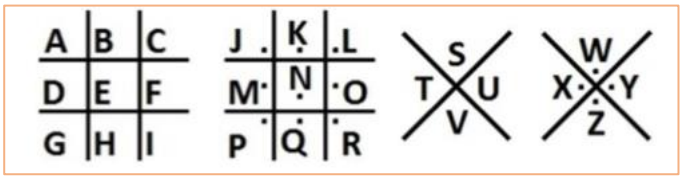
Aquest mètode consisteix a buscar paraules repetides al text, per tal de poder descobrir la llargada de la paraula clau. Kasiski es va adonar que hi havia paraules repetides en el text xifrat, les quals, amb molta probabilitat, també eren la mateixa paraula al text original i, a més a més, la clau coincidia igual per a les dues paraules. Llavors, Kasiski sabia que la distància entre les dues paraules repetides era múltiple de la llargada de la paraula clau i per tant, només era qüestió de buscar diverses paraules repetides i trobar-ne el màxim comú divisor, d'aquesta manera trobar un nombre proper a la longitud de la clau, la qual serà aquest mateix nombre o un factor primer d'aquest.

El mètode explicat pas a pas seria:

1. Busquem grups de lletres repetits al text
2. Contem el nombre de lletres entre repetició i repetició (des d'on comença el primer grup de paraules repetides a on torna a comença al segon grup, és a dir, del mateix lloc al mateix lloc)
3. Amb tots els nombres aconseguits busquem el màxim comú divisor.
4. Un cop tenim el màxim comú divisor, dividim el text en grups de n lletres (el nombre de lletres que ens indica el màxim comú divisor)
5. Llavors, sabem que cada lletra està codificada amb un codi diferent, però la primera de cada grup amb el mateix codi, igual que la segona de cada grup, que també està codificada amb el mateix codi, i així amb totes.
6. Finalment, per descobrir la paraula clau s'utilitza el mètode de freqüències dels xifrats monoalfabètics generals, que explicarem més endavant.

3.4.6 Xifrat de Pigpen

El xifrat de pigpen és un altre xifrat que utilitza la substitució, en aquest cas, el missatge original no se substitueix per lletres ni nombres, sinó que va marcat per un codi de símbols fix i universal:

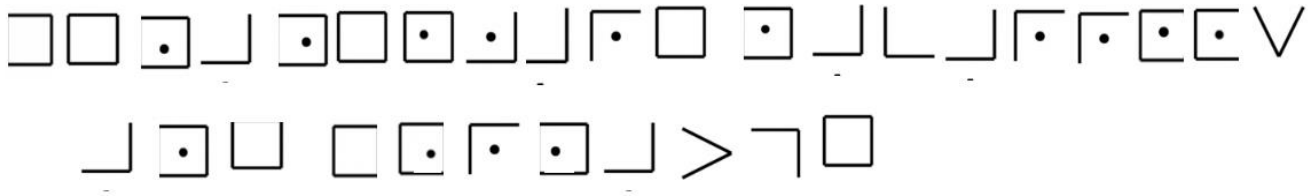


Il·lustració 8: Codi de signes de Pigpen

Per escriure el missatge xifrat es dibuixa el tros de dibuix que ocupa la lletra, és a dir, els segments i els punts.

Per exemple:
Missatge: “Demà menjaré macarrons amb formatge”

Missatge xifrat:



Per desxifrar-lo, el receptor ha d’invertir el procés i fàcilment trobarà el missatge.

3.4.7 Xifrat monoalfabètic general

Aquest, juntament amb el xifrat de Vigènere, són els mètodes emprats en la part pràctica.

Tots els anteriors mètodes de substitució, menys el xifrat de pigpen, es poden incloure en aquest xifrat, on a cada lletra n’hi correspon una altra de qualsevol.

Per exemple:

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

A l'hora d'encriptar el missatge funciona igual que en els mètodes anomenats anteriorment, és a dir, substituint la lletra del text original per la que la codifica. Però, a l'hora que el receptor hagi de desencriptar el missatge, ha de conèixer molt bé la clau per invertir el procés, ja que aquest mètode té moltes possibles claus: la lletra *a* pot ser codificada per totes les 26 lletres; la *b* pot anar amb totes les lletres exceptuant la que va amb la lletra a, per tant, pot codificar amb 25 lletres; la lletra *c* pot anar amb totes les lletres exceptuant les que van amb la *a* i la *b*, és a dir, pot anar amb 24 lletres, per tant, en total hi ha $26 \cdot 25 \cdot 24 \cdot \ldots \cdot 3 \cdot 2 \cdot 1 \simeq 4 \cdot 10^{26}$ possibles claus.

Per tant, com podem desxifrar un missatge que ha estat encriptat amb el xifrat monoalfabètic generat sense saber-ne la clau?

Els mètodes més utilitzats són buscar lletres repetides com "ss" o "rr", en el cas del català, o buscar apòstrofs, ja que només poden estar envoltats d'unes certes lletres. Un altre mètode seria mirant la freqüència de cadascuna de les lletres, o de grups de lletres, i consultar taules que ens donen la freqüència en què s'utilitzen en funció de l'idioma. Cada idioma té unes freqüències diferents que poden variar segons el text que s'ha escollit.

Per exemple, en català, la freqüència mitjana seria:

Taula 3: Freqüències de les lletres en la llengua Catalana.

lletra	A	B	C	Ç	D	E	F	G	H	I	J	K	L	M
%	12,55	1,32	3,60	1,06	3,94	13,89	1	1,28	0,72	6,99	0,3	0	7,74	3,16
lletra	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
%	6,40	5,71	2,72	1,35	6,76	8,43	6,11	4,18	1,4	0	0,52	0	0,01	

En un text xifrat en català, probablement, les lletres que apareguin més correspondran a la *e* i la *a*.

Normalment, quan has de desxifrar un missatge i veus que és molt llarg et penses que és més complicat que no pas si fos més curt però, és tot el contrari, els missatges llargs solen ser més fàcils de desxifrar, ja que, és on pots trobar més pistes, com apòstrofs, o lletres repetides, etc.

3.4.8 Màquina Enigma

Amb la màquina enigma avancem en el temps fins al segle XX. Fins llavors, els mètodes d'encriptació havien de ser desxifrats manualment.

Il·lustració 9: Màquina enigma exposada en el museu Criptogràfic Nacional, Fort Meade, Maryland, USA

L'alemany Arthur Scherbius va inventar Enigma l'any 1918 perquè els alemanys la poguessin utilitzar a la primera guerra mundial.

Els primers models de la màquina, el model A i el model B, eren pesats i ocupaven força espai però, l'any 1925 va sortir el model C, un model més lleuger i petit que, a més a més, tenia un reflector (ja n'explicarem la funció més endavant). El model bàsic constava d'un teclat per escriure, un panell de llums, tres o quatre rotors i un reflector.

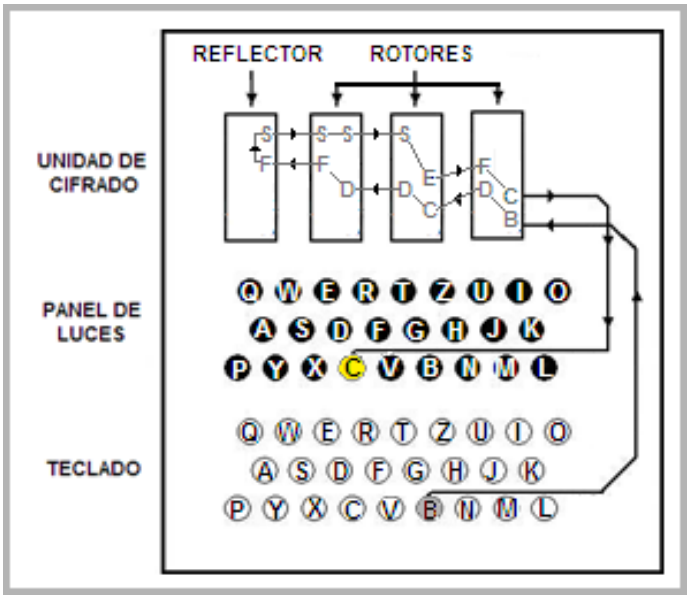
De màquines de desxifratge n'hi havia moltes, per exemple, es diu que els alemanys van utilitzar més de 30.000 màquines diferents segons si eren atacs submarins, terrestres... durant la guerra.

Però, com funcionava la famosa Màquina Enigma?

És una màquina electromecànica, té una part mecànica i una part elèctrica. La part mecànica consisteix en un teclat, com un teclat qualsevol d'una màquina d'escriure però, amb la diferència que en clicar la tecla s'activen uns interruptors que fan girar els rotors que hi ha a l'interior de la màquina. El que fan aquests rotors és canviar les posicions de les lletres de l'alfabet, cada vegada que s'escriu una lletra el rotor es desplaça una posició, per això l'alfabet canvia. Però, si només hi hagués un sol rotor, quan haguéssim codificat una lletra 26 vegades, llavors obtindríem la codificació inicial. És per això que hi ha tres rotors, per evitar aquesta repetició. Dels tres rotors, n'hi ha un que va de pressa, un que no va tan ràpid i un tercer que va lent. Quan es canvia una lletra, el primer rotor, el ràpid, es desplaça una posició; quan el primer rotor ha canviat 26 vegades de posició, el segon rotor canvia una posició, i el mateix passa amb el tercer. Per entendre'ns, és com si fos un rellotge, quan

la broca dels segons ha fet una volta sencera, la dels minuts avança una posició, i el mateix amb les hores, quan la dels minuts ha fet tota la volta, avança.

El que fa el reflector és permetre que es torni a reflectir el senyal, d'aquesta manera torna a passar pels rotors i apareix al panell de llums la lletra codificada.

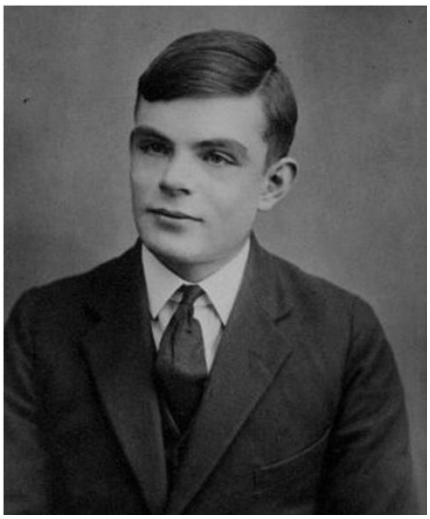


Il·lustració 10: Parts del mecanisme d'una màquina Enigma i el seu funcionament

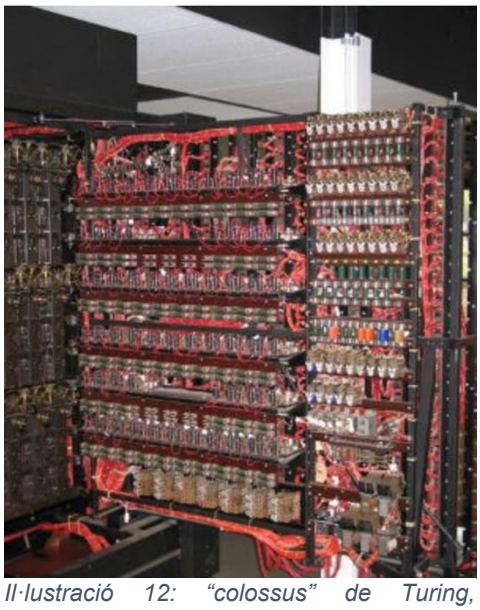
A més a més, els alemanys hi van introduir un claviller per poder canviar lletres, per exemple, si s'intercanviaven la C per la M, cada vegada que s'escrivia la C era com escriure una M, i el mateix a la inversa. Això ho feien per, en cas que algú aconseguís desxifrar els missatges, algunes lletres no li lliguessin i no pogués entendre del tot el missatge.

Un nom per recordar, **Alan Turing**, un matemàtic britànic considerat el pare de la ciència de la computació i la informàtica, ja que va aconseguir desxifrar la màquina Enigma, cosal que li va permetre escurçar la guerra uns dos anys i salvar milers de vides.

No obstant això, el mèrit inicial era dels polonesos, que portaven des de 1919 amb una unitat especialitzada intentant desxifrar missatges. Però, tot això no va ser possible fins que un agent francès va aconseguir les taules de combinacions de dos mesos que li van permetre al matemàtic Marian Rejewski entendre el funcionament exacte de la màquina Enigma. Llavors, ell i el seu equip van construir un objecte electromagnètic capaç de desxifrar missatges anomenat “Bomba” pel soroll que feien els motors quan funcionaven.



Il·lustració 11: Alan Turing a l’edat de 16 anys



Il·lustració 12: “colossus” de Turing, Bletchley Park. IAN PETTICREW.

El 25 de juliol de 1939, poc abans que Polònia caigués en mans dels alemanys, el servei d’intel·ligència polonesa va informar dels seus avenços a França i a Gran Bretanya. En un principi no els va servir de gaire, però els britànics van formar una divisió criptogràfica anomenada Bletchley Park al nord de Londres, on treballava Turing. Allà, i com a part del programa Ultra (ultrasecret), Turing va construir un ordinador anomenat “colossus” que era exclusiu per a trobar claus que l’ajudessin amb la reconfiguració de la màquina després del canvi de rotors.

L’èxit de la descodificació es deu, en part, a l’esforç de desenes de matemàtics, enginyers i oficials d’intel·ligència però també, a alguns errors per part dels alemanys. Aquest èxit, però, va romandre secret durant la guerra i alguns anys després també, per així evitar que Alemanya descobrís que el codi de la màquina Enigma havia estat descodificat, ja que en pocs dies l’haguessin pogut canviar i tot l’esforç dels polonesos i britànics no hauria servit per res.

3.4.9 DES

Després de la Màquina Enigma, i amb els avenços tecnològics, els mètodes criptogràfics van agafar una gran complexitat i dificultat a l'hora de desxifrar. Un exemple de mètode criptogràfic modern és el DES (Data Encryption Standard), dissenyat l'agost de 1974, amb la idea de ser un estàndard de xifrat per a totes les institucions governamentals dels Estats Units.

Es tracta d'un xifrat simètric (ja veurem què significa més endavant) on un text amb una longitud fixa pateix una sèrie d'operacions d'acord amb la clau acordada per obtenir un text xifrat de la mateixa longitud que la inicial. En el DES s'utilitzen claus de 56 bits i mides de blocs de 64 bits. Per entendre-ho amb més facilitat, es podria comparar amb un xifrat monoalfabètic general, amb la diferència que en lloc d'haver-hi 26! (on n!=n·(n-1)(n-2)...3·2·1) permutacions n'hi ha 2^{64}!, ja que hi ha 64 bits, és a dir, un nombre molt gran.
És un mètode considerat insegur perquè les claus són massa curtes i, a causa d'això, es diu que la NSA (National Security Agency) té un mètode per desxifrar-lo.

Més tard, es van dissenyar nous mètodes a partir del DES, entre ells, el Triple DES (TDES), que consistia a aplicar el DES tres vegades, amb dues o tres claus diferents, anomenats 2TDES i 3TDES, respectivament. Aquest mètode era més segur que el DES, però era més lent.

A arrel d'aquest mètode, van sorgir forces mètodes criptogràfics moderns i complexos, per exemple el RC5, el Blowfish, l'IDEA, el NewDES, el SAFER, el CAST5, el DES-X i el GDES, entre d'altres.

3.4.10 Criptografia moderna

En els apartats anteriors he explicat els mètodes de criptografia clàssics que es podrien aplicar d'una manera "manual" o amb petites maquinetes. Podríem seguir amb nous mètodes cada cop més i més complexos que requereixen més capacitat de càlcul, algoritmes molt elaborats i ordinadors més potents. Tots aquests mètodes són els que

s’apliquen avui dia en molts àmbits de la vida (Whatsapp, Telegram, transaccions bancàries, etc.).

Tots aquests mètodes no els he considerat perquè requereixen ordinadors més potents amb capacitat de fer càlculs amb algoritmes molt complexos, els quals estan fora del meu abast.

3.5 Mètodes d'encriptació

Els principals mètodes d'encriptació es poden dividir en dos grups, la criptografia simètrica i la criptografia asimètrica, depenen de si una sola clau es fa servir per xifrar i desxifrar o no.

3.5.1 Criptografia simètrica

La criptografia simètrica només utilitza una sola clau per xifrar i desxifrar, la qual han de conèixer tant l'emissor com el receptor.

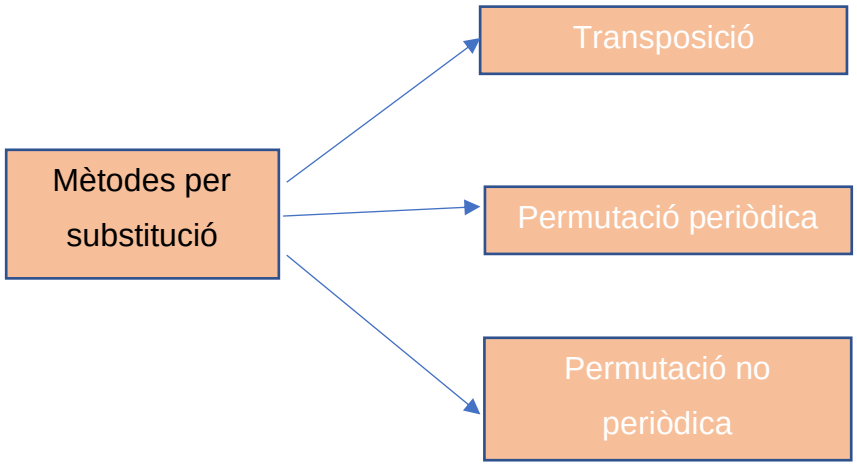
Els xifrats simètrics són els més ràpids i eficients, tot i que quan dos usuaris es volen enviar un missatge s'han de trobar per acordar una clau, ja que el mètode més segur de donar la clau al receptor és trobar-se amb ell i així assegurar-se que ha rebut correctament la clau i que ningú més la sap (recordem que en la comunicació la responsabilitat és de l'emissor, és l'emissor qui s'ha d'assegurar que el receptor sap la clau). És per això que, majoritàriament, la criptografia simètrica s'utilitza per a l'emmagatzematge de dades on només una persona necessita la clau.

Aquest és el tipus de xifrat més antic i l'únic que s'utilitzava a l'inici de la criptografia fins fa uns 40 anys, quan Diffie i Hellman van inventar el xifrat asimètric.

Dins del xifrat simètric hi trobem els dos grans grups on es classifiquen els mètodes d'encriptació:

Mètodes de permutació

Els mètodes més senzills són els de permutació, ja que l'únic que es modifica del missatge és el seu ordre, el qual ha de ser prèviament acordat entre l'emissor i el receptor. Aquests mètodes es poden classificar tres grups:



- En la **transposició** s'ha de dividir el missatge a xifrar en blocs de n lletres i llavors es van permutant les lletres de cada bloc de la mateixa manera, és a dir, cada bloc es desordena de la mateixa manera.

Un exemple seria el **mètode dels blocs**, que consisteix a canviar l'ordre de les lletres del missatge mitjançant una clau composta per una sèrie de nombres que ens indiquen l'ordre final, és a dir, si la clau consta de 5 nombres per exemple (2,3,5,1,4) dividim el missatge en blocs de cinc lletres i a l'hora de xifrar-lo en primer lloc hi posarem la lletra que en el missatge original està en segona posició, llavors la de la tercera, i així successivament. Finalment, es treuen els espais. Per desxifrar el missatge, si es té el coneixement de la clau, és tan fàcil com invertir el procés.

- Clau: **(2,3,5,1,4)** – hi ha 5 nombres, per tant, el text es divideix en blocs de 5 lletres, també ens indica l'ordre en què mourem les lletres, la segona del missatge original passarà a ser la primera i el mateix amb les altres. Finalment es treuen els espais.
- Missatge:

"**demà menjaré macarrons amb formatge**"
demam enjar emaca rrons ambfo rmatg e
emmda njrea maaec rosrn mboaf magrt e
"**emmdanjreamaaecrosrnmboafmagrte**"

El **mètode de les caixes** utilitza una clau que sol ser una paraula però no s'utilitzen les lletres sinó que el que fa servei és l'ordre en què apareixen a l'alfabet, d'aquesta manera el receptor, si sap la paraula clau, ja sap l'ordre en què ha estat modificat el missatge.

- Clau: **MARTINA (4,1,6,7,3,5,2)**– L'ordre en què surten a l'alfabet. Que s'utilitzarà per determinar l'ordre en què agafarem els blocs de lletres: primer s'agafarà el 4, després l'1 i fins a agafar el 2.
- Missatge: "**demà menjaré macarrons amb formatge**"

1	**2**	**3**	**4**	**5**	**6**	**7**
D	E	M	A	M	E	N
J	A	R	E	M	A	C
A	R	R	O	N	S	A
M	B	F	O	R	M	A
T	G	E				

AEOO / DJAMT / EASM / NCAA / MRRFE / MMNR / EARBG

- Missatge xifrat: **aeoodjamteasmncaamrrfemmnrearbg**

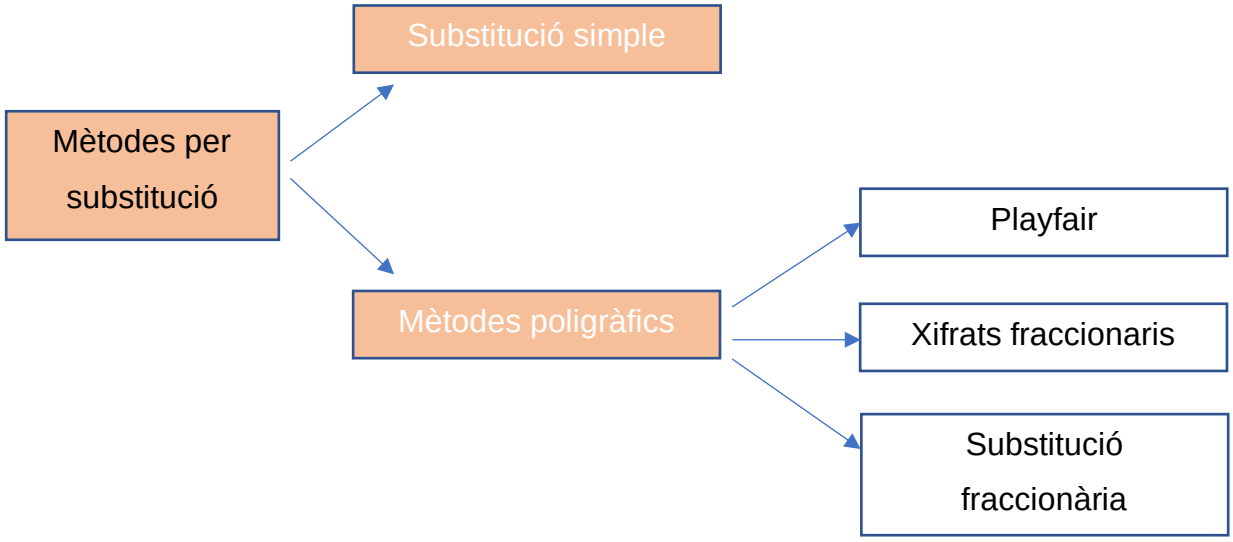
Però, són segurs els mètodes de permutació? Hi ha una anècdota històrica que enforteix la seguretat d'aquests mètodes. A l'agost de l'any 1610, Galileu va enviar un missatge xifrat amb aquest mètode a Kepler, SMAISMRMILMEPOETALEVMIBVNENVGTTAVIRES el qual té unes 9603027212041843553021368320000000 combinacions, però Kepler ho va interpretar malament, entenent SALVE VMBISTINEVM GEMINATVM MARTIA PROLES, que significa "Salve, ardents bessons, fills de mart". Kepler no anava mal encaminat, ja que el missatge original era ALTISSIMVM PLANETAM TERGEMINVM OBSERVAVI, que traduït és "vaig observar que el planeta més alt era triple". Aquesta equivocació ens suggereix que la barreja de lletres dona molta seguretat i que si no sabem amb certesa el mètode utilitzat, ens podem trobar com Kepler, que va interpretar un missatge que tenia sentit però, era erroni.

Mètodes per substitució

Els mètodes per substitució consisteixen a canviar els caràcters del missatge original per altres de diferents que poden ser lletres, números, símbols... Aquests mètodes són els més

comuns i els que la majoria de xifrats utilitzen, com ara el Xifrat de Cèsar, el Xifrat Afí, o el de Vigènere.

Els mètodes per substitució es classifiquen en:



La **substitució simple** és el mètode més senzill de tots. Consisteix a canviar una lletra de l'alfabet per una altra, sempre la mateixa i diferent de la original. Dintre la substitució simple hi trobaríem el xifrat de Cèsar, anteriorment descrit. Un exemple seria:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|
f	**h**	**j**	**l**	**n**	**o**	**r**	**t**	**v**	**x**	**z**	**c**	**e**	**g**	**i**	**k**	**m**	**p**	**q**	**s**	**w**	**y**	**u**	**a**	**d**	**b**

Missatge original: "Demà menjaré macarrons amb formatge"

Missatge xifrat: "lnef engrfpn efjfppigq feh oipefsrn" – llavors es treuen els espais. – "**inefengrfpnefjfppigqfehoipefsrn**"

Els **mètodes poligràfics** són més complexos, ja que la substitució és duta a terme amb blocs de diverses lletres en comptes de substituir-ne només una. Aquests mètodes queden subdividits en 3 grups:

Playfair, o també conegut com a **substitució digràmica**, consisteix a dividir el text en blocs de dues lletres, les quals són substituïdes per una altra parella de lletres diferents, per exemple:

de	**ma**	**me**	**nj**	**ar**	**em**	**ac**	**ar**	**ro**	**ns**	**am**	**bf**	**or**	**ma**	**tg**	**e**
l	l	l	l	l	l	l	l	l	l	l	l	l	l	l	l
jk	**ac**	**rf**	**gv**	**tx**	**gh**	**em**	**fr**	**bn**	**lk**	**ws**	**ab**	**mn**	**er**	**po**	**q**

“**demà menjaré macarrons amb formatge**”

“de ma me nj ar em ac ar ro ns am bf or ma tg e”

“jk ac rf gv tx gh em fr bn lk ws ab mn er po q”

“**jkacrfgvtxghemfrbnlkwsabmnerpoq**”

Els **xifrats fraccionaris** consisteixen a dividir el text en blocs de n lletres, els quals passen a ser nombres, que llavors són canviats per altres de diferents i, finalment, són tornats a convertir en lletres. A cada nombre li correspon un grup de n lletres i hi haurà tants nombres com lletres hi hagi. Al final és com si fos un xifrat de permutació perquè al final és com si s’hagués modificat l’ordre de les lletres.

Per exemple: n=3

dem	ame	nja	rem	aca	rro	nsa	mbf	orm	atg	e
I	I	I	I	I	I	I	I	I	I	I
145	984	244	376	812	357	342	785	120	320	4

145	984	244	376	812	357	324	785	120	320	4
I	I	I	I	I	I	I	I	I	I	I
812	145	320	324	785	145	984	376	320	4	244

“**demà menjaré macarrons amb formatge**”

“14598424437681235734278512032 04”

“81214532032478514598437632042 44”

“**academatgnsambfdemameremat genja**”

Els mètodes per **substitució fraccionària** s’utilitza una matriu com a clau a més a més d’un nombre. A cada lletra li correspon un nombre, llavors, les lletres s’agrupen en blocs de ‘n’ lletres. Aquests s’operen com vectors i es multipliquen per una matriu quadrada. D’aquesta manera obtenim un altre vector, que serà el bloc xifrat. Per a desxifrar el missatge cal multiplicar el vector xifrat per la matriu inversa de la utilitzada anteriorment.

- Clau: **n=3 i** $\begin{pmatrix} \mathbf{1} & \mathbf{3} & \mathbf{2} \\ \mathbf{4} & \mathbf{2} & \mathbf{1} \\ \mathbf{1} & \mathbf{2} & \mathbf{4} \end{pmatrix}$ ⟶ **d-3, e-6, m-2, a-4, n-1, j-5, r-7, c-9, o-8, s-0**

Missatge: **Demà menjaré macarrons ⟶ dem ame nja rem aca rro ns ⟶**

362 426 154 762 494 778 10

$$(3 \quad 6 \quad 2) \cdot \begin{pmatrix} 1 & 3 & 2 \\ 4 & 2 & 1 \\ 1 & 2 & 4 \end{pmatrix} = (25 \quad 25 \quad 20\ ) \ (mod\ 9) = (\ 7 \quad 7 \quad 2)$$

$$(4 \quad 2 \quad 6) \cdot \begin{pmatrix} 1 & 3 & 2 \\ 4 & 2 & 1 \\ 1 & 2 & 4 \end{pmatrix} = (24 \quad 28 \quad 30\ ) \ (mod\ 9) = (\ 6 \quad 1 \quad 3)$$

$$(1 \quad 5 \quad 4) \cdot \begin{pmatrix} 1 & 3 & 2 \\ 4 & 2 & 1 \\ 1 & 2 & 4 \end{pmatrix} = (25 \quad 21 \quad 23\ ) \ (mod\ 9) = (\ 7 \quad 3 \quad 5)$$

$$(7 \quad 6 \quad 2) \cdot \begin{pmatrix} 1 & 3 & 2 \\ 4 & 2 & 1 \\ 1 & 2 & 4 \end{pmatrix} = (33 \quad 37 \quad 28\ ) \ (mod\ 9) = (\ 6 \quad 1 \quad 1)$$

$$(4 \quad 9 \quad 4) \cdot \begin{pmatrix} 1 & 3 & 2 \\ 4 & 2 & 1 \\ 1 & 2 & 4 \end{pmatrix} = (44 \quad 38 \quad 33\ ) \ (mod\ 9) = (\ 8 \quad 2 \quad 6)$$

$$(7 \quad 7 \quad 8) \cdot \begin{pmatrix} 1 & 3 & 2 \\ 4 & 2 & 1 \\ 1 & 2 & 4 \end{pmatrix} = (43 \quad 51 \quad 53\ ) \ (mod\ 9) = (\ 7 \quad 6 \quad 8)$$

10

Missatge xifrat: **772613735611826768l0 ⟶ rrmendrdjennomereons**

3.5.2 Criptografia asimètrica

La criptografia asimètrica va ser inventada per W. Diffie i M. Hellman, dos matemàtics de la Universitat de Stanford, l'any 1975. Diffie i Hellman van tenir la idea sobre inventar la criptografia asimètrica per tal que l'emissor i el receptor no s'haguessin de trobar prèviament per acordar la clau, sinó que cadascú tingués una clau pública, la qual podria conèixer tothom, i una clau privada, la qual només podria conèixer el propietari de la clau. Això es podria dur a terme utilitzant unes funcions matemàtiques d'un sol sentit, és a dir, que siguin senzilles de calcular per un sentit, però molt difícils per l'altre.

La criptografia asimètrica se sol utilitzar per intercanviar claus de manera segura, i la simètrica, per enviar missatges i dades. Per exemple, el protocol d'intercanvi de claus de Diffie i Hellman:

Protocol d'intercanvi de clau de Diffie-Hellman

Hi ha una fase prèvia abans de començar amb l'intercanvi. Tenim a l'Anna (A) i en Bernat (B), junts escullen dos nombres (per telèfon), per exemple, 6 i 8. Llavors, tots dos saben que faran servir la següent funció:

$$\mathbf{f(x)} = \boldsymbol{6^x\ (mod\ 8)}$$

Comença l'intercanvi de clau, tots dos trien un nombre i en mantenen en secret.

$$\boldsymbol{S_A = 4}$$
$$\boldsymbol{S_B = 2}$$

Seguidament, tant l'Anna com en Bernat calculen la funció aplicada al seu nombre que mantenen en secret.

$$\boldsymbol{f(4) = 6^4 (mod\ 8) = 1296\ (mod\ 8) = 0}$$
$$\boldsymbol{f(2) = 6^2 (mod\ 8) = 36\ (mod\ 8) = 4}$$

Llavors, l'Anna envia el resultat de la seva funció, és a dir, 0. I el mateix fa en Bernat amb el 4. En aquest pas qualsevol pot escoltar la transmissió.

Finalment, amb el nombre que han rebut un de l'altre l'eleven amb el seu secret.

$$\mathbf{4^{SA}(mod\ 8) = 4^{4}(mod\ 8) = 0}$$
$$\mathbf{0^{SB}(mod\ 8) = 0^{2}(mod\ 8) = 0}$$

Tots dos obtenen el mateix: 0, que és la clau! Aquesta clau es pot utilitzar per diversos mètodes criptogràfics, com per exemple en el mètode de Railfence o el xifrat de Cèsar.

3.6 Tipus de textos

Hi ha diversos tipus de missatges: els missatges que s'entenen perfectament, els que són força complicats de desxifrar, els que no ho són tant i els que són impossibles de desxifrar. Els missatges encriptats ens poden classificar en 4 casos tot seguint una taula com aquesta:

	Llengua coneguda	Llengua desconeguda
Escriptura coneguda	Cas 1	Cas 2
Escriptura desconeguda	Cas 3	Cas 4

Cas 1: En textos que siguin del cas 1 no tenen cap problema, ja que els podem llegir i entendre perfectament.

Cas 2: En el cas 2 hi trobaríem l'etrusc, una llengua procedent del nord d'Itàlia utilitzada per la civilització etrusca al segle VII a.C. L'alfabet etrusc està inspirat en el grec, per tant transcriu sons tant vocàlics com consonàntics, és per això que nosaltres som capaços de llegir en veu alta els textos però no entenem res del que posa. Aquest cas ens demostra el que havíem dit abans, que la llengua és una forma d'encriptar, i que no cal remuntar-nos a segles abans de crist per trobar exemples. Per exemple, avui dia qualsevol persona que no sàpiga anglès, per molt que llegeixi textos en veu alta perquè estan escrits amb un alfabet molt semblant al nostre, no entendrà el que hi posa.

Cas 3: Els textos dins del cas 3 s'acaben desxifrant a cop de proves, com per exemple els jeroglífics egipcis o els petròglifs maies. Per desxifrar els textos es poden utilitzar les taules de freqüències que hi ha per cada llengua, i així anar fent proves i que el text agafi forma i sentit.

Cas 4: Són textos impossibles de desxifrar, l'única manera és reduir-los al cas 3, per aconseguir això s'han de fer hipòtesis raonables sobre quina és la llengua de l'escriptura.

4. PART PRÀCTICA

La part pràctica d'aquest treball es divideix en dues parts:

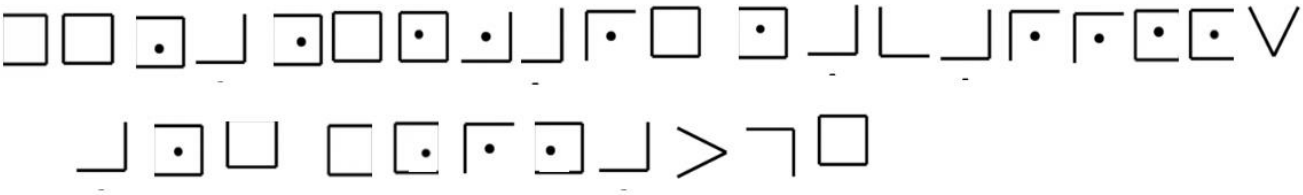
- La primera part es tracta del procés d'encriptació, la qual està inclosa en la part teòrica perquè són exemples dels mètodes explicats.
- La segona part és com un repte per mi, ja que intentaré desxifrar 3 missatges encriptats sense cap ajuda electrònica (ordinador, programa electrònic...) i sense saber-ne la clau ni el mètode, només sabré el mètode utilitzat en un sol text, per tant, els altres dos mètodes els descobriré al llarg del treball, o no.

4.1 Part 1: Un mateix missatge xifrat en diversos mètodes

Al llarg de la part teòrica he hagut de fer diversos exemples amb tots els mètodes criptogràfics estudiats, és per això que puc fer-ne un recull per poder veure'n amb més claredat les diferències.

He utilitzat el mateix missatge pels diferents mètodes: "Demà menjaré macarrons amb formatge". I xifrat ha quedat així:

- Escítala Espartana: **dmaaraoteercomrgmneanbmeajmrsfa**
- Xifrat de Cèsar**: ghpdphqmduhpdfduurqvdpeirupdwjh**
- Xifrat de Vigènere**: qefeernçejqmtveidogxszbztjzamlx**
- Xifrat de Pigpen**:**



- Mètode dels blocs**: emmdanjreamaaecrosrnmboafmagrte**
- Mètode de les caixes**: aeoodjamteasmncaamrrfemmnrearbg**
- Substitució simple**: inefengrfpnefjfppigqfehoipefsrn**
- Playfair**: jkacrfgvtxghemfrbnlkwsabmnerpoq**
- Xifrats fraccionaris**: academatgnsambfdemamerematgenja**
- Substitució fraccionària: **rrmendrdjennomereons (demà menjaré macarrons)**

4.2 Part 2: El repte

Com ja he dit abans, la part 2 és com un repte per mi, i consisteix a intentar desxifrar 3 missatges sense saber-ne la clau ni el mètode.

El primer pas per poder començar a desxifrar és conèixer una mica d'on prové el text, en quin idioma està escrit l'original, qui és l'emissor i qui és el receptor i, sobretot, conèixer la clau. Però, és clar, aquestes informacions no sempre se saben, i menys la clau, ja que només és coneguda per l'emissor i el receptor. I això és el que consisteix aquesta part pràctica, ja que, tal com he dit abans, no sóc coneixedora de cap d'aquestes dades. D'aquesta manera és com si jo fos una persona no autoritzada que intenta interceptar el missatge per desxifrar-lo i així saber-ne el contingut.
Aquesta part del treball té la finalitat de qüestionar i experimentar la seguretat dels mètodes criptogràfics, dels 3 utilitzats quin és més segur, quin menys, quin és més difícil de desxifrar...

4.2.1 Text xifrat 1

El primer text que em va passar en David Juher és un text xifrat per algun mètode de substitució el qual no en tinc coneixença.

hw bzbfodhqb uqauwthqwfeoh cyh fcyhwbf uqkzjdfnuz hwbumyu iukjfaf wu fcyhwbf qhnhwwubfb ah tjzbhnnuz yw whdeof hifmhjfaf thqwhy cyh qz nfohq yqw nzqhuihdhqbw mfujh dhw hohpfbw ahow cyh tzb bhquj cyfowhpzo oounhqnufb hq uqkzjdfbunf z bhohnzdyqunfnuzqw thj tzahj fbfnfj kuwunfdhqb of ifjif u oohmuj cyfowhpzo duwwfbmh cyh gu nujnyou

És un text xifrat per substitució on es mantenen els espais. No sé en quina llengua està escrit, per tant el puc classificar dins el cas 4 explicat prèviament, llavors, hauria d'estudiar-ne la història, el seu origen... però com que és un text que m'ha passat en David Juher, professor de la Universitat de Girona penso que està escrit en Català, Castellà o Anglès, com que no ho tinc clar començaré per determinar la quantitat de cada lletra diferent per

llavors utilitzar les taules de freqüències que tenen els diversos idiomes, ja que en ser un text xifrat per substitució entra dins el xifrat monoalfabètic general el qual es descodifica mitjançant les freqüències.
Aquests són els caràcters més freqüents després de fer un recompte de totes les lletres:

h (41)	o (17)	c (8)	p (3)
f (32)	n (16)	a (6)	e (2)
u (27)	z (15)	t (6)	g (1)
w (23)	y (14)	m (5)	
b (19)	j (13)	i (5)	
q (18)	d (9)	k (4)	

Un cop ja tinc totes les lletres comptades i tinc clar quines són les més freqüents he d'utilitzar les taules de freqüència en funció de l'idioma que creiem que ha estat utilitzat. En aquest cas utilitzaré la taula de freqüència de la llengua catalana. Que el text estigui escrit és una hipòtesi que pot ser certa o no, en cas que no i a mesura que el text vagi agafant forma i vegi que no té sentit tornaré a començar agafant la taula de freqüència d'una altra llengua com el castellà o l'anglès.

lletra	A	B	C	Ç	D	E	F	G	H	I	J	K	L	M
%	12,55	1,32	3,60	1,06	3,94	13,89	1	1,28	0,72	6,99	0,3	0	7,74	3,16
lletra	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
%	6,40	5,71	2,72	1,35	6,76	8,43	6,11	4,18	1,4	0	0,52	0	0,01	

Segons la taula puc suposar que:

h (41) = E	o (17)	c (8)	p (3)
f (32) = A	n (16)	a (6)	e (2)
u (27)	z (15)	t (6)	g (1)
w (23)	y (14)	m (5)	
b (19)	j (13)	i (5)	
q (18)	d (9)	k (4)	

Ew bzbAodEqb uqauwtEqwAeoE cyE AcyEwbA uqkzjdAnuz Ewbumyu iukjAaA wu AcyEwbA qEnEwwubAb aE tjzbEnnuz yw wEdeoA EiAmEjAaA tEqwEy cyE qz nAoEq yqw nzqEuiEdEqbw mAujE dEw EoEpAbw aEow cyE tzb bEquj cyAowEpzo oounEqnuAb Eq uqkzjdAbunA z bEoEnzdyqunAnuzqw tEj tzaEj AbAnAj kuwunAdEqb oA iAjiA u ooEmuj cyAowEpzo duwwAbmE cyE gu nujnyou

Un cop he substituït les E i les A al text puc comprovar que hi ha un grup de 3 lletres que es repeteix, i que la última lletra és una E, per tant, he de buscar algunes lletres que sempre vagin juntes, per exemple la Q i la U, que juntament amb la E fan QUE.

h (41) = E	o (17)	c (8) = Q	p (3)
f (32) = A	n (16)	a (6)	e (2)
u (27)	z (15)	t (6)	g (1)
w (23)	y (14) = U	m (5)	
b (19)	j (13)	i (5)	
q (18)	d (9)	k (4)	

Ew bzbAodEqb uqauwtEqwAeoE QUE AQUEwbA uqkzjdAnuz EwbumUu iukjAaA wu AQUEwbA qEnEwwubAb aE tjzbEnnuz Uw wEdeoA EiAmEjAaA tEqwEU QUE qz nAoEq Uqw nzqEuiEdEqbw mAujE dEw EoEpAbw aEow QUE tzb bEquj QUAowEpzo oounEqnuAb Eq uqkzjdAbunA z bEoEnzdUqunAnuzqw tEj tzaEj AbAnAj kuwunAdEqb oA iAjiA u ooEmuj QUAowEpzo duwwAbmE QUE gu nujnUou

Amb aquesta substitució de la Q i la U ja es poden començar a deduir algunes paraules, com per exemple, les assenyalades al text superior. Puc pensar que poden ser AQUELLA

o AQUESTA, però les dues lletres desconegudes són diferents, per tant, em decantaré per AQUESTA.

h (41) = E	o (17)	c (8) = Q	p (3)
f (32) = A	n (16)	a (6)	e (2)
u (27)	z (15)	t (6)	g (1)
w (23) = S	y (14) = U	m (5)	
b (19) = T	j (13)	i (5)	
q (18)	d (9)	k (4)	

ES TzTAodEqT uqauStEqSAeoE QUE AQUESTA uqkzjdAnuz ESTumUu iukjAaA Su AQUESTA qEnESSuTAT aE tjzTEnnuz US SEdeoA EiAmEjAaA tEqSEU QUE qz nAoEq UqS nzqEuiEdEqTS mAujE dES EoEpATS aEoS QUE tzT TEquj QUAoSEpzo oounEqnuAT Eq uqkzjdATunA z TEoEnzdUqunAnuzqS tEj tzaEj ATAnAj kuSunAdEqT oA iAjiA u ooEmuj QUAoSEpzo duSSATmE QUE gu nujnUou

Cada vegada tenim més lletres i més pistes. El següent pas que seguiré serà buscar lletres repetides que vagin juntes en parella, ja que en català hi puc trobar doble ss, rr, mm, nn, ll. Però a principi de mot només hi ha la possibilitat de trobar doble l, així que substituiré les O per L.

h (41) = E	o (17) = L	c (8) = Q	p (3)
f (32) = A	n (16)	a (6)	e (2)
u (27)	z (15)	t (6)	g (1)
w (23) = S	y (14) = U	m (5)	
b (19) = T	j (13)	i (5)	
q (18)	d (9)	k (4)	

ES TzTALdEqT uqauStEqSAeLE QUE AQUESTA uqkzjdAnuz ESTumUu iukjAaA Su AQUESTAqEnESSuTAT aE tjzTEnnuz US SEdeLA EiAmEjAaA tEqSEU QUE qz nALEq UqS nzqEuiEdEqTS mAujE dES ELEpATS aELS QUE tzT TEquj QUALSEpzL LLunEqnuAT Eq uqkzjdATunA z TELEnzdUqunAnuzqS tEj tzaEj ATAnAj kuSunAdEqT LA iAjiA u LLEmuj QUALSEpzL duSSATmE QUE gu nujnULu

A poc a poc es van deduint paraules, ara puc deduir que les marcades volen dir QUALSEVOL.

h (41) = E	o (17) = L	c (8) = Q	p (3) = V
f (32) = A	n (16)	a (6)	e (2)
u (27)	z (15) = O	t (6)	g (1)
w (23) = S	y (14) = U	m (5)	
b (19) = T	j (13)	i (5)	
q (18)	d (9)	k (4)	

ES TOTALdEqT uqauStEqSAeLE QUE AQUESTA uqkOjdAnuO ESTumUu iukjAaA Su AQUESTA qEnESSuTAT aE tjOTEnnuO US SEdeLA EiAmEjAaA tEqSEU QUE qO nALEq UqS nOqEuiEdEqTS mAujE dES ELEVATS aELS QUE tOT TEquj QUALSEVOL LLunEqnuAT Eq uqkOjdATunA O TELEnOdUqunAnuOqS tEj tOaEj ATAnAj kuSunAdEqT LA iAjiA u LLEmuj QUALSEVOL duSSATmE QUE gu nujnULu

A aquestes altures moltes paraules ja poden ser deduïdes, per tant es poden substituir força lletres, per exemple puc deduir que la paraula marcada és TELECOMUNICACIONS.

h (41) = E	o (17) = L	c (8) = Q	p (3) = V
f (32) = A	n (16) = C	a (6)	e (2)
u (27) = I	z (15) = O	t (6)	g (1)
w (23) = S	y (14) = U	m (5)	
b (19) = T	j (13)	i (5)	
q (18) = N	d (9) = M	k (4)	

ES TOTALMENT lNaIStENSAeLE QUE AQUESTA lNkOjMACIO ESTlmUl ilkjAaA SI AQUESTA NECESSITAT aE tjOTECCIO US SEMeLA EiAmEjAaA tENSEU QUE NO CALEN UNS CONEIiEMENTS mAIjE MES ELEVATS aELS QUE tOT TENIj QUALSEVOL LLICENCIAT EN lNkOjMATICA O TELECOMINICACIONS tEj tOaEj ATACAj kISICAMENT LA iAjiA I LLEmIj QUALSEVOL MISSATmE QUE gI CIjCILI

A hores d'ara ja puc tenir una idea del text i, encara que faltin algunes lletres per substituir, seria capaç d'entendre'l. Però jo seguiré substituint lletres com per exemple, canviaré la lletra K per la lletra F i la J per la R...

h (41) = E	o (17) = L	c (8) = Q	p (3) = V
f (32) = A	n (16) = C	a (6) = D	e (2) = B
u (27) = I	z (15) = O	t (6) = P	g (1)
w (23) = S	y (14) = U	m (5) = G	
b (19) = T	j (13) = R	i (5) = X	
q (18) = N	d (9) = M	k (4) = F	

ES TOTALMENT INDISPENSABLE QUE AQUESTA INFORMACIO ESTIGUI XIFRADA SI AQUESTA NECESSITAT DE PROTECCIO US SEMBLA EXAGERADA PENSEU QUE NO CALEN UNS CONEIXEMENTS GAIRE MES ELEVATS DELS QUE POT TENIR QUALSEVOL LLICENCIAT EN INFORMATICA O TELECOMINICACIONS PER PODER ATACAR FISICAMENT LA XARXA I LLEGIR QUALSEVOL MISSATGE QUE gl CIRCULI

Quasi tinc tot el text desxifrat, només em falta una lletra, la G que la canviaré per una H.

h (41) = E	o (17) = L	c (8) = Q	p (3) = V
f (32) = A	n (16) = C	a (6) = D	e (2) = B
u (27) = I	z (15) = O	t (6) = P	g (1) = H
w (23) = S	y (14) = U	m (5) = G	
b (19) = T	j (13) = R	i (5) = X	
q (18) = N	d (9) = M	k (4) = F	

ÉS TOTALMENT INDISPENSABLE QUE AQUESTA INFORMACIÓ ESTIGUI XIFRADA SI AQUESTA NECESSITAT DE PROTECCIÓ US SEMBLA EXAGERADA PENSEU QUE NO CALEN UNS CONEIXEMENTS GAIRE MÉS ELEVATS DELS QUE POT TENIR QUALSEVOL LLICENCIAT EN INFORMÀTICA O TELECOMINICACIONS PER PODER ATACAR FÍSICAMENT LA XARXA I LLEGIR QUALSEVOL MISSATGE QUE HI CIRCULI

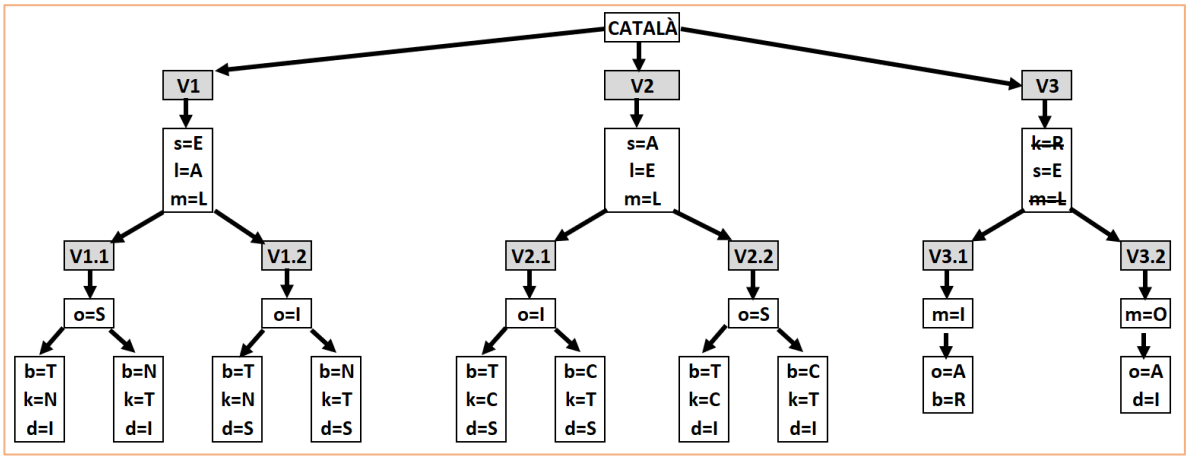
Finalment he aconseguit el missatge completament desxifrat!

4.2.2 Text xifrat 2

El segon text és un altre text xifrat utilitzant la substitució, amb la diferència que en aquest no s'han mantingut els espais, per tant, és un xic més complicat. Igual que en el primer text, no sé en quin idioma està escrit l'original, tampoc sé la seva procedència ni la seva destinació. Aquest és el text a desxifrar:

> gsjestdbdadcpbgjcasedysboskosnlbcnjltdasklhpsmmhpslacbksnpsdwcapmoljtdkdalysbosmydkklo
> nsolglbomcctsbomcdbqdkdimsocodhpssmydkklonsacylolmskgjsksbosblmnpbmmcadkdklisycbkly
> lnlcdbqsjodysmgjcasedysboecapmoladcklijsylaasedjlmoswodmmsndjmcdsbosbejsygsjtsaolysbolm
> mchpskfdedplhpskoskosabdhpskesalyptmlonskflbpodmdozlolmmmljnesocolmlfdkocjdl

Aquest text m'ha portat molta feina, al contrari que el text 1 on amb una única prova en vaig fer prou, en aquest text he fet diverses versions i proves que es troben exposades al final del treball en l'apèndix. Per poder controlar aquestes versions podem veure a continuació un gràfic on es marquen les diferències del que he anat provant en els diferents intents.



En aquests sis intents, com es veu en el quadre, he anat fent diferents substitucions de lletres i diferents combinacions d'aquestes substitucions, però en tots els intents al final arribava a una via morta on res tenia sentit.

Finalment, a la setena prova, i després de fer (com explico més endavant) una substitució massiva de lletres he vist la llum i he aconseguit arribar fins al final resolent el text. A continuació hi podem trobar aquest setè intent:

Text xifrat:

gsjestdbdadcpbgjcasedysboskosnlbcnjltdasklhpsmmhpslacbksnpsdwcapmoljtdkdalysbosmydkklo
nsolglbomcctsbomcdbqdkdimsocodhpssmydkklonsacylolmskgjsksbosblmnpbmmcadkdklisycbkly
lnlcdbqsjodysmgjcasedysboecapmoladcklijsylaasedjlmoswodmmsndjmcdsbosbejsygsjtsaolysbolm
mchpskfdedplhpskoskosabdhpskesalyptmlonskflbpodmdozlolmmmljnesocolmlfdkocjdl

En ser un text xifrat de la mateixa manera que el text 1, però amb la diferència dels espais, seguiré els mateixos passos, és a dir, començaré per determinar el nombre de cada lletra, per així ordenar-les de més freqüents a menys:

s (46)	k (21)	p (14)	t (6)
l (32)	c (20)	y (13)	h (6)
d (31)	b (20)	n (10)	w (2)
o (29)	a (16)	e (9)	z (1)
m (26)	j (14)	g (6)	

Ara ja tinc totes les lletres comptades i ordenades. Ja puc començar a substituir. Primer de tot agafaré la taula de freqüències de la llengua catalana, ja que, com que el primer text també me'l va passar en David Juher i estava escrit en català, penso que aquest podria estar també en català.

lletra	A	B	C	Ç	D	E	F	G	H	I	J	K	L	M
%	12,55	1,32	3,60	1,06	3,94	13,89	1	1,28	0,72	6,99	0,3	0	7,74	3,16
lletra	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
%	6,40	5,71	2,72	1,35	6,76	8,43	6,11	4,18	1,4	0	0,52	0	0,01	

He fet una estimació del que podria codificar cada lletra en funció de la taula de freqüències:

s (46) ~ E	m (26) ~ I	a (16) ~ O	n (10) ~ M
l (32) ~ A	k (21) ~ R	j (14) ~ U	e (9) ~ P
d (31) ~ S	c (20) ~ N	p (14) ~ D	g (6) ~ V
o (29) ~ L	b (20) ~ T	y (13) ~ C	t (6) ~ Q

h (6) ~ B w (2) ~ G z (1) ~ Ç

VERSIÓ 7:

Després de totes les provatures d'anar canviant lletra a lletra, i veient que cada cop acabo en un punt mort, miraré de fer-ho fent un canvi massiu de totes les lletres, a veure si amb un canvi massiu apareixen possibles paraules que em puguin donar alguna pista. Per a fer aquest canvi massiu el que faré serà aplicar estrictament la taula de freqüències i a veure què em surt. De la taula de freqüències només modificarem que intercanviarem la L i la I perquè si l'apliquéssim estrictament tenim tres mmm seguides que haurien de ser tres III, i en una altra de les versions ja hem provat de buscar sentit amb les tres I i no ho hem aconseguit. Per tant, el que farem serà intercanviar-les amb la de dalt i fer que la o = I i que la m = L ..... les altres les canviaré en el mateix ordre de la taula de freqüències.

s (46) ~ E	k (21) ~ R	p (14) ~ D	t (6) ~ Q
l (32) ~ A	c (20) ~ N	y (13) ~ C	h (6) ~ B
d (31) ~ S	b (20) ~ T	n (10) ~ M	w (2) ~ G
o (29) ~ L → I	a (16) ~ O	e (9) ~ P	z (1) ~ Ç
m (26) ~ I → L	j (14) ~ U	g (6) ~ V	

VEUPEQSTSOSNDTVUNOEPSCETIERIEMATNMUAQSOERABDELLBDEAONTREMDESGN
ODLIAUQSRSOACETIELCSRRAIMEIAVATILNNQETILNSTqSRSiLEINISBDE EL
CSRRAIMEONCAIALERVUERETIETALMDTLLNOSRSRAiECNTRACAMANSTqEUISCELVU
NOEPSCETIPNODLIAOSNRAiUECAOOEPSUALIEGISLLEMSULNSETIETPUECVEUQEOIAC
ETIALLNBDERfSPSDABDERIERIEOTSBDERPEOACDQLAIMERfATDISLSIzAIAL
LLAUMPEINIALAfSRINUSA

D'entrada el primer que faré serà separar dues E (així ja tenim un espai) i veure si podem intercanviar algunes lletres per donar sentit a alguna paraula. Per exemple al principi

comença per VEUPE, podria ser VEURE? Provem-ho, per a fer-ho hem de canviar la P per una R.

Com que la P té una freqüència baixa, potser el que hauria de fer és fer córrer totes les lletres un punt, no posar la R al lloc de la P..... per tant canviem les P per R i fem córrer les altres, però respectant la U que ja em va bé.

s (46) ~ E	k (21) ~ R – N	p (14) ~D – C	t (6) ~ Q
l (32) ~ A	c (20) ~ N –T	y (13) ~C – M	h (6) ~ B
d (31) ~ S	b (20) ~ T – O	n (10) ~M – P	w (2) ~ G
o (29) ~ L	a (16) ~O – D	e (9) ~P – R	z (1) ~ Ç
m (26) ~ I	j (14) ~ U	g (6) ~ V	

VEURE QSO SDSTCO

VUTDERSMEOIENIEPAOTPUAQSDENABCELLBCEADTONEPCESGTDCLIAUQSNSDAMEO I EL MSNNAIPE IAVAOILTTQEOILTSOqSNSiLEITISBCE EL MSNNAIPE DT MAI AL ENVUENEOIEOALPCOLLTDSNSNAiEMTONAMAPATSOqEUISMELVUTDERSMEOIRTDCLI ADSTNAiUEMAD

DERSUALIEGISLLEPSULTSEOIEORUEMVEUQEDIAMEOIALLTBCENfSRSCABCENIENIEDO SBC ENREDA MCQLAIPENfAOCISLSIzA I AL LLAUPREITIALAfSNITUSA

Guardem aquest VEURE i posem sentit a alguna altra paraula. Podria tenir un sentit per exemple que el text marcat en lila i que surt dues vegades, digués EL MISSATGE... això voldria dir que la S seria una I, que les N serien S, que la I seria T i la P seria G.

Per a fer aquests canvis, però, he de canviar també altres lletres afectades, ja que alguna de les que vull posar ara ja està agafada. Per a reassignar lletres seguiré igualment la taula de freqüències, intentant no moure's massa lluny d'on els tocaria.

Així doncs, a la T li assignaré la N (quadra bastant amb les freqüències) i a la P la faig córrer avall amb totes fins a la G.

s (46) ~ E	k (21) ~ N -- S	p (14) ~ C	t (6) ~ Q --V
l (32) ~ A	c (20) ~ T -- N	y (13) ~ M	h (6) ~ B -- Q
d (31) ~ S -- I	b (20) ~ O	n (10) ~ P -- G	w (2) ~ G -- B
o (29) ~ L	a (16) ~ D	e (9) ~ R -- P	z (1) ~ Ç
m (26) ~ I -- T	j (14) ~ U	g (6) ~ V -- R	

REUPE VIO IDINCO

RUNDEPIMEOTESTEGAONGUAVIDESAQCELLQCEADNOSEGCEIBNDCLTAUVISIDAMEO

T EL MISSATGE TARAOTLNNVEOTLNIOqISIiLETNTIQCE EL MISSATGE DN MAT AL

ESRUESEOTEOALGCOLLNDISISAiEMNOSAMAGANIOqEUTIMELRUNDEPIMEOTPNDCLT

ADINSAiUEMADDEPIUALTEBTILLEGIULNIEOTEOPUEMREUVEDTAMEOTALLNQCESfIPI

CAQCESTESTEDOIQC ESPEDA MCVLATGESfAOCTILIT zATAL

LLAUGPETNTALAfISTNUIA

Ull, que ara he vist que hi havia encara unes “i” (3) i unes “q” (2) i unes f (2) que no havia considerat, i que em poden fer variar les posicions de les lletres....

Tornem a posar la taula i hi afegim aquestes lletres que em falten. El que faré serà també moure l’ordre per a mantenir-lo tal com està en la taula de freqüències, això em fa canviar la lletra B per una X, doncs ara la B és la i que m’havia descuidat. També aprofito per posar a la z=F doncs al final sembla que hi ha una paraula que podria dir fatal, i la F mirant la taula de freqüències surt molt poc (o sigui que ja quadraria).

s (46) ~ E	c (20) ~ N	n (10) ~ G	q (2) - H
l (32) ~ A	b (20) ~ O	e (9) ~ P	w (2) ~ *B* –X
d (31) ~ I	a (16) ~ D	g (6) ~ R	f (2) - Y
o (29) ~ L	j (14) ~ U	t (6) ~ V	z (1) ~ F
m (26) ~ T	p (14) ~ C	h (6) ~ Q	
k (21) ~ S	y (13) ~ M	i (3) – B	

REUPE VIO IDINCO
RUNDEPIMEOTESTEGAONGUAVIDESAQCELLQCEADNOSEGCEIXNDCLTAUVISIDAMEO
T EL MISSATGE TARAOTLNNVEOTLN IOHISIBLE TNT I QCE EL MISSATGE DN MAT AL
ESRUESEOTEOALGCOLLNDISISABEMNOSAMAGANIOHEUTIMELRUNDEPIMEOTPNDCL
TADINSABUEMADDEPIUALTEXTILLEGIULNIEOTEOPUEMREUVEDTAMEOTALLNQCESY
IPICAQCESTESTEDOIQC ESPEDA MCVLATGESYAOCTILIT FATAL
LLAUGPETNTALAYISTNUIA

Amb aquestes noves lletres afegides començo a trobar no ja paraules soltes, sinó una frase que podria tenir sentit, com és el tall que diu **IOHISIBLE TNT I QCE EL MISSATGE** que semblaria que vol dir **"INVISIBLE TOT I QUE EL MISSATGE"**, cosa que voldria dir que tinc la O i la N capgirades. Anem doncs a canviar les O per N i les N per O, i he de canviar la C per una U (aquestes dues les intercanvio també doncs són molt properes) i la H per una V (també les intercanvio)

s (46) ~ E	c (20) ~ N -- O	n (10) ~ G	q (2) - H -- V
l (32) ~ A	b (20) ~ O -- N	e (9) ~ P	w (2) ~ X
d (31) ~ I	a (16) ~ D	g (6) ~ R	f (2) - Y
o (29) ~ L	j (14) ~ U -- C	t (6) ~ V -- H	z (1) ~ F
m (26) ~ T	p (14) ~ C -- U	h (6) ~ Q	
k (21) ~ S	y (13) ~ M	i (3) – B	

RECPE HIN IDIOUN
RCODEPIMENTESTEGANOGCAHIDESAQUELLQUEADONSEGUEIXODULTACHISIDAMEN
T EL MISSATGE TARANTLOO HENT LO INVISIBLE TOT I QUE EL MISSATGE DO MAT AL
ESRCESENTENALGUNLLODISISABEMONSAMAGAOINVECTIMELRCODEPIMENTPODUL
TADIOSABCEMADDEPICALTEXTILLEGICLOIENTENPCEMRECHEDTAMENTALLOQUESY
IPIUAQUESTESTEDNIQU ESPEDA MUHLATGESYANUTILIT FAT AL LLACG PE TOTA LA
YISTOCIA

Ara ja es comencen a veure coses amb més sentit, per exemple tinc ja tota una frase llarga marcada en vermell que podem dir que és quasi bona (falla una lletra). També puc veure al final que posa TOTA LA YISTOCIA, cosa que diu que la Y és una H i que el canvi que he fet de canviar la U per una C no era correcte, per tant ara hauria de canviar la Y per una H i la C per una R (aquest últim no el fem encara).
També mirant HENT i UTILITFAT, semblaria que la H ha de ser una F i que la F ha de ser una Z, ja ho puc canviar. Faré aquests 3 canvis

s (46) ~ E	c (20) ~ O	n (10) ~ G	q (2) - V
l (32) ~ A	b (20) ~ N	e (9) ~ P	w (2) ~ X
d (31) ~ I	a (16) ~ D	g (6) ~ R	f (2) – Y -- H
o (29) ~ L	j (14) ~ C	t (6) ~ H -- F	z (1) ~ F--Z
m (26) ~ T	p (14) ~ U	h (6) ~ Q	
k (21) ~ S	y (13) ~ M	i (3) – B	

RECPE FIN IDIOUN
RCODEPIMENTESTEGANOGCAFIDESAQUELLQUEADONSEGUEIXODULTACFISIDAMENT EL MISSATGE TARANTLOO FENT LO INVISIBLE TOT I QUE EL MISSATGE DOMAT AL ESRCESENTEN ALGUN LLOD I SI SABEM ON SAMAGA O INVECTIM EL RCODEPIMENT PODULTADIOSABCEMADDEPICALTEXTILLEGICLOIENTENPCEMRECFEDTAMENTALLO QUESHIPIUAQUESTESTEDNIQU ESPEDA MUFLATGESHAN UTILITZAT AL LLACG PE TOTA LA HISTOCIA

De la part marcada en blau **UTILITZAT AL LLACG PE TOTA LA HISTOCIA** veig clar que la C ha de ser una R i que la P ha de ser una D, vaig a veure com puc fer aquests canvis. També si miro la paraula **RCODEPIMENT,** vieg que segurament el que vol dir és **PROCEDIMENT.** Per tant el que tinc és que la R és una P, la C es R (ja ho havia vist) i la D es C, per tant he d'intercanviar totes aquestes...

s (46) ~ E	c (20) ~ O	n (10) ~ G	q (2) - V
l (32) ~ A	b (20) ~ N	e (9) ~ P --D	w (2) ~ X
d (31) ~ I	a (16) ~ D --C	g (6) ~ R -- P	f (2) – H
o (29) ~ L	j (14) ~ C -- R	t (6) ~ F	z (1) ~Z
m (26) ~ T	p (14) ~ U	h (6) ~ Q	
k (21) ~ S	y (13) ~ M	i (3) – B	

PERDE FIN ICIOUN PROCEDIMENTESTEGANOGRAFICESAQUELLQUEACONSEGUEIXOCULTARFISICAMENT EL MISSATGE TAPANTLOO FENT LO INVISIBLE TOT I QUE EL MISSATGE COMAT AL ESPRESENTEN ALGUN LLOC I SI SABEM ON SAMAGA O INVERTIM EL PROCEDIMENT DOCULTACIOSABREMACCEDIRALTEXTILLEGIRLOIENTENDREMPERFECTAMENTALLO QUESHIDIUAQUESTESTECNIQU ESDECA MUFLATGESHAN UTILITZAT AL LLARG DE TOTA LA HISTORIA

I ara ja ho tinc, si intento llegir el text tot seguit, veig que té sentit i que només em falta posar-li els espais i els signes de puntuació i ortogràfics...

PER DEFINICIÓ UN PROCEDIMENT ESTEGANOGRÀFIC ÉS AQUELL QUE ACONSEGUEIX OCULTAR FÍSICAMENT EL MISSATGE TAPANT-LO O FENT-LO INVISIBLE, TOT I QUE EL MISSATGE COM A TAL ÉS PRESENT EN ALGUN LLOC I SI SABEM ON S'AMAGA O INVERTIM EL PROCEDIMENT D'OCULTACIÓ SABREM ACCEDIR AL TEXT I LLEGIR-LO, I ENTENDREM PERFECTAMENT ALLÒ QUE S'HI DIU. AQUESTES TÈCNIQUES DE CAMUFLATGE S'HAN UTILITZAT AL LLARG DE TOTA LA HISTÒRIA

El punt definitiu per a resoldre aquest exercici ha estat el fet de fer la substitució massiva de lletres. Al principi no m'atrevia a fer-ho i anava fent lletra a lletra, però no hi havia manera

d'avançar, ja que no era capaç de trobar cap mena de patró que em pogués donar idea de per on anar. Quan m'he decidit a fer la substitució massiva i a intentar donar significat a paraules és quan realment he avançat, tot i que és curiós que la primera paraula amb la qual m'he fixat i que he intentat donar-li significat ha estat la primera del text (intentava buscar una paraula que servis per a començar un text), i he trobat **VEUPE** que semblava que tenia sentit si la P era una R... al final aquest "VEURE" ha estat "PER DEFINICIÓ", és a dir, que no ha tingut res a veure.
La segona amb la qual m'he fixat ha estat **EL MSNNAIPE** que resulta que sortia dues vegades i que posant-hi ganes podia voler dir "EL MISSATGE" (cal tenir en compte que donat el tema del treball he pensat que el text podia tenir a veure amb la criptografia, i que per tant la paraula missatge podia molt ben ser que hi fos). Aquesta suposició ha estat la clau que m'ha portat a resoldre el text, ja que un cop he tingut MISSATGE m'han anat apareixent altres possibles paraules i anant intercanviant lletres han anat agafant sentit.

Podríem dir que un punt molt important per a poder desxifrar un missatge quan no saps com està xifrat és que com a mínim sàpigues de què pot anar, perquè així quan trobes una possible paraula et dóna més idees...

Tot i això, al final l'única manera de resoldre'l és a força de fer moltes iteracions i canvis de lletres, i de posar-hi hores (amb aquest he estat moltes hores i molts dies davant l'ordinador per a treure'l). Lògicament, si hagués tingut un ordinador que hagués fet totes les iteracions i canvis de lletres segurament hauria durat segons.

4.2.3 Text xifrat 3

Nota important: A l´hora de explicar el tercer exercici he anat fent-ho a mesura que anava resolent-ho (o intentant resoldre'l), i a vegades he hagut de tornar amunt i afegir lletres o suposicions, que en algun moment pot fer que sigui difícil de seguir la explicació, però ho he fet així per no repetir mil vegades les taules i no allargar-me massa. Si en algun punt no s'entén prou millor seguir llegint i més endavant ja es va clarificant.

El missatge número 3 és un text xifrat sense espais utilitzant el mètode de vigènere, és per això que no es poden utilitzar les taules de freqüències, ja que no sé la llargada de la clau. En aquest cas, el missatge xifrat és en majúscules, per tant, substituirem amb minúscules.

PTPVTVSXLMXYVSXLHKWLNWPWDKRNCDHOIIEHLHYKJAQQMLBJQYPWOFGRILXKJL
EROIXBKUROIVLUOWSSWXJAGZRCXXUITBMTGTYCEBOZUYYIHXDPPLVPXDERTMOE
UOQPWDBTAEXFOEKEQAWCTUORLUEXVLQZRCMIEIILSUVIBLPQNESWTKXXJDMYXO
ECIKPRMBRIIYGOKKEWZGKLZORDJSGJIXZXOFVTYYWMTETMNWKFSEPDUETCSWPQ
LERCSXYXBTAVDIKFSEPDWONJCSYKOGVRIDXYMVSGZPDTETEEIXMRMIYXOEJUHZPC
WVLQZRCMIEIWTBHKAKZRSLKAMOIXMZFMNEEGJPEEVYGJSSYSBLHUIPWBXGEXPM
HXEMSWXCHMIRE

Per poder desxifrar aquest missatge utilitzaré el Mètode Kasiski, explicat anteriorment. Per començar, buscaré grups de lletres que es repeteixin:

PTPVT VSXLM XYVSX LHKWL NWPWD KRNCD HOIIE HLHYK JAQQM LBJQY PWOFG
RILXK JLERO IXBKU ROIVL UOWSS WXJAG ZRCXX UITBM TGTYC EBOZU YYIHX DPPLV
PXDER TMOEU OQPWD BTAEX FOEKE QAWCT UORLU EXVLQ ZRCMI EIILS UVIBL
PQNES WTKXX JDMYX OFCIK PRMBR IIYGO KKEWZ GKLZO RDJSG JIXZX OFVTY
YWMTE TMNWK FSEPD UETCS WPQLE RCSXY XBTAV DIKFS EPDWO NJCSY KOGVR
IDXYM VSGZP DTETE EIXMR MIYXO EJUHZ PCWVL QZRCM IEIWT BHKAK ZRSLK
AMOIX MZFMN EEGJP EEVYG JSSYS BLHUI PWBXG EXPMH XEMSW XCHMI RE

Un cop ja tinc repeticions puc aplicar el mètode, el que he de fer és: determinar la distància entre repetició i repetició i llavors buscar el màxim comú divisor (m.c.d)

De VLQZRCMIEI a VLQZRCMIEI hi ha 161 lletres.
De KFSEPD a KFSEPD hi ha 28 lletres.
De YXOE a YXOE hi ha 119 lletres
De TET a TET hi ha 63

No considero repeticions de dues lletres doncs fàcilment podrien ser dues lletres iguals dins una mateixa paraula...

Si miro els que tinc:

Els divisors de 161 són: 7 i 23
Els divisors de 28 són: 4 i 7
Els divisors de 119 són: 7 i 17
Els divisors de 63 son: 7 i 9

Per tant la paraula clau té una longitud de 7 caràcters.

Un cop descoberta la longitud de la paraula clau, ara el que he de fer és agafar el text i dividir-lo en grups de 7 lletres (longitud paraula inicial) i després fer 7 sub-textos, el primer agafant la primera lletra de cada grup, el segon amb la segona... fins a l'última, doncs cada un d'aquests sub-textos estarà codificat amb la mateixa seqüència de lletres. Analitzant aquests sub-textos hauríem de ser capaços de trobar la paraula clau.

Divideixo en grups de 7:

PTPVTVS XLMXYVS XLHKWLN WPWDKRN CDHOIIE HLHYKJA QQMLBJQ YPWOFGR
ILXKJLE ROIXBKU ROIVLUO WSSWXJA GZRCXXU ITBMTGT YCEBOZU YYIHXDP
PLVPXDE RTMOEUO QPWDBTA EXFOEKE QAWCTUO RLUEXVL QZRCMIE IILSUVI
BLPQNES WTKXXJD MYXOECI KPRMBRI IYGOKKE WZGKLZO RDJSGJI XZXOFVT
YYWMTET MNWKFSE PDUETCS WPQLERC SXYXBTA VDIKFSE PDWONJC SYKOGVR
IDXYMVS GZPDTET EEIXMRM IYXOEJU HZPCWVL QZRCMIE IWTBHKA KZRSLKA
MOIXMZF MNEEGJP EEVYGJS SYSBLHU IPWBXGE XPMHXEM SWXCHMI RE

I ara creo 7 sub-divisions:

Primera lletra:

PXXWCHQYIRRWGIYYPRQEQRQIBWMKIWRXYMPWSVPSIGEIHQIKMMESIXSR

Segona lletra:

TLLPDLQPLOOSZTCYLTPXALZILTYPYZDZYNDPXDDYDZEYZZWZONEYPPWE

Tercera lletra:

PMHWHHMWXIISRBEIVMWFWURLPKXRGGJXWWUQYIWKXPIXPRTRIEVSWMX

Quarta lletra:

VXKDOYLOKXVWCMBHPODOCECSQXOMOKSOMKELXKOOYDXOCCBSXEYBBHC

Cinquena lletra:

TYWKIKBFJBLXXTOXXEBETXMUNXEBKLGFTFYEBFNGMTMEWMHLMGGLXXH

Sisena lletra:

VVLRIJJGLKUJXGZDDUTKUVIVEJCRKZJVESCRTSJVVERJVIKKZJJHGEM

Setena lletra:

SSNNEAQREUOAUTUPEOAEOLEISDIIEOITTESCAECRSTMULEAAFPSUEMI

Un cop fets els grups, he d'aplicar l'anàlisi de freqüències a cada un dels grups i intentaré trobar quina és la lletra més repetida a veure si em dóna idea de quina pot ser la paraula clau (la lletra més repetida, per l'anàlisi de freqüència hauria de ser una E). Més endavant, com que he vist que amb només la lletra més repetida no arribava enlloc, el que faig es agafar més possibilitats, o sigui que marco totes les més repetides i les considero possibles E. Les diferencio per colors per tenir en compte quines són més probables (més repetides)

Primera lletra:

PXXWCHQYIRRWGIYYPRQEQRQIBWMKIWRXYMPWSVPSIGEIHQIKMMESIXSR

P=4 → E	W=5 →E	H=2
X=4→ E	C=1	Q=5→E

Y=4 →E	E=3	S=4→E
I=8 → E	B=1	V=1
R=6 → E	M=4→E	
G=2	K=2	

lletra	A	B	C	Ç	D	E	F	G	H	I	J	K	L	M
%	12,55	1,32	3,60	1,06	3,94	13,89	1	1,28	0,72	6,99	0,3	0	7,74	3,16
lletra	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
%	6,40	5,71	2,72	1,35	6,76	8,43	6,11	4,18	1,4	0	0,52	0	0,01	

Segona lletra:

TLLPDLQPLOOSZTCYLTPXALZILTYPYZDZYNDPXDDYDZEYZZWZONEYPPWE

T=4→E	S=1	I=1
L=7 →E	Z=8→ E	N=2
P=7 →E	C=1	E=3→E
D=6 →E	Y=7→ E	W=2
Q=1	X=2	
O=3→E	A=1	

lletra	A	B	C	Ç	D	E	F	G	H	I	J	K	L	M
%	12,55	1,32	3,60	1,06	3,94	13,89	1	1,28	0,72	6,99	0,3	0	7,74	3,16
lletra	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
%	6,40	5,71	2,72	1,35	6,76	8,43	6,11	4,18	1,4	0	0,52	0	0,01	

Tercera lletra:

PMHWHHMWXIISRBEIVMWFWURLPKXRGGJXWWUQYIWKXPIXPRTRIEVSWMX

P=4→ E
M=4→ E
H=3 → E
W=8→E
X=6 →E
I=6 → E
S=2→ E

R=5→ E
B=1
E=2→ E
V=2→ E
F=1
U=2→ E
L=1

G=2→ E
J=1
Q=1
Y=1
T=1
K=2→ E

lletra	A	B	C	Ç	D	E	F	G	H	I	J	K	L	M
%	12,55	1,32	3,60	1,06	3,94	13,89	1	1,28	0,72	6,99	0,3	0	7,74	3,16
lletra	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
%	6,40	5,71	2,72	1,35	6,76	8,43	6,11	4,18	1,4	0	0,52	0	0,01	

Quarta lletra:

VXKDOYLOKXVWCMBHPODOCECSQXOMOKSOMKELXKOOYDXOCCBSXEYBBHC

V=2
X=6 →E
K=5 → E
D=3→ E
O=10→E
Y=3→ E

L=2
W=1
C=6→E
M=3 → E
B=4→ E
H=2

P=1
E=3→ E
S=3→ E
Q=1

lletra	A	B	C	Ç	D	E	F	G	H	I	J	K	L	M
%	12,55	1,32	3,60	1,06	3,94	13,89	1	1,28	0,72	6,99	0,3	0	7,74	3,16
lletra	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
%	6,40	5,71	2,72	1,35	6,76	8,43	6,11	4,18	1,4	0	0,52	0	0,01	

Cinquena lletra:

TYWKIKBFJBLXXTOXXEBETXMUNXEBKLGFTFYEBFNGMTMEWMHLMGGLXXH

T=5→E
Y=2
W=2
K=3 → E
I=1
B=5 → E
F=4→ E
J=1
L=4→ E
X=8→E
O=1
E=5 → E
M=5→ E
U=1
N=2
G=4→ E
H=2

lletra	A	B	C	Ç	D	E	F	G	H	I	J	K	L	M
%	12,55	1,32	3,60	1,06	3,94	13,89	1	1,28	0,72	6,99	0,3	0	7,74	3,16
lletra	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
%	6,40	5,71	2,72	1,35	6,76	8,43	6,11	4,18	1,4	0	0,52	0	0,01	

Sisena lletra:

VVLRIJJGLKUJXGZDDUTKUVIVEJCRKZJVESCRTSJVVERJVIKKZJJHGEM

V=8→E
L=2
R=4→ E
I=3→ E
J=9 →E
G=3→ E
K=5→ E
U=3→ E
X=1
Z=3→ E
D=2
T=2
E=4 → E
C=2
S=2
M=1
H=1

lletra	A	B	C	Ç	D	E	F	G	H	I	J	K	L	M
%	12,55	1,32	3,60	1,06	3,94	13,89	1	1,28	0,72	6,99	0,3	0	7,74	3,16
lletra	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
%	6,40	5,71	2,72	1,35	6,76	8,43	6,11	4,18	1,4	0	0,52	0	0,01	

Setena lletra:

SSNNEAQREUOAUTUPEOAEOLEISDIIEOITTESCAECRSTMULEAAFPSUEMI

S=6 →E	U=5→E	D=1
N=2	O=4 → E	C=2
E=10→E	T=4 → E	M=2
A=6 → E	P=2	F=1
Q=1	L=2	
R=2	I=5 →E	

lletra	A	B	C	Ç	D	E	F	G	H	I	J	K	L	M
%	12,55	1,32	3,60	1,06	3,94	13,89	1	1,28	0,72	6,99	0,3	0	7,74	3,16
lletra	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
%	6,40	5,71	2,72	1,35	6,76	8,43	6,11	4,18	1,4	0	0,52	0	0,01	

Ara tinc detectades quines són de cada grup les possibles lletres E, pel que, ara amb la taula de Vigènere hauria de veure quin moviment s'ha fet amb cada lletra per tal d'esbrinar

la paraula clau. Agafaré la columna de la E i buscaré quina lletra de la clau hauria de ser,

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

de fet és com jugar a vaixells i acaba essent entretingut.

Primera lletra:

Si la I és la lletra E, voldria dir de la taula que la primera lletra de la paraula clau seria una

D

Segona lletra:

Si la Z és la lletra E, voldria dir de la taula que la primera lletra de la paraula clau seria una

U

Tercera lletra:

Si la W és la lletra E, voldria dir de la taula que la primera lletra de la paraula clau seria una **R**

Quarta lletra:

Si la O és la lletra E, voldria dir de la taula que la primera lletra de la paraula clau seria una **J**

Cinquena lletra:

Si la X és la lletra E, voldria dir de la taula que la primera lletra de la paraula clau seria una **S**

Sisena lletra:

Si la J és la lletra E, voldria dir de la taula que la primera lletra de la paraula clau seria una **E**

Si la V és la lletra E, voldria dir de la taula que la primera lletra de la paraula clau seria una **Q**

Setena lletra:

Si la E és la lletra E, voldria dir de la taula que la primera lletra de la paraula clau seria una **A**

M'acaba de sortir que la paraula clau seria:

DURJSEA

DURJSQA

Que no té massa sentit...

Com que per la taula de freqüències entre la E i la A no hi ha molta distància, miraré què passaria si en comptes de E les que hem trobat fossin A.... i potser serà una combinació de les dues.

Si la que més surt és una A, vol dir que no hi ha moviment de lletres, és a dir, la A sempre coincideix amb la paraula clau, per tant en el cas que la que més surt fos una A la paraula clau hauria de ser:

IZWOXJE

Que tampoc té molt de sentit...

Com que no ens ha sortit res coherent, podria ser que el que ha codificat el text hagués agafat una taula de Vigènere sense la Ç, o sigui que faré ara la prova amb una nova taula de Vigènere:

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Primera lletra:

Si la I és la lletra E, voldria dir de la taula que la primera lletra de la paraula clau seria una **E**

Segona lletra:

Si la Z és la lletra E, voldria dir de la taula que la primera lletra de la paraula clau seria una **V**

Tercera lletra:

Si la W és la lletra E, voldria dir de la taula que la primera lletra de la paraula clau seria una **S**

Quarta lletra:

Si la O és la lletra E, voldria dir de la taula que la primera lletra de la paraula clau seria una **K**

Cinquena lletra:

Si la X és la lletra E, voldria dir de la taula que la primera lletra de la paraula clau seria una **T**

Sisena lletra:

Si la J és la lletra E, voldria dir de la taula que la primera lletra de la paraula clau seria una **F**

Si la V és la lletra E, voldria dir de la taula que la primera lletra de la paraula clau seria una **R**

Setena lletra:

Si la E és la lletra E, voldria dir de la taula que la primera lletra de la paraula clau seria una **A**

M’acaba de sortir que la paraula clau seria:

EVSKTFA

EVSKTRA

Que tampoc te molt de sentit...

Com que les lletres que tenen més freqüència de sortir sempre son primer la E i després la A, miraré totes les lletres que més surten, si una és la E si n´hi ha alguna altra que pugui ser la A (ha de ser una altra de les que estan a la columna). Per a fer-ho es aquí on aprofito que al principi he marcat com a possibles E totes les lletres que més surten i les he diferenciat en colors per a valorar la freqüència.

De fet en les taules de sota podem veure dos grups de lletres, el primer en negre són les que vaig valorar de inici, però com que no em sortia res amb sentit, vaig afegir en blau clar totes les possibles lletres per a ampliar la cerca (això sortirà més endavant)

1a lletra:

	Amb ç	Sense ç
I		A
R	E; A	A
W	E; A	E
Q	A	E
P		
X	E; A	A
Y		A
M	A	A E
S	A	A
E		
G	E	E; A
H		
K		E
C	A; E	A; E

B	E	E
V	E	E

2a lletra:

	Amb ç	Sense ç
Z	A	A
L		A
P		E; A
Y	E	A
D	E; A	E
T	A	E; A
O		O
E	A	A
X	E; A	E
N	E; A	
W		E; A
Q	E	
S	A; E	A; E
C	E	E
A		E
I	A; E	E

3a lletra:

	Amb ç	Sense ç
W	E; A	
X		A
I		A
R	A, E	A
P	A	A
M	A, E	E; A

H	A	A
S		
E	A	
V		E
U	E	A
G	A	A
K		E
B	E; A	E; A
F	E	E; A
L	E; A	E
J	E	E
Q	E	E
Y	E	E
T	A	E

4a lletra:

	Amb ç	Sense ç
O		E, A
X	A	A
C	E	
K	A; A	A
B	E	E
D		A
Y		
M		A
E		
S		E; A
V	E	
L	A	E; A
H		A; E

W		E
P	E	E
Q	A; E	E

5a lletra:

	Amb ç	Sense ç
X		A; A
T	A	E
B	A	E,A
E	A	A
M		
G	A	A
F	E, A	E; A
L	E	
K	E	E; A
Y	E	E
W		
N	E	E
H		
I	A	E
J	E; A	A; E
O	E	E
U		A

6a lletra:

	Amb ç	Sense ç
J	E	
V		E, A
K		E

E	A	A
R		A
I		E; A
G	A	A
U	A	
Z	E; A	E; A
L	E	E
D	E	E; A
T		A
C	E	
S	A	
X	A; E	E
M	E	E
H	A	A; E

7a lletra:

	Amb ç	Sense ç
E	E	E, A
S		E
A	A	A
U		
I	A	E; A
O	A	A
T	E	
N	E	A
R	E	E
P		E
L	A	A
C		

M	A	E; A
Q	E	E
D		
F		

Ara faig un quadre amb les A, que són les possibles lletres de la paraula clau, que trobo en funció de quina és la lletra E. Les ordenaré de més freqüència a menys (tal com estan fetes les taules anteriors) per llavors buscar combinacions que em puguin donar paraules clau.

	Amb ç	**Sense ç**
Primera lletra	R-M-S-W-Q-X-C	I-M-S-R-X-Y-G-C
Segona lletra	Z-T-D-E-X-N-S-I	Z-L-P-Y-T-E-W-S
Tercera lletra	R-M-H-P-W-E-G-B-L-T	I-G-R-X-P-M-H-U-B-F
Quarta lletra	X-K-L-Q	X-K-O-D-M-S-L-H
Cinquena lletra	B-G-T-E-F-I-J	X-B-E-G-F-K-J
Sisena lletra	E-U-G-Z-S-X-H	V-E-R-G-I-Z-D-T-H
Setena lletra	A-O-I-L-M	E-A-O-I-N-M-L

NO SÓC CAPAÇ DE TROBAR CAP PARAULA QUE TINGUI SENTIT.

Vist que no sóc capaç de trobar cap paraula amb sentit, el que faré serà acabar de posar totes les lletres possibles que em surten que podrien ser la A (agafant totes les de cada grup independentment del número de vegades que surtin), són totes les lletres que estan en color blau.

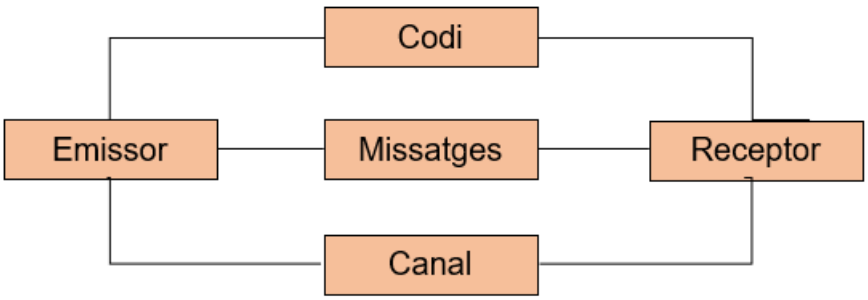
Ara agafant totes les lletres em surten tantes possibles combinacions que tampoc sóc capaç de trobar-ne cap que tingui sentit.

5. CONCLUSIONS

Com deia en la introducció, em vaig plantejar aquest treball amb diversos objectius, per una banda, volia entendre què és la criptografia i veure com i perquè s'havia originat; per una altra banda, volia entendre com funcionava i s'aplicava per poder-ne valorar la seva complexitat i fiabilitat, i, perquè no, volia aprendre a fer missatges encriptats i a desencriptar-los.

En la part teòrica he après moltes coses:

- La criptografia no és, al contrari del que em pensava, una invenció moderna dels WhatsApp o de fa un parell de segles de les guerres com em deien els més grans. La criptografia ha existit des de sempre doncs no és més que una variant de la comunicació. La criptografia és una comunicació en la qual el Codi és només conegut per l'Emissor i el Receptor.



  Per exemple, he après que podem considerar com a criptografia els jeroglífics que utilitzaven els egipcis, doncs els missatges que es trametien entre ells complien totes les característiques de la criptografia (un codi que només emissor i receptor saben), i de fet hi ha missatges que encara avui dia no s'han desxifrat.

- També he après que la Criptografia és una ciència, que no és quelcom abstracte, sinó que com que es vol trametre un missatge i es vol que el receptor sigui capaç de llegir-lo, el que fan tots els mètodes és alterar l'ordre de les lletres o canviar les lletres per unes altres tot seguint unes regles (que després el receptor ha de seguir a la inversa per a desxifrar el missatge).

- Aquestes regles han anat variant al llarg de la història per a fer-les més complexes, i sobretot, més segures (com em plantejava en la meva hipòtesi). Això ha configurat els diferents mètodes d'encriptat, però tots ells tenen en comú que hi ha un procediment que un cop el descobreixes és fàcilment reversible. I que ha de ser-ho perquè si no el receptor no podria desxifrar el missatge.

- Hi ha mètodes (sobretot els més antics i simples) que només es basen substituir unes lletres per unes altres seguint una certa lògica, i que això fa que a l'hora de desxifrar el codi sigui relativament senzill, mentre que hi ha altres mètodes més sofisticats en què aquesta substitució es fa d'acord amb un altre codi que només saben l'emissor i el receptor, i que això fa que sigui molt més complicat poder-lo desxifrar (un cop més es va verificant la meva hipòtesi).

- Si aquest segon codi és un mitjà mecànic (màquina enigma, escítala...) es fa molt més difícil d'interceptar el missatge si no tens el mitjà, per tant, és més segur.

En la part pràctica he descobert que si bé encriptar és relativament fàcil, a l'hora de desxifrar es necessiten moltes hores, moltes proves o un equip de moltes persones, o segurament (tot i que no hi he tingut accés) un ordinador amb un bon programa de desencriptació (he anat verificant la meva hipòtesi).

Desxifrant el primer text he après que cada llengua té una taula amb les freqüències de les diferents lletres i que, si estàs desxifrant un text que ha estat encriptat mitjançant la substitució, és una bona eina per poder començar a substituir. També, un punt en contra de la fiabilitat de la criptografia és que, si en el text xifrat s'hi mantenen els espais, la feina de desencriptar és menor que si han estat suprimits, ja que amb espais ràpidament es poden intuir paraules gràcies a la capacitat que tenim de llegir paraules encara que els hi faltin lletres.

A l'hora de desxifrar el segon text he trobat a faltar els espais, ja que anava substituint però no arribava a cap idea lògica. És per això que, si el que es vol fer és encriptar un text i que sigui molt difícil de desencriptar és recomanable treure-hi els espais. Però no és del tot

fiable, ja que al cap d'hores de fer proves s'ha pogut arribar al missatge original. Sense la necessitat d'un ordinador amb el qual hauria estat segurament cosa de segons.

Finalment, penso que en l'exercici 3 el que m'he trobat és que estic ja davant una codificació molt complicada, i a la que veig tres principals punts:

En dividir en frases petites (a causa de la paraula clau), com que tinc moltes menys lletres fa que l'anàlisi de freqüències potser no és prou acurat, i per això no em quadra.
També pot ser que en fer la separació manualment i al analitzar-lo m'hagi embolicat, a més tenint en compte que no sé si la taula de Vigènere és amb Ç o sense Ç, de fet no sé ni quina ha fet servir (igual en la que ha utilitzat hi ha la Ç, la L·L...) i tot plegat pot ajudar que no trobi res amb sentit.
En el tercer punt en què com que no trobava res amb sentit he posat totes les lletres, hi ha moltíssimes combinacions possibles que no sóc capaç d'analitzar, segurament amb un ordinador es podria i seria relativament fàcil, però jo no me n'he sortit.

Per tant, i com a conclusió d'aquest tercer exercici jo diria que es demostra perfectament la meva hipòtesi que l'encriptació ha anat evolucionant a mesura que la gent ha anat trobant maneres de desencriptar, fins al punt que manualment ja sigui impossible resoldre-ho i es necessitin altres mitjans... Que és el que passa amb les encriptacions modernes que ja es fan amb ordinadors i òbviament només es poden resoldre amb ordinadors...

Conclusió Final:

La conclusió final és que la meva hipòtesi que ***la criptografia ha anat evolucionant amb mètodes cada cop més complexos a mesura que s'han anat trobant maneres de desencriptar-los, i que al final arriba un moment que si no tens ajudes (siguin màquines, ordinadors, pistes...) ja no pots desencriptar-los*** és del tot certa.

La criptografia ha existit des de sempre, inicialment era més senzill, i avui en dia amb les capacitats dels ordinadors moderns és molt més complexa i per tant molt més segura.

Els mètodes tradicionals de criptografia basats en substitució poden ser resolts fins i tot manualment, però quan introduïm codis més complexos o múltiples, llavors sense l'ajuda d'un ordinador és impossible, i segurament fins i tot amb ella hi ha encriptats que no es poden desxifrar, o almenys això ens pensem quan ens atrevim a pagar amb la targeta de crèdit, a fer compres per internet, a enviar missatges de WhatsApp.

6. EPÍLEG

En el moment que se'm va plantejar fer el treball de recerca sobre la criptografia em van sorgir molts dubtes, ja que, la veritat, tenia un desconeixement total de la criptografia: m'agradarà fer aquest treball? Aprendré alguna cosa? M'agraden les matemàtiques, hi tindrà relació? Què em suposarà la part pràctica del TdR?

Al principi era tot molt abstracte i em va costar enfocar el tema. A mesura que vaig anar recopilant informació, gràcies a la meva tutora i a en David Juher es va anar clarificant en què consistia la criptografia. A banda de la informació general, entrar a desxifrar textos encriptats m'ha ajudat a entendre la teoria i alhora m'ha suposat un repte a aconseguir. Hi he dedicat moltes hores, algun moment m'hi he desesperat però, he après que és molt reconfortant quan ho aconsegueixes i també he après que no aconseguir-ho és part de la criptografia.

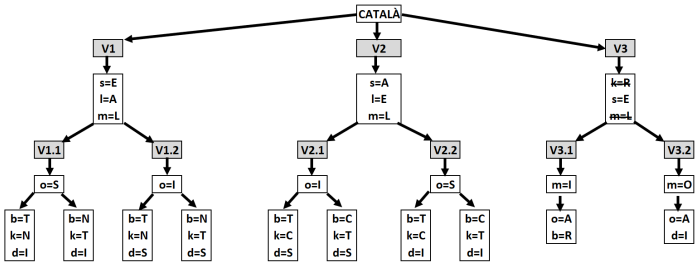
7. AGRAÏMENTS

Agraeixo a David Juher la idea de la part pràctica. Donar-li les gràcies per passar-me els tres textos xifrats i per deixar-me assistir a una conferència que va fer per professors de batxillerat.

Finalment, també agrair als meus pares pel suport i implicació que m'han estat donant durant la realització d'aquest treball.

8. APÈNDIX

8.1 Primer intent de desencriptació del text 2 (versió 1.1)



TEXT 2: El segon text és un altre text xifrat utilitzant la substitució, amb la diferència que en aquest no s'han mantingut els espais, per tant, és un xic més complicat. Igual que en el primer text, no sé en quin idioma està escrit l'original, tampoc sé la seva procedència ni la seva destinació.

gAjeAtdbdadcpbgjcaAedyAboAkoAnlbcnjltdaAklhpALLhpAlacbkAnpAdwcapLoljtdkdalyAboA
LydkklonAolglboLcctAboLcdbqdkdELAocodhpAALydkklonAacylolLAkgjAkAboAblLnpbLLcad
kdklEAycbklylnlcdbqAjodyALgjcaAedyAboecapLoladcklEjAylaaAedjlLoAwodLLAndjLcdAboA
bejAygAjtAaolyAbolLLchpAkfdedplhpAkoAkoAabdhpAkeAalyptLlonAkflbpodLdozlolLL
LljneAocolLlfdkocjdl

En ser un text xifrat de la mateixa manera que el text 1, però amb la diferència dels espais, seguirem els mateixos passos, és a dir, començarem per determinar el nombre de cada lletra, per així ordenar-les de més freqüents a menys:

s (46)	k (21)	p (14)	t (6)
l (32)	c (20)	y (13)	h (6)
d (31)	b (20)	n (10)	w (2)
o (29)	a (16)	e (9)	z (1)
m (26)	j (14)	g (6)	

Ara ja tenim totes les lletres comptades i ordenades. Ja podem començar a substituir. Primer de tot agafarem la taula de freqüències de la llengua catalana, ja que, com que el primer text també me'l va passar en David Juher i estava escrit en català, penso que aquest podria estar també en català.

lletra	A	B	C	Ç	D	E	F	G	H	I	J	K	L	M
%	12,55	1,32	3,60	1,06	3,94	13,89	1	1,28	0,72	6,99	0,3	0	7,74	3,16
lletra	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
%	6,40	5,71	2,72	1,35	6,76	8,43	6,11	4,18	1,4	0	0,52	0	0,01	

s (46) ~ E	k (21) ~ R	p (14) ~ D	t (6) ~ Q
l (32) ~ A	c (20) ~ N	y (13) ~ C	h (6) ~ B
d (31) ~ S	b (20) ~ T	n (10) ~ M	w (2) ~ G
o (29) ~ L	a (16) ~ O	e (9) ~ P	z (1) ~ Ç
m (26) ~ I	j (14) ~ U	g (6) ~ V	

Amb la taula podríem suposar que la S codifica per la lletra E i la L per la lletra A.

s (46) = E	k (21)	p (14)	t (6)
l (32) = A	c (20)	y (13)	h (6)
d (31)	b (20)	n (10)	w (2)
o (29)	a (16)	e (9)	z (1)
m (26)	j (14)	g (6)	

gEjeEtdbdadcpbgjcaEedyEboEkoEnAbcnjAtdaEkAhpEmmhpEAacbkEnpEdwcapmoAjtdkdaAyE
boEmydkkAonEoAgAbomcctEbomcdbqdkdimEocodhpEEmydkkAonEacyAoAmEkgjEkEboEbA
mnpbmmcadkdkAiEycbkAyAnAcdbqEjodyEmgjcaEedyEboecapmoAadckAijEyAaaEedjAmoEwo
dmmEndjmcdEboEbejEygEjtEaoAyEboAmmchpEkfdedpAhpEkoEkoEabdhpEkeEaAyptmAonEk
fAbpodmdozAoAmmmAjneEocoAmAfdkocjdA

Amb aquesta substitució, si és que hem encertat l'idioma i és Català, ja podem intuir alguns espais, ja que, en català, dues E no van mai juntes.

gEjeEtdbdadcpbgjcaEedyEboEkoEnAbcnjAtdaEkAhpEmmhpEAacbkEnpEdwcapmoAjtdkdaAyE
boEmydkkAonEoAgAbomcctEbomcdbqdkdimEocodhpE
EmydkkAonEacyAoAmEkgjEkEboEbAmnpbmmcadkdkAiEycbkAyAnAcdbqEjodyEmgjcaEedyE
boecapmoAadckAijEyAaaEedjAmoEwodmmEndjmcdEboEbejEygEjtEaoAyEboAmmchpEkfdedp
AhpEkoEkoEabdhpEkeEaAyptmAonEkfAbpodmdozAoAmmmAjneEocoAmAfdkocjdA

En català només existeixen les ss, rr, ll, mm, nn, però mai n'hi ha de 3, per tant, significa que han d'anar separades i que dues de seguides seran a inici o final de paraula, les quals de parelles que hi poden anar només n'hi ha una, la LL. Així doncs, substituirem la M per la L.

s (46) = E	k (21)	p (14)	t (6)
l (33) = A	c (20)	y (13)	h (6)
d (31)	b (20)	n (10)	w (2)
o (29)	a (16)	e (9)	z (1)
m (26) = L	j (14)	g (6)	

gEjeEtdbdadcpbgjcaEedyEboEkoEnAbcnjAtdaEkAhpELLhpEAacbkEnpEdwcapLoAjtdkdaAyEbo
ELydkkAonEoAgAboLcctEboLcdbqdkdiLEocodhpE
ELydkkAonEacyAoALEkgjEkEboEbALnpbLLcadkdkAiEycbkAyAnAcdbqEjodyELgjcaEedyEboe
capLoAadckAijEyAaaEedjALoEwodLLEndjLcdEboEbejEygEjtEaoAyEboALLchpEkfdedpAhpEko
EkoEabdhpEkeEaAyptLAonEkfAbpodLdozAoALL
LAjneEocoALAfdkocjdA

El següent pas a seguir és buscar conjunt de lletres repetides per tal de poder imaginar quina paraula potser. Per exemple, el conjunt Eko es repeteix 3 vegades; Ebo, 6 vegades i ELydkkAonE, dues vegades, el qual pot ser una paraula o dues, sense espais és complicat. Ara mateix no sé per on tirar, no em venen paraules que puguin funcionar en aquest text ni lletres que vagin bé a Ebo o Eko. El que sí que m'he adonat és que necessito saber quina lletra és codificada per la O, ja que surt moltes vegades i potser si la pogués substituir, trobaria més lletres.

Substituirem la O guiant-nos per la taula de freqüències, i penso que podria ser la S o la I, així que ho substituiré amb les dues per veure quina hi va millor.

s (46) = E	k (21)	p (14)	t (6)
l (32) = A	c (20)	y (13)	h (6)
d (31)	b (20)	n (10)	w (2)
o (29) = S	a (16)	e (9)	z (1)
m (26) = L	j (14)	g (6)	

gEjeEtdbdadcpbgjcaEedyEbSEkSEnAbcnjAtdaEkAhpELLhpEAacbkEnpEdwcapLSAjtdkdaAyEbS
ELydkkASnESAgAbSLcctEbSLcdbqdkdiLEScSdhpE
ELydkkASnEacyASALEkgjEkEbSEbALnpbLLcadkdkAiEycbkAyAnAcdbqEjSdyELgjcaEedyEbSe
capLSAadckAijEyAaaEedjALSEwSdLLEndjLcdEbSEbejEygEjtEaSAyEbSALLchpEkfdedpAhpEkS
EkSEabdhpEkeEaAyptLASnEkfAbpSdLdSzASALL
LAjneEScSALAfdkScjdA

Amb la substitució de la lletra S, podem pensar que EbS i EkS són ETS, ELS O ENS, però com que la L ja la tenim substituïda, ja descartem el ELS. Llavors falta saber si la B codifica per la T o és la K la que codifica per la T, per tant ho provarem en els dos casos: en la versió en blau substituirem la B per la T, i en la versió en verd la K serà canviada per la T:

En aquest cas provarem que la B codifica per la T i la K per la N.

s (46) = E	d (31)	m (26) = L	c (20)
l (32) = A	o (29) = S	k (21) = N	b (20) = T

a (16)	y (13)	g (6)	w (2)
j (14)	n (10)	t (6)	z (1)
p (14)	e (9)	h (6)	

gEjeEtdTdadcpTgjcaEedyET SENSEnATcnjAtdaENAhpELLhpEAacTNEnpEdwcapLSAjtdNdaAy
ETS ELydN NASnESAgATSLcctETSLcdTqdNdiLEScSdhpE
ELydNNASnEacyASALENgjENETSETALnpTLLcadNdNAiEycTNAyAnAcdTqEjSdyELgjcaEedyE
TSecapLSAadcNAijEyAaaEedjALSEwSdLLEndjLcdETSETejEygEjtEaSAyETSALLchpENfdedpAh
pEN SENSEaTdhp EN eEaAyptLASn EN fATpSdLdSzASALL
Lajne Esc SALAfdNScjdA

Amb les poques lletres que tenim desxifrades i els pocs espais podem començar a deduir algunes paraules, com per exemple, SENSE.

gEjeEtdTdadcpTgjcaEedyET SENSE
nATcnjAtdaENAhpELLhpEAacTNEnpEdwcapLSAjtdNdaAyETSELydNNASnESAgATSLcctETSL
cdTqdNdiLEScSdhpE
ELydNNASnEacyASALENgjENETSETALnpTLLcadNdNAiEycTNAyAnAcdTqEjSdyELgjcaEedyE
TSecapLSAadcNAijEyAaaEedjALSEwSdLLEndjLcdETSETejEygEjtEaSAyETSALLchpENfdedpAh
pEN SENSE aTdhpENeEaAyptLASnENfATpSdLdSzASALL
LAjneEScSALAfdNScjdA

Com que hem deixat la D pel mig, i de D en tenim 31, anem a veure per freqüències què podria ser la d. Segons la taula de freqüències li tocaria la S, però com que ja hem suposat que era la o, agafarem la que estigui més propera, la d hauria de ser o bé una L o una I. Com que la L ja l'hem feta servir anirem per la I.

s (46) = E	k (21) = N	p (14)	t (6)
l (32) = A	c (20)	y (13)	h (6)
d (31) = I	b (20) = T	n (10)	w (2)
o (29) = S	a (16)	e (9)	z (1)
m (26) = L	j (14)	g (6)	

gEjeEtITIaIcpTgjcaEeIy ETS EN SE nATcnjAtIa EN Ahp ELL hpEAacTNEnpEIwcapLSAjtINIaAy ETS EL yINNASnE SAgATSLcct ETS LcITqINIiLEScSIhpE
EL yINNASnE acyASALENgjEN ETS ETALnpT LLcaININAiEycTNAyAnAcITqEjSIyELgjcaEeIy ETS ecapLSAaIcNAijEyAaaEeIjALSEwSILLEnIjLcI ETS EtejEygEjtEaSAy ETS ALLchpENfIeIpAhpEN SENSE aTIhpENeEaAyptLASnENfATpSILISzASALL LAjneEScSALAfINScjIA

Anem a provar ara al revés, que la B codifica per la N i la K codifica per la T

gEjeEtdNdadcpNgjcaEedyENSETSEnANcnjAtdaETAhpELLhpEAacNTEnpEdwcapLSAjtdTdaAy ENSELydTTASnESAgANSLcctENSLcdNqdTdiLEScSdhpE
ELydTTASnEacyASALETgjETENSENALnpNLLcadTdTAiEycNTAyAnAcdNqEjSdyELgjcaEedyE NSecapLSAadcTAijEyAaaEedjALSEwSdLLEndjLcdENSENejEygEjtEaSAyENSALLchpETfdedpAh pETSETSEaNdhpETeEaAyptLASnETfANpSdLdS zASAL
LLAjneEScSALAfdTScjdA

Com que hem deixat la D pel mig, i de D en tenim 31, anem a veure per freqüències què podria ser la d. Segons la taula de freqüències li tocaria la S, però com que ja hem suposat que era la o, agafarem la que estigui més propera, la d hauria de ser o bé una L o una I. Com que la L ja l'hem feta servir anirem per la I.

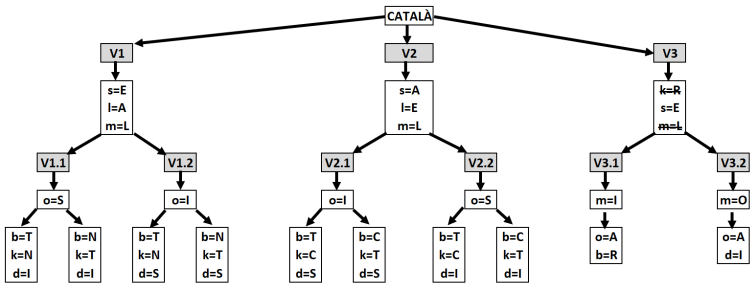
s (46) = E	k (21) = T	p (14)	t (6)
l (32) = A	c (20)	y (13)	h (6)
d (31) = I	b (20) = N	n (10)	w (2)
o (29) = S	a (16)	e (9)	z (1)
m (26) = L	j (14)	g (6)	

gEjeEtINIaIcpNgjcaEeIyENSETSEnANcnjAtIaETAhpELLhpEAacNTEnpEIwcapLSAjtITIaAyENS
ELyITTASnESAgANSLcctENSLcINqITIiLEScSIhpE
ELyITTASnEacyASALETgjETENSENALnpNLLcaITITAiEycNTAyAnAcINqEjSIyELgjcaEeIyENS
ecapLSAaIcTAijEyAaaEeIjALSEwSILLEnIjLcIENSENejEygEjtEaSAyENSALLchpETfIeIpAhpETS
ETSEaNIhpETeEaAyptLASnETfANpSILIS zAS AL LLAjneEScSALAfITScjIA

Veig una possible paraula amb zASAL, que podria ser CASAL, BASAL o NASAL, però la N ja l'he agafat, i la C i la B tenen freqüències.

Ho deixem aquí, perquè no veig que pugui arribar enlloc per aquest camí

8.2 Segon intent de desencriptació del text 2 (versió 1.2)



TEXT 2: El segon text és un altre text xifrat utilitzant la substitució, amb la diferència que en aquest no s'han mantingut els espais, per tant, és un xic més complicat. Igual que en el primer text, no sé en quin idioma està escrit l'original, tampoc sé la seva procedència ni la seva destinació.

En ser un text xifrat de la mateixa manera que el text 1, però amb la diferència dels espais, seguirem els mateixos passos, és a dir, començarem per determinar el nombre de cada lletra, per així ordenar-les de més freqüents a menys:

gAjeAtdbdadcpbgjcaAedyAboAkoAnlbcnjltdaAklhpALLhpAlacbkAnpAdwcapLoljtdkdalyAboA
LydkklonAolglboLcctAboLcdbqdkdELAocodhpAALydkklonAacylolLAkgjAkAboAblLnpbLLcad
kdklEAycbklylnlcdbqAjodyALgjcaAedyAboecapLoladcklEjAylaaAedjlLoAwodLLAndjLcdAboA
bejAygAjtAaolyAbolLLchpAkfdedplhpAkoAkoAabdhpAkeAalyptLlonAkflbpodLdozlolLL
LljneAocolLlfdkocjdl

s (46)	k (21)	p (14)	t (6)
l (32)	c (20)	y (13)	h (6)
d (31)	b (20)	n (10)	w (2)
o (29)	a (16)	e (9)	z (1)
m (26)	j (14)	g (6)	

Ara ja tenim totes les lletres comptades i ordenades. Ja podem començar a substituir. Primer de tot agafarem la taula de freqüències de la llengua catalana, ja que, com que el primer text també me'l va passar en David Juher i estava escrit en català, penso que aquest podria estar també en català.

lletra	A	B	C	Ç	D	E	F	G	H	I	J	K	L	M
%	12,55	1,32	3,60	1,06	3,94	13,89	1	1,28	0,72	6,99	0,3	0	7,74	3,16
lletra	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
%	6,40	5,71	2,72	1,35	6,76	8,43	6,11	4,18	1,4	0	0,52	0	0,01	

s (46) ~ E	k (21) ~ R	p (14) ~ D	t (6) ~ Q
l (32) ~ A	c (20) ~ N	y (13) ~ C	h (6) ~ B
d (31) ~ S	b (20) ~ T	n (10) ~ M	w (2) ~ G
o (29) ~ L	a (16) ~ O	e (9) ~ P	z (1) ~ Ç
m (26) ~ I	j (14) ~ U	g (6) ~ V	

Amb la taula podríem suposar que la S codifica per la lletra E i la L per la lletra A.

s (46) = E	k (21)	p (14)	t (6)
l (32) = A	c (20)	y (13)	h (6)
d (31)	b (20)	n (10)	w (2)
o (29)	a (16)	e (9)	z (1)
m (26)	j (14)	g (6)	

gEjeEtdbdadcpbgjcaEedyEboEkoEnAbcnjAtdaEkAhpEmmhpEAacbkEnpEdwcapmoAjtdkdaAyE
boEmydkkAonEoAgAbomcctEbomcdbqdkdimEocodhpEEmydkkAonEacyAoAmEkgjEkEboEbA
mnpbmmcadkdkAiEycbkAyAnAcdbqEjodyEmgjcaEedyEboecapmoAadckAijEyAaaEedjAmoEwo
dmmEndjmcdEboEbejEygEjtEaoAyEboAmmchpEkfdedpAhpEkoEkoEabdhpEkeEaAyptmAonEk
fAbpodmdozAoAmmmAjneEocoAmAfdkocjdA

Amb aquesta substitució, si és que hem encertat l'idioma i és Català, ja podem intuir alguns espais, ja que, en català, dues E no van mai juntes.

gEjeEtdbdadcpbgjcaEedyEboEkoEnAbcnjAtdaEkAhpEmmhpEAacbkEnpEdwcapmoAjtdkdaAyE
boEmydkkAonEoAgAbomcctEbomcdbqdkdimEocodhpE
EmydkkAonEacyAoAmEkgjEkEboEbAmnpbmmcadkdkAiEycbkAyAnAcdbqEjodyEmgjcaEedyE
boecapmoAadckAijEyAaaEedjAmoEwodmmEndjmcdEboEbejEygEjtEaoAyEboAmmchpEkfdedp
AhpEkoEkoEabdhpEkeEaAyptmAonEkfAbpodmdozAoAmmmAjneEocoAmAfdkocjdA

En català només existeixen les ss, rr, ll, mm, nn, però mai n'hi ha de 3, per tant, significa que han d'anar separades i que dues de seguides seran a inici o final de paraula, les quals de parelles que hi poden anar només n'hi ha una, la LL. Així doncs, substituirem la M per la L.

gEjeEtdbdadcpbgjcaEedyEboEkoEnAbcnjAtdaEkAhpELLhpEAacbkEnpEdwcapLoAjtdkdaAyEbo
ELydkkAonEoAgAboLcctEboLcdbqdkdiLEocodhpE
ELydkkAonEacyAoALEkgjEkEboEbALnpbLLcadkdkAiEycbkAyAnAcdbqEjodyELgjcaEedyEboe
capLoAadckAijEyAaaEedjALoEwodLLEndjLcdEboEbejEygEjtEaoAyEboALLchpEkfdedpAhpEko
EkoEabdhpEkeEaAyptLAonEkfAbpodLdozAoALL
LAjneEocoALAfdkocjdA

s (46) = E	k (21)	p (14)	t (6)
l (33) = A	c (20)	y (13)	h (6)
d (31)	b (20)	n (10)	w (2)
o (29)	a (16)	e (9)	z (1)
m (26) = L	j (14)	g (6)	

El següent pas a seguir és buscar conjunt de lletres repetides per tal de poder imaginar quina paraula potser. Per exemple, el conjunt Eko es repeteix 3 vegades; Ebo, 6 vegades i ELydkkAonE, dues vegades, el qual pot ser una paraula o dues, sense espais és complicat. Ara mateix no sé per on tirar, no em venen paraules que puguin funcionar en aquest text ni lletres que vagin bé a Ebo o Eko. El que sí que m'he adonat és que necessito saber quina lletra és codificada per la O, ja que surt moltes vegades i potser si la sé, podré substituir més lletres.

Substituirem la O guiant-nos per la taula de freqüències, i penso que podria ser la S o la I, així que ho substituiré amb les dues per veure quina hi va millor. FEM LA o=I

s (46) = E	d (31)	m (26) = L	c (20)
l (32) = A	o (29) = I	k (21)	b (20)

a (16)	y (13)	g (6)	w (2)
j (14)	n (10)	t (6)	z (1)
p (14)	e (9)	h (6)	

gEjeEtdbdadcpbgjcaEedyEblEkIEnAbcnjAtdaEkAhpELLhpEAacbkEnpEdwcapLIAjtdkdaAyEblE
LydkkAInEIAgAbILcctEblLcdbqdkdiLEIcIdhpE
ELydkkAInEacyAIALEkgjEkEblEbALnpbLLcadkdkAiEycbkAyAnAcdbqEjIdyELgjcaEedyEbleca
pLIAadckAijEyAaaEedjALIEwIdLLEndjLcdEblEbejEygEjtEaIAyEblALLchpEkfdedpAhpEklEklE
abdhpEkeEaAyptLAInEkfAbpIdLdIzAIALL
LAjneEIcIALAfdkIcjdA

Amb la substitució de la lletra l, podem pensar que Ebl i Ekl són ECl O ETl, però. Llavors falta saber si la B codifica per la T o és la K la que codifica per la T, en color blau farem que la B codifica per la T i en verd al revés, la K codifica per la T.

En aquest cas provarem que la B codifica per la T i la K per la C.

s (46) = E	k (21) = C	p (14)	t (6)
l (32) = A	c (20)	y (13)	h (6)
d (31)	b (20) = T	n (10)	w (2)
o (29) = S	a (16)	e (9)	z (1)
m (26) = L	j (14)	g (6)	

gEjeEtdTdadcpTgjcaEedyET IEC IECATcCjAtdaECAhpELLhpEAacTCECpEdwcapLIAjtdCdaAy
ETI ELydC CAICEIAgATILcctETILcdTqdCdiLEIcIdhpE
ELydCCAICEacyAIALECgjECETIETALCpTLLcadCdCAiEycTCAyACAcdTqEjIdyELgjcaEedyET
IecapLIAadcCAijEyAaaEedjALIEwIdLLECdjLcdETIETejEygEjtEaIAyETIALLchpECfdedpAhpEC
IECIEaTdhp EC eEaAyptLAIC EC fATpIdLdIzAIALL
LajCe EIc IALAfdCIcjdA

Com que hem deixat la D pel mig, i de D en tenim 31, anem a veure per freqüències què podria ser la d. Segons la taula de freqüències li tocaria la S.

s (46) = E	k (21) = C	p (14)	t (6)
l (32) = A	c (20)	y (13)	h (6)
d (31) = S	b (20) = T	n (10)	w (2)
o (29) = I	a (16)	e (9)	z (1)
m (26) = L	j (14)	g (6)	

gEjeEtSTSaScpTgjcaEeSyET IEC IECATcCjAtSaECAhpELLhpEAacTCECpESwcapLIAjtSCSaAy
ETI ELySC CAICEIAgATILcctETILcSTqSCSiLEIcIShpE
ELySCCAICEacyAIALECgjECETIETALCpTLLcaSCSCAiEycTCAyACAcSTqEjISyELgjcaEeSyETI
ecapLIAaScCAijEyAaaEeSjALIEwISLLECSjLcSETIETejEygEjtEaIAyETIALLchpECfSeSpAhpEC
IECIEaTShp EC eEaAyptLAIC EC fATpISLSIzAIALL
LajCe EIc IALAfSCIcjSA

No li veig cap sentit, provem ara al revés, que la B codifica per la C i la K codifica per la T.

gEjeEtdCdadcpCgjcaEedyECIETIEnACcnjAtdaETAhpELLhpEAacCTEnpEdwcapLIAjtdTdaAyEC
IELydTTAInEIAgACILcctECILcdCqdTdiLEIcIdhpE
ELydTTAInEacyAIALETgjETECIECALnpCLLcadTdTAiEycCTAyAnAcdCqEjIdyELgjcaEedyECI
ecapLIAadcTAijEyAaaEedjALIEwIdLLEndjLcdECIECejEygEjtEaIAyECIALLchpETfdedpAhpETI
ETIEaCdhpETeEaAyptLAInETfACpIdLdI zAIAL
LLAjneEIcIALAfdTIcjdA

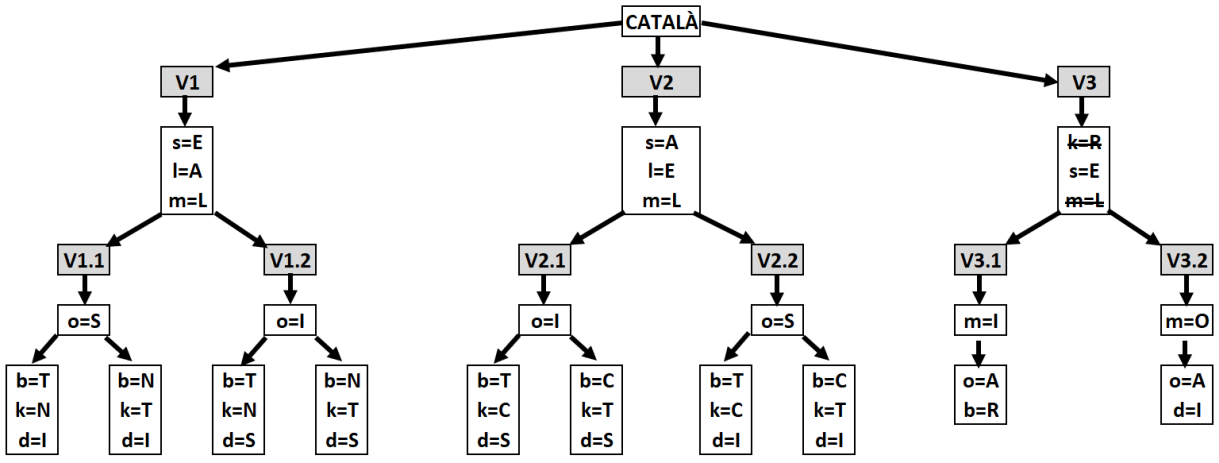
Com que hem deixat la D pel mig, i de D en tenim 31, anem a veure per freqüències què podria ser la d. Segons la taula de freqüències li tocaria la S.

s (46) = E	k (21) = N	p (14)	t (6)
l (32) = A	c (20)	y (13)	h (6)
d (31) = S	b (20) = T	n (10)	w (2)
o (29) = I	a (16)	e (9)	z (1)
m (26) = L	j (14)	g (6)	

gEjeEtSCSaScpCgjcaEeSyECIETIEnACcnjAtSaETAhpELLhpEAacCTEnpESwcapLIAjtSTSaAyECI
ELySTTAInEIAgACILcctECILcSCqSTSiLEIcIShpE
ELySTTAInEacyAIALETgjETECIECALnpCLLcaSTSTAiEycCTAyAnAcSCqEjISyELgjcaEeSyECIe
capLIAaScTAijEyAaaEeSjALIEwISLLEnSjLcSECIECejEygEjtEaIAyECIALLchpETfSeSpAhpETIE
TIEaCShpETeEaAyptLAInETfACpISLSI zAIAL
LLAjneEIcIALAfSTIcjSA

Segueixo sense veure-li cap possible sentit, aniré cap a una altra direcció....

8.3 Tercer intent de desencriptació del text 2 (versió 2.1)



TEXT 2: El segon text és un altre text xifrat utilitzant la substitució, amb la diferència que en aquest no s'han mantingut els espais, per tant, és un xic més complicat. Igual que en el

gAjeAtdbdadcpbgjcaAedyAboAkoAnlbcnjltdaAklhpALLhpAlacbkAnpAdwcapLoljtdkdalyAboA
LydkklonAolglboLcctAboLcdbqdkdELAocodhpAALydkklonAacylolLAkgjAkAboAblLnpbLLcad
kdklEAycbklylnlcdbqAjodyALgjcaAedyAboecapLoladcklEjAylaaAedjlLoAwodLLAndjLcdAboA
bejAygAjtAaolyAbolLLchpAkfdedplhpAkoAkoAabdhpAkeAalyptLlonAkflbpodLdozlolLL
LljneAocolLlfdkocjdl

primer text, no sé en quin idioma està escrit l'original, tampoc sé la seva procedència ni la seva destinació.

En ser un text xifrat de la mateixa manera que el text 1, però amb la diferència dels espais, seguirem els mateixos passos, és a dir, començarem per determinar el nombre de cada lletra, per així ordenar-les de més freqüents a menys:

s (46)	k (21)	p (14)	t (6)
l (32)	c (20)	y (13)	h (6)
d (31)	b (20)	n (10)	w (2)
o (29)	a (16)	e (9)	z (1)
m (26)	j (14)	g (6)	

Ara ja tenim totes les lletres comptades i ordenades. Ja podem començar a substituir. Primer de tot agafarem la taula de freqüències de la llengua catalana, ja que, com que el primer text també me'l va passar en David Juher i estava escrit en català, penso que aquest podria estar també en català.

lletra	A	B	C	Ç	D	E	F	G	H	I	J	K	L	M
%	12,55	1,32	3,60	1,06	3,94	13,89	1	1,28	0,72	6,99	0,3	0	7,74	3,16
lletra	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
%	6,40	5,71	2,72	1,35	6,76	8,43	6,11	4,18	1,4	0	0,52	0	0,01	

s (46) ~ E	d (31) ~ S	m (26) ~ I	c (20) ~ N
l (32) ~ A	o (29) ~ L	k (21) ~ R	b (20) ~ T

a (16) ~ O	y (13) ~ C	g (6) ~ V	w (2) ~ G
j (14) ~ U	n (10) ~ M	t (6) ~ Q	z (1) ~ Ç
p (14) ~ D	e (9) ~ P	h (6) ~ B	

En aquesta versió el que farem serà capgirar la lletra E i la A i suposar que la S codifica per la lletra A i la L per la lletra E.

s (46) = A	k (21)	p (14)	t (6)
l (32) = E	c (20)	y (13)	h (6)
d (31)	b (20)	n (10)	w (2)
o (29)	a (16)	e (9)	z (1)
m (26)	j (14)	g (6)	

gAjeAtdbdadcpbgjcaAedyAboAkoAnEbcnjEtdaAkEhpAmmhpAEacbkAnpAdwcapmoEjtdkdaEy
AboAmydkkEonAoEgEbomcctAbomcdbqdkdimAocodhpAAmydkkEonAacyEoEmAkgjAkAboA
bEmnpbmmcadkdkEiAycbkEyEnEcdbqAjodyAmgjcaAedyAboecapmoEadckEijAyEaaAedjEmoA
wodmmAndjmcdAboAbejAygAjtAaoEyAboEmmchpAkfdedpEhpAkoAkoAabdhpAkeAaEyptmE
onAkfEbpodmdozEoEmmmEjneAocoEmEfdkocjdE

Amb aquesta substitució, si és que hem encertat l'idioma i és Català, ja podem intuir alguns espais, ja que, en català, dues A no van mai juntes.

gAjeAtdbdadcpbgjcaAedyAboAkoAnEbcnjEtdaAkEhpAmmhpAEacbkAnpAdwcapmoEjtdkdaEy
AboAmydkkEonAoEgEbomcctAbomcdbqdkdimAocodhpA
AmydkkEonAacyEoEmAkgjAkAboAbEmnpbmmcadkdkEiAycbkEyEnEcdbqAjodyAmgjcaAedy
AboecapmoEadckEijAyEaaAedjEmoAwodmmAndjmcdAboAbejAygAjtAaoEyAboEmmchpAkfd
edpEhpAkoAkoAabdhpAkeAaEyptmEonAkfEbpodmdozEoEmmmEjneAocoEmEfdkocjdE

En català només existeixen les ss, rr, ll, mm, nn, però mai n'hi ha de 3, per tant, significa que han d'anar separades i que dues de seguides seran a inici o final de paraula, les quals de parelles que hi poden anar només n'hi ha una, la LL. Així doncs, substituirem la M per la L.

s (46) = E	k (21)	p (14)	t (6)
l (33) = A	c (20)	y (13)	h (6)
d (31)	b (20)	n (10)	w (2)
o (29)	a (16)	e (9)	z (1)
m (26) = L	j (14)	g (6)	

gAjeAtdbdadcpbgjcaAedyAboAkoAnEbcnjEtdaAkEhpALLhpAEacbkAnpAdwcapLoEjtdkdaEyA
boALydkkEonAoEgEboLcctAboLcdbqdkdiLAocodhpA
ALydkkEonAacyEoELAkgjAkAboAbELnpbLLcadkdkEiAycbkEyEnEcdbqAjodyALgjcaAedyAbo
ecapLoEadckEijAyEaaAedjELoAwodLLAndjLcdAboAbejAygAjtAaoEyAboELLchpAkfdedpEhpA
koAkoAabdhpAkeAaEyptLEonAkfEbpodLdozEoELL
LEjneAocoELEfdkocjdE

El següent pas a seguir és buscar conjunt de lletres repetides per tal de poder imaginar quina paraula potser. Per exemple, el conjunt Ako es repeteix 3 vegades; Abo, 6 vegades i ALydkkEonA, dues vegades, el qual pot ser una paraula o dues, sense espais és complicat. Ara mateix no sé per on tirar, no em venen paraules que puguin funcionar en aquest text ni lletres que vagin bé a Abo o Ako.

El que sí que m'he adonat és que necessito saber quina lletra és codificada per la O, ja que surt moltes vegades i potser si la sé, podré substituir més lletres.

Substituirem la O guiant-nos per la taula de freqüències, i penso que podria ser la S o la I, així que ho substituiré amb les dues per veure quina hi va millor. FEM LA o=I

s (46) = E	d (31)	m (26) = L	c (20)
l (32) = A	o (29) = I	k (21)	b (20)

a (16)	y (13)	g (6)	w (2)
j (14)	n (10)	t (6)	z (1)
p (14)	e (9)	h (6)	

Amb la substitució de la lletra I, podem pensar que AbI i AkI podrien ser ACI O ATI (no té massa sentit, però intentem tirar endavant). Llavors falta saber si la B codifica per la T o és la K la que codifica per la T, en aquest cas provarem que la B codifica per la T i la K per la C. (blau). En verd provarem que la K codifica per la T.

gAjeAtdbdadcpbgjcaAedyAbIAkIAnEbcnjEtdaAkEhpALLhpAEacbkAnpAdwcapLIEjtdkdaEyAb
IALydkkEInAIEgEbILcctAbILcdbqdkdiLAIcIdhpA
ALydkkEInAacyEIELAkgjAkAbIAbELnpbLLcadkdkEiAycbkEyEnEcdbqAjIdyALgjcaAedyAbIec
apLIEadckEijAyEaaAedjELIAwIdLLAndjLcdAbIAbejAygAjtAaIEyAbIELLchpAkfdedpEhpAkIA
kIAabdhpAkeAaEyptLEInAkfEbpIdLdIzEIELL
LEjneAIcIELEfdkIcjdE

s (46) = E	k (21) = C	p (14)	t (6)
l (32) = A	c (20)	y (13)	h (6)
d (31)	b (20) = T	n (10)	w (2)
o (29) = I	a (16)	e (9)	z (1)
m (26) = L	j (14)	g (6)	

Com que hem deixat la D pel mig, i de D en tenim 31, anem a veure per freqüències què podria ser la D. Segons la taula de freqüències li tocaria la S.

gAjeAtdTdadcpTgjcaAedyAT IAC ACETcCjEtdaACEhpALLhpAEacTCACpAdwcapLIEjtdCdaEy
ATI ALydC CEICAIEgETILcctATILcdTqdCdiLAIcIdhpA
ALydCCEICAacyEIELACgjACATIATELCpTLLcadCdCEiAycTCEyECEcdTqAjIdyALgjcaAedyA
TIecapLIEadcCEijAyEaaAedjELIAwIdLLACdjLcdATIATejAygAjtAaIEyATIELLchpACfdedpEhp
AC IACIAaTdhp AC eAaEyptLEIC AC fETpIdLdIzEIELL
LajCe AIc IELEfdCIcjdE

s (46) = E	k (21) = C	p (14)	t (6)
l (32) = A	c (20)	y (13)	h (6)
d (31) = S	b (20) = T	n (10)	w (2)
o (29) = I	a (16)	e (9)	z (1)
m (26) = L	j (14)	g (6)	

gAjeAtSTSaScpTgjcaAeSyAT IAC IACETcCjEtSaACEhpALLhpAEacTCACpASwcapLIEjtSCSaEy
ATI ALySC CEICAIEgETILcctATILcSTqSCSiLAIcIShpA
ALySCCEICAacyEIELACgjACATIATELCpTLLcaSCSCEiAycTCEyECEcSTqAjISyALgjcaAeSyAT
IecapLIEaScCEijAyEaaAeSjELIAwISLLACSjLcSATIATejAygAjtAaIEyATIELLchpACfSeSpEhpA
C IACIAaTShp AC eAaEyptLEIC AC fETpISLSIzEIELL
LajCe AIc IELEfSCIcjSE

Provem ara al revés, que la B codifica per la C i la K codifica per la T

gAjeAtdCdadcpCgjcaAedyACIATIAnECcnjEtdaATEhpALLhpAEacCTAnpAdwcapLIEjtdTdaEy
ACIALydTTEInAIEgECILcctACILcdCqdTdiLAIcIdhpA
ALydTTEInAacyEIELATgjATACIACELnpCLLcadTdTEiAycCTEyEnEcdCqAjIdyALgjcaAedyAC
IecapLIEadcTEijAyEaaAedjELIAwIdLLAndjLcdACIACejAygAjtAaIEyACIELLchpATfdedpEhpA
TIATIAaCdhpATeAaEyptLEInATfECpIdLdI zEIEL
LLEjneAIcIELEfdTIcjdE

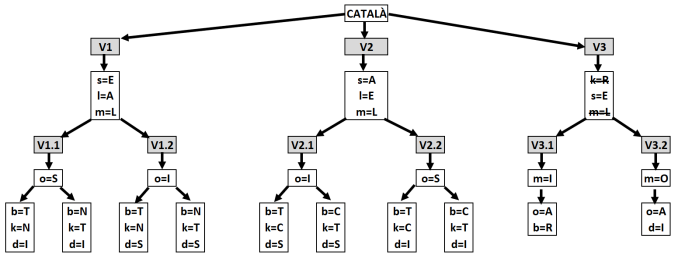
I com abans, com que hem deixat la D pel mig, i de D en tenim 31, anem a veure per freqüències què podria ser la D. Segons la taula de freqüències li tocaria la S.

gAjeAtSCSaScpCgjcaAeSyACIATIAnECcnjEtSaATEhpALLhpAEacCTAnpASwcapLIEjtSTSaEyA
CIALySTTEInAIEgECILcctACILcSCqSTSiLAIcIShpA
ALySTTEInAacyEIELATgjATACIACELnpCLLcaSTSTEiAycCTEyEnEcSCqAjISyALgjcaAeSyACI
ecapLIEaScTEijAyEaaAeSjELIAwISLLAnSjLcSACIACejAygAjtAaIEyACIELLchpATfSeSpEhpAT
IATIAaCShpATeAaEyptLEInATfECpISLSI zEIEL
LLEjneAIcIELEfSTIcjSE

s (46) = E	k (21) = N	p (14)	t (6)
l (32) = A	c (20)	y (13)	h (6)
d (31) = S	b (20) = T	n (10)	w (2)
o (29) = I	a (16)	e (9)	z (1)
m (26) = L	j (14)	g (6)	

Com que no li acabo de veure sentit, seguiré amb una nova opció de l'esquema que m´he fet, i si de cas després ja ho seguiré.

8.4 Quart intent de desencriptació del text 2 (versió 2.2)



TEXT 2: El segon text és un altre text xifrat utilitzant la substitució, amb la diferència que en aquest no s'han mantingut els espais, per tant, és un xic més complicat. Igual que en el primer text, no sé en quin idioma està escrit l'original, tampoc sé la seva procedència ni la seva destinació.

gAjeAtdbdadcpbgjcaAedyAboAkoAnlbcnjltdaAklhpALLhpAlacbkAnpAdwcapLoljtdkdalyAboA
LydkklonAolglboLcctAboLcdbqdkdELAocodhpAALydkklonAacylolLAkgjAkAboAblLnpbLLcad
kdklEAycbklylnlcdbqAjodyALgjcaAedyAboecapLoladcklEjAylaaAedjlLoAwodLLAndjLcdAboA
bejAygAjtAaolyAbolLLchpAkfdedplhpAkoAkoAabdhpAkeAalyptLlonAkflbpodLdozlolLL
LljneAocolLlfdkocjdl

Al ser un text xifrat de la mateixa manera que el text 1, però amb la diferència dels espais, seguirem els mateixos passos, és a dir, començarem per determinar el nombre de cada lletra, per així ordenar-les de més freqüents a menys:

s (46)	k (21)	p (14)	t (6)
l (32)	c (20)	y (13)	h (6)
d (31)	b (20)	n (10)	w (2)
o (29)	a (16)	e (9)	z (1)
m (26)	j (14)	g (6)	

Ara ja tenim totes les lletres comptades i ordenades. Ja podem començar a substituir. Primer de tot agafarem la taula de freqüències de la llengua catalana, ja que, com que el

primer text també me'l va passar en David Juher i estava escrit en català, penso que aquest podria estar també en català.

lletra	A	B	C	Ç	D	E	F	G	H	I	J	K	L	M
%	12,55	1,32	3,60	1,06	3,94	13,89	1	1,28	0,72	6,99	0,3	0	7,74	3,16
lletra	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
%	6,40	5,71	2,72	1,35	6,76	8,43	6,11	4,18	1,4	0	0,52	0	0,01	

s (46) ~ E
l (32) ~ A
d (31) ~ S
o (29) ~ L
m (26) ~ I
k (21) ~ R
c (20) ~ N
b (20) ~ T
a (16) ~ O
j (14) ~ U
p (14) ~ D
y (13) ~ C
n (10) ~ M
e (9) ~ P
g (6) ~ V
t (6) ~ Q
h (6) ~ B
w (2) ~ G
z (1) ~ Ç

Amb la taula podríem suposar que la S codifica per la lletra A i la L per la lletra E.

s (46) = A
l (32) = E
d (31)
o (29)
m (26)
k (21)
c (20)
b (20)
a (16)
j (14)
p (14)
y (13)
n (10)
e (9)
g (6)
t (6)
h (6)
w (2)
z (1)

gAjeAtdbdadcpbgjcaAedyAboAkoAnEbcnjEtdaAkEhpAmmhpAEacbkAnpAdwcapmoEjtdkdaEy
AboAmydkkEonAoEgEbomcctAbomcdbqdkdimAocodhpAAmydkkEonAacyEoEmAkgjAkAboA
bEmnpbmmcadkdkEiAycbkEyEnEcdbqAjodyAmgjcaAedyAboecapmoEadckEijAyEaaAedjEmoA
wodmmAndjmcdAboAbejAygAjtAaoEyAboEmmchpAkfdedpEhpAkoAkoAabdhpAkeAaEyptmE
onAkfEbpodmdozEoEmmmEjneAocoEmEfdkocjdE

Amb aquesta substitució, si és que hem encertat l'idioma i és Català, ja podem intuir alguns espais, ja que, en català, dues A no van mai juntes.

gAjeAtdbdadcpbgjcaAedyAboAkoAnEbcnjEtdaAkEhpAmmhpAEacbkAnpAdwcapmoEjtdkdaEy
AboAmydkkEonAoEgEbomcctAbomcdbqdkdimAocodhpA
AmydkkEonAacyEoEmAkgjAkAboAbEmnpbmmcadkdkEiAycbkEyEnEcdbqAjodyAmgjcaAedy
AboecapmoEadckEijAyEaaAedjEmoAwodmmAndjmcdAboAbejAygAjtAaoEyAboEmmchpAkfd
edpEhpAkoAkoAabdhpAkeAaEyptmEonAkfEbpodmdozEoEmmmEjneAocoEmEfdkocjdE

En català només existeixen les ss, rr, ll, mm, nn, però mai n'hi ha de 3, per tant, significa que han d'anar separades i que dues de seguides seran a inici o final de paraula, les quals de parelles que hi poden anar només n'hi ha una, la LL. Així doncs, substituirem la M per la L.

s (46) = E	k (21)	p (14)	t (6)
l (33) = A	c (20)	y (13)	h (6)
d (31)	b (20)	n (10)	w (2)
o (29)	a (16)	e (9)	z (1)
m (26) = L	j (14)	g (6)	

gAjeAtdbdadcpbgjcaAedyAboAkoAnEbcnjEtdaAkEhpALLhpAEacbkAnpAdwcapLoEjtdkdaEyA
boALydkkEonAoEgEboLcctAboLcdbqdkdiLAocodhpA
ALydkkEonAacyEoELAkgjAkAboAbELnpbLLcadkdkEiAycbkEyEnEcdbqAjodyALgjcaAedyAbo
ecapLoEadckEijAyEaaAedjELoAwodLLAndjLcdAboAbejAygAjtAaoEyAboELLchpAkfdedpEhpA
koAkoAabdhpAkeAaEyptLEonAkfEbpodLdozEoELL
LEjneAocoELEfdkocjdE

El següent pas a seguir és buscar conjunt de lletres repetides per tal de poder imaginar quina paraula potser. Per exemple, el conjunt Ako es repeteix 3 vegades; Abo, 6 vegades i ALydkkEonA, dues vegades, el qual pot ser una paraula o dues, sense espais és complicat. Ara mateix no sé per on tirar, no em venen paraules que puguin funcionar en aquest text ni lletres que vagin bé a Abo o Ako. El que sí que m'he adonat és que necessito saber quina

lletra és codificada per la O, ja que surt moltes vegades i potser si la sé, podré substituir més lletres.

Substituirem la O guiant-nos per la taula de freqüències, i penso que podria ser la S o la I, així que ho substituiré amb les dues per veure quina hi va millor. FEM LA o=S

s (46) = E	k (21)	p (14)	t (6)
l (32) = A	c (20)	y (13)	h (6)
d (31)	b (20)	n (10)	w (2)
o (29) = S	a (16)	e (9)	z (1)
m (26) = L	j (14)	g (6)	

gAjeAtdbdadcpbgjcaAedyAbSAkSAnEbcnjEtdaAkEhpALLhpAEacbkAnpAdwcapLSEjtdkdaEyAbSALydkkESnASEgEbSLcctAbSLcdbqdkdiLAScSdhpA
ALydkkESnAacyESELAkgjAkAbSAbELnpbLLcadkdkEiAycbkEyEnEcdbqAjSdyALgjcaAedyAbSecapLSEadckEijAyEaaAedjELSAwSdLLAndjLcdAbSAbejAygAjtAaSEyAbSELLchpAkfdedpEhpAkSAkSAabdhpAkeAaEyptLESnAkfEbpSdLdSzESELL
LEjneAScSELEfdkScjdE

Seguim ara amb l'esquema, tot i que ja vaig veient que no té massa sentit, ja que AbS AkS no acabo de veure què poden ser. Anem però a provar que la B codifica per la T i la K per la C.

s (46) = a	k (21) = C	p (14)	t (6)
l (32) = e	c (20)	y (13)	h (6)
d (31)	b (20) = T	n (10)	w (2)
o (29) = S	a (16)	e (9)	z (1)
m (26) = L	j (14)	g (6)	

gAjeAtdTdadcpTgjcaAedyATSACSAnETcnjEtdaACEhpALLhpAEacTCAnpAdwcapLSEjtdCdaEy
ATSALydCCESnASEgETSLcctATSLcdTqdCdiLAScSdhpA
ALydCCESnAacyESELACgjACATSATELnpTLLcadCdCEiAycTCEyEnEcdTqAjSdyALgjcaAedyA
TSecapLSEadcCEijAyEaaAedjELSAwSdLLAndjLcdATSATejAygAjtAaSEyATSELLchpACfdedpE
hpACSACSAaTdhpACeAaEyptLESnACfETpSdLdSzESELL
LEjneAScSELEfdCScjdE

Com que hem deixat la D pel mig, i de D en tenim 31, anem a veure per freqüències què podria ser la D. Segons la taula de freqüències li tocaria la S, però com que ja hem suposat que era la O, agafarem la que estigui més propera, la d hauria de ser o bé una L o una I. Com que la L ja l'hem feta servir anirem per la I.

s (46) = A	k (21) = C	p (14)	t (6)
l (32) = E	c (20)	y (13)	h (6)
d (31) = I	b (20) = T	n (10)	w (2)
o (29) = S	a (16)	e (9)	z (1)
m (26) = L	j (14)	g (6)	

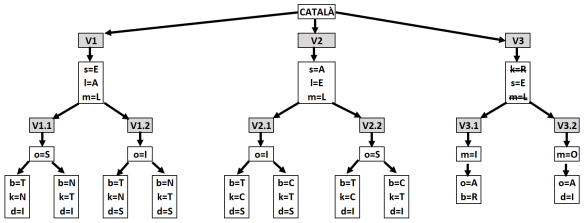
gAjeAtITIaIcpTgjcaAeIyATSACSAnETcnjEtIaACEhpALLhpAEacTCAnpAIwcapLSEjtICIaEyAT
SALyICCESnASEgETSLcctATSLcITqICIiLAScSIhpA
ALyICCESnAacyESELACgjACATSATELnpTLLcaICICEiAycTCEyEnEcITqAjSIyALgjcaAeIyATS
ecapLSEaIcCEijAyEaaAeIjELSAwSILLAnIjLcIATSATejAygAjtAaSEyATSELLchpACfIeIpEhpAC
SACSAaTIhpACeAaEyptLESnACfETpSILISzESELL
LEjneAScSELEfICScjIE

Provem ara al revés, que la B codifica per la C i la K codifica per la T.

gAjeAtICIaIcpCgjcaAeIyACSATSAnECcnjEtIaATEhpALLhpAEacCTAnpAIwcapLSEjtITIaEyAC
SALyITTESnASEgECSLcctACSLcICqITIiLAScSIhpA
ALyITTESnAacyESELATgjATACSACELnpCLLcaITITEiAycCTEyEnEcICqAjSIyALgjcaAeIyACS
ecapLSEaIcTEijAyEaaAeIjELSAwSILLAnIjLcIACSACejAygAjtAaSEyACSELLchpATfIeIpEhpAT
SATSAaCIhpATeAaEyptLESnATfECpSILISzESELL
LEjneAScSELEfITScjIE

Un cop més em veig en una via morta, no veig què puc fer amb tantes ACS ATS.....,

8.5 Cinquè intent de desencriptació del text 2 (versió 3.1)



TEXT 2: El segon text és un altre text xifrat utilitzant la substitució, amb la diferència que en aquest no s'han mantingut els espais, per tant, és un xic més complicat. Igual que en el primer text, no sé en quin idioma està escrit l'original, tampoc sé la seva procedència ni la seva destinació.

gsjestdbdadcpbgjcasedysboskosnlbcnjltdasklhpsmmhpslacbksnpsdwcapmoljtdkdalysbosmydkkl
onsolglbomcctsbomcdbqdkdimsocodhpssmydkklonsacylolmskgjsksbosblmnpbmmcadkdklisycb
klylnlcdbqsjodysmgjcasedysboecapmoladcklijsylaasedjlmoswod
mmsndjmcdsbosbejsygsjtsaolysbolmmchpskfdedplhpskoskosabdhpskesalyptmlonskflbpodmdozl
olmmmljnesocolmlfdkocjdl

En ser un text xifrat de la mateixa manera que el text 1, però amb la diferència dels espais, seguirem els mateixos passos, és a dir, començarem per determinar el nombre de cada lletra, per així ordenar-les de més freqüents a menys:

s (46)	k (21)	p (14)	t (6)
l (32)	c (20)	y (13)	h (6)
d (31)	b (20)	n (10)	w (2)
o (29)	a (16)	e (9)	z (1)
m (26)	j (14)	g (6)	

Ara ja tenim totes les lletres comptades i ordenades. Ja podem començar a substituir. Primer de tot agafarem la taula de freqüències de la llengua catalana, ja que, com que el primer text també me'l va passar en David Juher i estava escrit en català, penso que aquest podria estar també en català.

lletra	A	B	C	Ç	D	E	F	G	H	I	J	K	L	M
%	12,55	1,32	3,60	1,06	3,94	13,89	1	1,28	0,72	6,99	0,3	0	7,74	3,16
lletra	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
%	6,40	5,71	2,72	1,35	6,76	8,43	6,11	4,18	1,4	0	0,52	0	0,01	

s (46) ~ E	k (21) ~ R	p (14) ~ D	t (6) ~ Q
l (32) ~ A	c (20) ~ N	y (13) ~ C	h (6) ~ B
d (31) ~ S	b (20) ~ T	n (10) ~ M	w (2) ~ G
o (29) ~ L	a (16) ~ O	e (9) ~ P	z (1) ~ Ç
m (26) ~ I	j (14) ~ U	g (6) ~ V	

Com que amb el que he anat fent fins ara no veig que avanci, el que faré serà buscar repeticions de 2 i de 3 lletres, per veure si les puc associar a les lletres que en català són dobles... Després el que faré serà anar per la taula de freqüències igualment, però fent variacions sobre el que havia fet a les altres 4 versions, i intercanviant alguna lletra.

gsjestdbdadcpbgjcasedysboskosnlbcnjltdasklhpsmmhpslacbksnpsdwcapmoljtdkdalysbosmydkkl
onsolglbomcctsbomcdbqdkdimsocodhpssmydkklonsacylolmskgjsksbosblmnpbmmcadkdklisycb
klylnlcdbqsjodysmgjcasedysboecapmoladcklijsylaasedjlmoswod
mmsndjmcdsbosbejsygsjtsaolysbolmmchpskfdedplhpskoskosabdhpskesalyptmlonskflbpodmdozl
olmmmljnesocolmlfdkocjdl

En català només existeixen les ss, rr, ll, mm, nn, però mai n'hi ha de 3, per tant, significa que han d'anar separades i que dues de seguides seran a inici o final de paraula, les quals de parelles que hi poden anar només n'hi ha una, la LL. Així doncs, substituirem la M per la L, i com que per freqüències surt més la R que no pas la S, posarem la k=R

gsjestdbdadcpbgjcasedysbosRosnlbcnjltdasRlhpsLLhpslacbRsnpsdwcapLoljtdRdalysbosLydRRl
onsolglboLcctsboLcdbqdRdiLsocodhpssLydRRlonsacylolLsRgjsRsbosblLnpbLLcadRdRlisycb
RlylnlcdbqsjodysLgjcasedysboecapLoladcRlijsylaasedjlLoswod
LLsndjLcdsbosbejsygsjtsaolysbolLLchpsRfdedplhpsRosRosabdhpsResalyptLlonsRflbpodLdozl
olLLLljnesocolLlfdRocjdl

Un cop fet això, comencem de nou amb la taula de freqüències, havíem partit del fet que les dues que més surten havien de ser E i A, però si mirem els números, i que ho assignàvem a les s (46) i l(32), però com que entre la l i la d (31) no hi ha molta diferència, anem a fer ara que la que més surt sigui la E i la segona que sigui la S

Farem doncs s=E i l=S

s (46) = E	k (21)	p (14)	t (6)
l (32) = S	c (20)	y (13)	h (6)
d (31)	b (20)	n (10)	w (2)
o (29)	a (16)	e (9)	z (1)
m (26)	j (14)	g (6)	

gEjeEtdbdadcpbgjcaEedyEboERoEnSbcnjStdaERShpELLhpESacbREnpEdwcapLoSjtdRdaSyEboE
LydRRSonEoSgSboLcctEboLcdbqdRdiLEocodhpE
ELydRRSonEacySoSLERgjEREboEbSLnpbLLcadRdRSiEycbRSySnScdbqEjodyELgjcaEedyEboeca
pLoSadcRSijEySaaEedjSLoEwodLLEndjLcdEboEbejEygEjtEaoSyEboSLLchpERfdedpShpERoERo
EabdhpEReEaSyptLSonERfSbpodLdozSoSLLLSjneEocoSLSfdRocjdS

Amb aquesta substitució, si és que hem encertat l'idioma i és Català, ja podem intuir alguns espais, ja que, en català, dues E no van mai juntes. També veiem que l'assumpció de que la k=R no té massa sentit doncs ens queden moltes consonants juntes (RRS) i també veiem que l'assumpció que la m=L tampoc tindria sentit, ja que ens queda SLLLS. Per tant si volem anar en aquesta direcció el que hem de fer és desfer els primers canvis... Desfarem la k=R i en comptes de m=L farem m=I que també podria ser si tinguéssim una paraula acabada en i, una i solta i una començada en i. Això ens fa a més posar espais entre totes les i, ja que mai van dues i seguides.

El següent pas a seguir és buscar conjunt de lletres repetides per tal de poder imaginar quina paraula potser. Per exemple, el conjunt Eko es repeteix 3 vegades; Ebo, 6 vegades i ELydkkAonE, dues vegades, el qual pot ser una paraula o dues, sense espais és complicat. Ara mateix no sé per on tirar, no em venen paraules que puguin funcionar en aquest text ni lletres que vagin bé a Ebo o Eko. El que sí que m'he adonat és que necessito saber quina lletra és codificada per la O, ja que surt moltes vegades i potser si la sé, podré substituir més lletres.

Substituirem la O guiant-nos per la taula de freqüències, i penso que podria ser la S o la I, però com que les he fet servir totes dues ja, posem-hi la A que també és de les que surt més.

gEjeEtdbdadcpbgjcaEedyEbAEkAEnSbcnjStdaEkShpEI
IhpESacbkEnpEdwcapIASjtdkdaSyEbAEIydkkSAnEASgSbAIcctEbAIcdbqdkdiIEAcAdhpE
EIydkkSAnEacySASIEkgjEkEbAEbSInpbI
IcadkdkSiEycbkSySnScdbqEjAdyEIgjcaEedyEbAecapIASadckSijEySaaEedjSIAEwAdI
IEndjIcdEbAEbejEygEjtEaASyEbASI
IchpEkfdedpShpEkAEkAEabdhpEkeEaSyptISAnEkfSbpAdIdAzSASI I ISjneEAcASISfdkAcjdS

s (46) = E	k (21)	p (14)	t (6)
l (32) = S	c (20)	y (13)	h (6)
d (31)	b (20)	n (10)	w (2)
o (29) = A	a (16)	e (9)	z (1)
m (26) = I	j (14)	g (6)	

Amb la substitució de la lletra A, podem pensar que EbA i EkA són EFA, EIA ELA, ERA, ETA, EMA, o ENA. Com que la B surt 20 vegades, la F ja la podem descartar, ja que és una lletra que surt molt poc, la I ja la tenim agafada. El problema és que la L, R, M, N i T surten quasi per igual, i per tant és molt difícil de treure'n una. De tota manera no sembla massa

lògic que tinguem una paraula que acabi en una d'aquestes terminacions i a continuació en comenci una altra amb una altra d'aquestes combinacions.

gEjeEtdbdadcpbgjcaEedyEboEkoEnSbcnjStdaEkShpEI

IhpESacbkEnpEdwcapIoSjtdkdaSyEboEIydkkSonEoSgSboIcctEboIcdbqdkdiIEocodhpE

EIydkkSonEacySoSIEkgjEkEboEbSInpbI

IcadkdkSiEycbkSySnScdbqEjodyEIgjcaEedyEboecapIoSadckSijEySaaEedjSIoEwodI

IEndjIcdEboEbejEygEjtEaoSyEboSI

IchpEkfdedpShpEkoEkoEabdhpEkeEaSyptISonEkfSbpodIdozSoSI I ISjneEocoSISfdkocjdS

Provarem de codificar la b per R, puix que hi ha moltes paraules que acaben i comencen en ERA.

s (46) = E	k (21)	p (14)	t (6)
l (32) = S	c (20)	y (13)	h (6)
d (31)	b (20) = R	n (10)	w (2)
o (29) = A	a (16)	e (9)	z (1)
m (26) = I	j (14)	g (6)	

gEjeEtdRdadcpRgjcaEedyERA EkAEnSRcnjStdaEkShpEI IhpESacRkEnpEdwcapIASjtdkdaSyERA

EIydkkSAnEASgSRAIcctERA IcdRqdkdiIEAcAdhpE

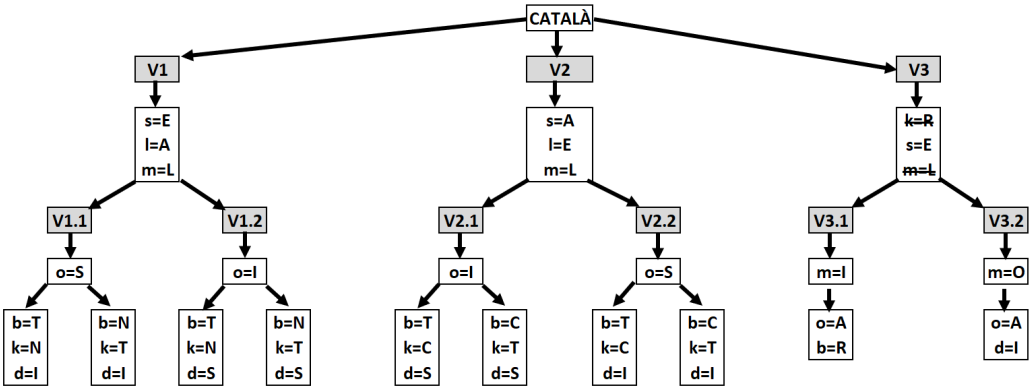
EIydkkSAnEacySASIEkgjEkERA ERSInpRI IcadkdkSiEycRkSySnScdRqEjAdyEIgjcaEedyERA

ecapIASadckSijEySaaEedjSIAEwAdI IEndjIcdERA ERejEygEjtEaASyERA SI

IchpEkfdedpShpEkAEkAEaRdhpEkeEaSyptISAnEkfSRpAdIdAzSASI I ISjneEAcASISfdkAcjdS

Amb les poques lletres que tenim desxifrades i els pocs espais podem començar veure que hi ha coses sense sentit, i per tant que no anem en bon camí. Per exemple **ERAEI o ERAER,** no veig com puc acabar en ERA per exemple i començar per EI, i no hi ha paraules que acabin en ERAE, de fet no hi ha paraules que acabin en E.AE. Penso que és una via morta.

8.6 Sisè intent de desencriptació del text 2 (versió 3.2)



TEXT 2: El segon text és un altre text xifrat utilitzant la substitució, amb la diferència que en aquest no s'han mantingut els espais, per tant, és un xic més complicat. Igual que en el primer text, no sé en quin idioma està escrit l'original, tampoc sé la seva procedència ni la seva destinació.

gsjestdbdadcpbgjcasedysboskosnlbcnjltdasklhpsmmhpslacbksnpsdwcapmoljtdkdalysbosmydkkl
onsolglbomcctsbomcdbqdkdimsocodhpssmydkklonsacylolmskgjsksbosblmnpbmmcadkdklisycb
klylnlcdbqsjodysmgjcasedysboecapmoladcklijsylaasedjlmoswod
mmsndjmcdsbosbejsygsjtsaolysbolmmchpskfdedplhpskoskosabdhpskesalyptmlonskflbpodmdozl
olmmmljnesocolmlfdkocjdl

En ser un text xifrat de la mateixa manera que el text 1, però amb la diferència dels espais, seguirem els mateixos passos, és a dir, començarem per determinar el nombre de cada lletra, per així ordenar-les de més freqüents a menys:

s (46)	k (21)	p (14)	t (6)
l (32)	c (20)	y (13)	h (6)
d (31)	b (20)	n (10)	w (2)
o (29)	a (16)	e (9)	z (1)
m (26)	j (14)	g (6)	

Ara ja tenim totes les lletres comptades i ordenades. Ja podem començar a substituir. Primer de tot agafarem la taula de freqüències de la llengua catalana, ja que, com que el primer text també me'l va passar en David Juher i estava escrit en català, penso que aquest podria estar també en català.

lletra	A	B	C	Ç	D	E	F	G	H	I	J	K	L	M
%	12,55	1,32	3,60	1,06	3,94	13,89	1	1,28	0,72	6,99	0,3	0	7,74	3,16
lletra	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
%	6,40	5,71	2,72	1,35	6,76	8,43	6,11	4,18	1,4	0	0,52	0	0,01	

s (46) ~ E	k (21) ~ R	p (14) ~ D	t (6) ~ Q
l (32) ~ A	c (20) ~ N	y (13) ~ C	h (6) ~ B
d (31) ~ S	b (20) ~ T	n (10) ~ M	w (2) ~ G
o (29) ~ L	a (16) ~ O	e (9) ~ P	z (1) ~ Ç
m (26) ~ I	j (14) ~ U	g (6) ~ V	

Com abans, anem ara a buscar repeticions de 2 i de 3 lletres

gsjestdbdadcpbgjcasedysboskosnlbcnjltdasklhpsmmhpslacbksnpsdwcapmoljtdkdalysbosmydkkl
onsolglbomcctsbomcdbqdkdimsocodhpssmydkklonsacylolmskgjsksbosblmnpbmmcadkdklisycb
klylnlcdbqsjodysmgjcasedysboecapmoladcklijsylaasedjlmoswod
mmsndjmcdsbosbejsygsjtsaolysbolmmchpskfdedplhpskoskosabdhpskesalyptmlonskflbpodmdozl
olmmmljnesocolmlfdkocjdl

En català només existeixen les ss, rr, ll, mm, nn, però mai n'hi ha de 3, per tant, significa que han d'anar separades i que dues de seguides seran a inici o final de paraula, les quals de parelles que hi poden anar només n'hi ha una, la LL. Així doncs, substituirem la M per la L.

gsjestdbdadcpbgjcasedysbosRosnlbcnjltdasRlhpsLLhpslacbRsnpsdwcapLoljtdRdalysbosLydRRl
onsolglboLcctsboLcdbqdRdiLsocodhpssLydRRlonsacylolLsRgjsRsbosblLnpbLLcadRdRlisycb
RlylnlcdbqsjodysLgjcasedysboecapLoladcRlijsylaasedjlLoswod
LLsndjLcdsbosbejsygsjtsaolysbolLLchpsRfdedplhpsRosRosabdhpsResalyptLlonsRflbpodLdozl
olLLLljnesocolLlfdRocjdl

Per freqüències surt més la R que no pas la S, posarem la k=R
Un cop fet això, comencem de nou amb la taula de freqüències, havíem partit del fet que les dues que més surten havien de ser E i A, però si mirem els números, i que ho assignàvem a les s (46) i l(32), però com que entre la l i la D (31) no hi ha molta diferència, anem a fer ara que la que més surt sigui la E i la segona que sigui la S
Farem doncs s=E i l=S

s (46) = E	k (21)	p (14)	t (6)
l (32) = S	c (20)	y (13)	h (6)
d (31)	b (20)	n (10)	w (2)
o (29)	a (16)	e (9)	z (1)
m (26)	j (14)	g (6)	

gEjeEtdbdadcpbgjcaEedyEboEkoEnSbcnjStdaEkShpEO

OhpESacbkEnpEdwcapOoSjtdkdaSyEboEOydkkSonEoSgSboOcctEboOcdbqdkdiOEocodhpE

EOydkkSonEacySoSOEkgjEkEboEbSOnpbO

OcadkdkSiEycbkSySnScdbqEjodyEOgjcaEedyEboecapOoSadckSijEySaaEedjSOoEwodO

OEndjOcdEboEbejEygEjtEaoSyEboSO

OchpEkfdedpShpEkoEkoEabdhpEkeEaSyptOSonEkfSbpodOdozSoSO O OSjneEocoSOSfdkocjdS

Amb aquesta substitució, si és que hem encertat l'idioma i és Català, ja podem intuir alguns espais, ja que, en català, dues E no van mai juntes. També veiem que l'assumpció que la k=R no té massa sentit doncs ens queden moltes consonants juntes (RRS) i també veiem que l'assumpció que la m=L tampoc tindria sentit, ja que ens queda SLLLS. Per tant si volem anar en aquesta direcció el que hem de fer és desfer els primers canvis... Desfarem la k=R i en comptes de m=L farem m=O que també podria ser si tinguéssim una paraula acabada en o, una o solta i una començada en o. Això ens fa a més posar espais entre totes les o, ja que mai van dues i seguides.

El següent pas a seguir és buscar conjunt de lletres repetides per tal de poder imaginar quina paraula potser. Per exemple, el conjunt Eko es repeteix 3 vegades; Ebo, 6 vegades i EOydkkSonE, dues vegades, el qual pot ser una paraula o dues, sense espais és complicat. Ara mateix no sé per on tirar, no em venen paraules que puguin funcionar en aquest text ni lletres que vagin bé a Ebo o Eko. El que sí que m'he adonat és que necessito saber quina lletra és codificada per la O, ja que surt moltes vegades i potser si la sé, podré substituir més lletres.

Substituirem la O guiant-nos per la taula de freqüències, i penso que podria ser la S, la A o la I. Per la taula de freqüències la A surt més que la I, i com que encara em queda per assignar la D que surt més, posarem d=A i o=I a veure què surt, i si no, ho creuarem.

s (46) = E	k (21)	p (14)	t (6)
l (32) = S	c (20)	y (13)	h (6)
d (31)= A	b (20)	n (10)	w (2)
o (29) = I	a (16)	e (9)	z (1)
m (26) = O	j (14)	g (6)	

gEjeEtAbAaAcpbgjcaEeAyEbIEkIEnSbcnjStAaEkShpEO
OhpESacbkEnpEAwcapOISjtAkAaSyEbIEOyAkkSInEISgSbIOcctEbIOcAbqAkAiOEIcIAhpE
EOyAkkSInEacySISOEkgjEkEbIEbSOnpbO
OcaAkAkSiEycbkSySnScAbqEjIAyEOgjcaEeAyEbIecapOISaAckSijEySaaEeAjSOIEwIAO
OEnAjOcAEbIEbejEygEjtEaISyEbISOchpEkfAeApShpEkIEkIEabAhpEkeEaSyptOSInEkfSbpIAO
AIzSISO O OSjneEIcISOSfAkIcjAS

Amb aquest canvi ja veiem que no anem bé, ja que ens surten moltes agrupacions de vocals que difícilment faran paraules, surten molts de EO, OI, IAO, OIE,... per tant anem a fer el canvi invers a veure si millora.

s (46) = E	k (21) =	p (14)	t (6)
l (32) = S	c (20)	y (13)	h (6)
d (31) = I	b (20) = R	n (10)	w (2)
o (29) = A	a (16)	e (9)	z (1)
m (26) = O	j (14)	g (6)	

gEjeEtIbIaIcpbgjcaEeIyEbAEkAEnSbcnjStIaEkShpEO

OhpESacbkEnpEIwcapOASjtIkIaSyEbAEOyIkkSAnEASgSbAOcctEbAOcIbqIkIiOEAcAIhpE

EOyIkkSAnEacySASOEkgjEkEbAEbSOnpbO

OcaIkIkSiEycbkSySnScIbqEjAIyEOgjcaEeIyEbAecapOASaIckSijEySaaEeIjSOAEwAIO

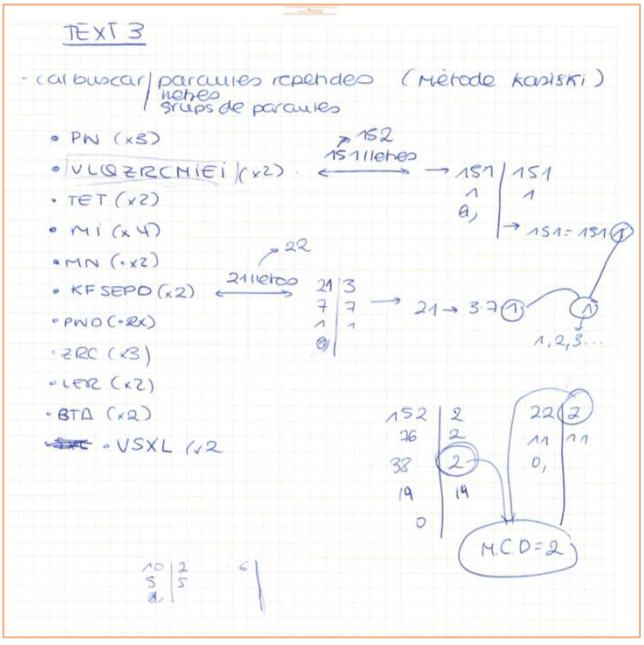
OEnIjOcIEbAEbejEygEjtEaASyEbASO

OchpEkfIeIpShpEkAEkAEabIhpEkeEaSyptOSAnEkfSbpAIOIAzSASO O OSjneEAcASOSfIkAcjIS

Igualment veiem moltes agrupacions de vocals que no ens donen confiança, penso que també és una via morta. Amb aquests experiments el que veig és que si la segona lletra més utilitzada la poso per una S, llavors les m només poden ser canviades per la L, doncs quan he fet el canvi per les I o per les O he acabat cada cop en una via morta.... I de fet quan he intentat fer la m per L tampoc ha funcionat, pel que dedueixo que anàvem millor quan consideràvem que les dues més utilitzades eren les de la taula de freqüències, la E i la A. Hauríem de tornar al principi.

8.7 Anotacions, proves i càlculs del text 3

A continuació hi ha una imatge de les anotacions i els càlculs que vaig fer per intentar resoldre el missatge xifrat 3:



9. FONTS D'INFORMACIÓ

Llibres

- JUHER, David. *L'art de la comunicació secreta.* Barcelona, Llibres de l'índex, 2004.
- SINGH, Simon. *Los códigos secretos.* Barcelona, Círculo de Lectores, 2000.

Webs

- *http://www.dma.fi.upm.es/recursos/aplicaciones/matematica_discreta/web/aritmetica_modular/criptografia.html#1* (04.03.29) Es tracta d'una pàgina web on t'introdueixen la criptografia d'entre altres temes de matemàtiques.
- *https://fme.upc.edu/ca/premi-poincare/arxius/criptografia_julia-alsina* (16.04.19) És un pdf d'un treball on s'estudia la criptografia.
- *https://www.recercat.cat/bitstream/handle/2072/2190/2005PJ00002.pdf?sequence=1* (16.04.19) Un pdf d'un treball de recerca on el tema era la criptografia.
- VIQUIPÈDIA, scytale. *https://en.wikipedia.org/wiki/Scytale* (16.04.19) L'explicació i una foto de la escítala espartana.
- GENEBETA, Tipus de criptografia, *https://www.genbeta.com/desarrollo/tipos-de-criptografia-simetrica-asimetrica-e-hibrida* (07.05.19) Hi ha una explicació de la criptografia simètrica, la asimètrica i la híbrida.
- VIQUIPÈDIA, història de la criptografia, *https://ca.wikipedia.org/wiki/Història_de_la_criptografia* (20.05.19) Explica tota la història de la criptografia, des dels seus inicis fins a l'actualitat.
- E-ADMINISTRACIÓN, métodos criptogràficos, *http://e-administracion.cea.es/metodos* (07.07.19) Fa una breu explicació de la criptografia simètrica i la asimètrica.
- LA CAMBRA NEGRA, Freqüència de les lletres, *https://mat-web.upc.edu/fme/codescryptography/CambraNegra/frequencyanalysis.html* Pàgina web d'on s'ha extret la taula de freqüències de la llengua catalana.
- VIQUIPÈDIA, Xifratge de Vigènere, *https://ca.wikipedia.org/wiki/Xifratge_de_Vigenère* (05.08.19) Fa una explicació del xifrat de vigènere.
- VIQUIPÈDIA, Mètode Kasiski, *https://ca.wikipedia.org/wiki/Mètode_Kasiski* (06.08.19) Hi ha una breu explicació del mètode Kasiski.

- EL DIARIO, Breve historia de la criptografia, *https://www.eldiario.es/turing/criptografia/Breve-historia-criptografia_0_261773822.html* (06.08.19) HI ha una explicació molt bona de les utilitats de la criptografia.
- BLOGGER, La criptografia, http://criptografiaenbachillerato.blogspot.com/2015/05/usos-de-la-criptografia.html (06.08.19) Es tracta d'una pàgina web on hi ha una llista d'utilitats de la criptografia.
- TODO LIBRO ANTIGUO, La Màquina Enigma, https://www.todolibroantiguo.es/criptografia-libros-antiguos/maquina.html (24.09.19) Fa una molt bona explicació de la màquina Enigma.
- EL PERIÓDICO, trobats els jeroglífics monumentals més antics https://www.elperiodico.cat/ca/oci-i-cultura/20170622/jeroglifics-monumentals-egipcis-mes-antics-elkab-6122510 (01.10.19) Una notícia dels jeroglífics més antics trobats al sud de Luxor.
- VIQUIPÈDIA, Piedra de Rosseta https://es.wikipedia.org/wiki/Piedra_de_Rosetta (01.10.19) Explicació de la pedra Rosseta.