Desenvolupament d'un *plugin* per a Chrome per xifrar/desxifrar correus utilitzant Gmail

Enginyeria Tècnica d'Informàtica de Sistemes

Autor: Boris Martín Toral

Consultora: Cristina Pérez Solà

Data de lliurament: 13/06/2016

Índex

1 Introducció

Cada vegada s'utilitzen més els correus web, ja que, ofereixen una alta flexibilitat i un accés des de qualsevol dispositiu amb connexió a internet. A més, la majoria de tots els serveis de correu web son gratuïts i donen accés a altres serveis com emmagatzematge al núvol, gestió i edició de documents en línia, mapes i navegació, etc. Això, tot i semblar un avantatge molt gran, té un cost. Aquest cost no és econòmic, sinó que consisteix en la pèrdua de part de privacitat de les comunicacions entre els usuaris d'aquests serveis.

Tots aquests serveis comporten unes despeses de manteniment, electricitat, marketing, etc., per les empreses que els ofereixen; Aquestes despeses s'han de compensar d'alguna manera i, la manera més comú de fer-ho, és mitjançant la publicitat. Aquest model de negoci no és visible directament quan s'està utilitzant el correu web, però el proveïdor aprofita totes les dades que els usuaris proporcionen durant la seva sessió per tal de proporcionar una publicitat personalitzada en funció del contingut escrit, les cerques o, inclús, per proximitat a la localització de l'usuari, resultant, així, més eficaç i, per tant, més valuosa.

Per tant, el fet d'enviar un missatge i que ningú pugui llegir-lo, tret del destinatari, és gairebé impossible utilitzant aquests tipus de servei. Tanmateix, se suposa, que les companyies només llegeixen els correus amb la finalitat d'oferir una publicitat personalitzada, adaptada als interessos i necessitats de l'usuari i que ningú té accés a cap informació individualitzada. A més, el tractament de la informació queda molt ben especificat en els acords que tots els serveis fan llegir en el moment de donar-te d'alta, acords que, d'altra banda, hi ha poca tendència a llegir amb deteniment.

Potser en les comunicacions més habituals, no resulta tant important mantenir en secret el contingut dels missatges redactats. Però en el cas de missatges que contenen informació més sensible (documents personals, números de compte, etc), sí que apareix la necessitat de mantenir oculta la informació a tot aquell que no sigui el destinatari. És en aquests casos, on els serveis de correu web actual no proporcionen les eines necessàries.

2 Descripció del TFC

2.1 Objectiu

Davant la necessitat d'enviar missatges segurs, és a dir, que ningú, excepte el destinatari, pugui llegir el seu contingut, aquest TFC tractarà de posar a l'abast dels usuaris la funcionalitat de poder xifrar/desxifrar missatges en un dels correus webs més populars com és Gmail. A més, si es disposa del temps suficient, s'intentarà implementar també la possibilitat de poder signar missatges i poder validar aquesta signatura.

Per desenvolupar aquesta funcionalitat, es farà servir una extensió o *plugin* per a Chrome. Aquest navegador, desenvolupat per Google, permet estendre la seva funcionalitat d'una manera fàcil utilitzant llenguatges de programació molt comuns en aplicacions web, com són:

- HTML
- CSS
- Javascript

2.2 Metodologia

Per tal de realitzar el TFC en el temps establert, es farà una planificació inicial amb totes les tasques identificades prèviament. Tot i que s'intentarà seguir aquesta planificació inicial, val a dir que aquesta s'anirà actualitzant a mesura que el treball es vagi desenvolupant. És a dir, s'anirà actualitzant cada vegada que s'afegeixi una nova tasca que no estava prevista o quan hi hagi qualsevol endarreriment respecte al pla inicial.

Un cop feta la planificació de les tasques a realitzar, es passarà a l'anàlisi i disseny del treball. En aquesta fase s'analitzaran els requeriments amb l'objectiu d'elaborar l'arquitectura general de l'aplicació.

Més endavant, es durà a terme la fase d'implementació del projecte. S'haurà d'adquirir el coneixement necessari per desenvolupar extensions per a Chrome i implementar el disseny resultant de la fase anterior. A més, a mesura que el treball vagi avançant, s'haurà de començar a escriure la memòria del TFC.

Un cop acabada la implementació, s'haurà d'acabar la redacció de la memòria i lliurar el producte resultant del TFC, que serà l'extensió amb la funcionalitat descrita en les fases anteriors.

2.3 Descomposició d'activitats i planificació

Les activitats a realitzar per tal d'assolir els objectius anteriorment descrits, seran:

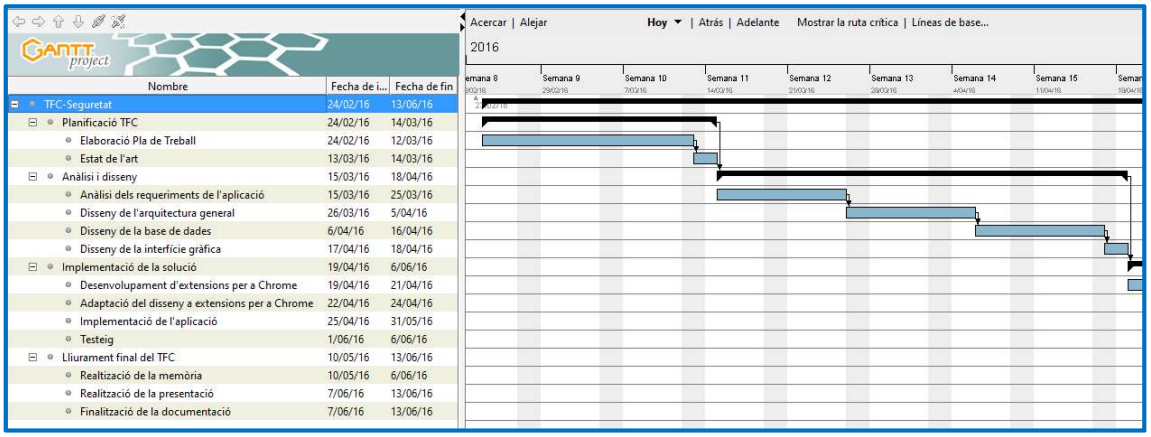
1. Revisió de l'estat de l'art

2. Anàlisi i disseny
   - Anàlisi del requeriments de l'aplicació
   - Disseny de l'arquitectura general
   - Disseny de la base de dades
   - Disseny de la interfície gràfica

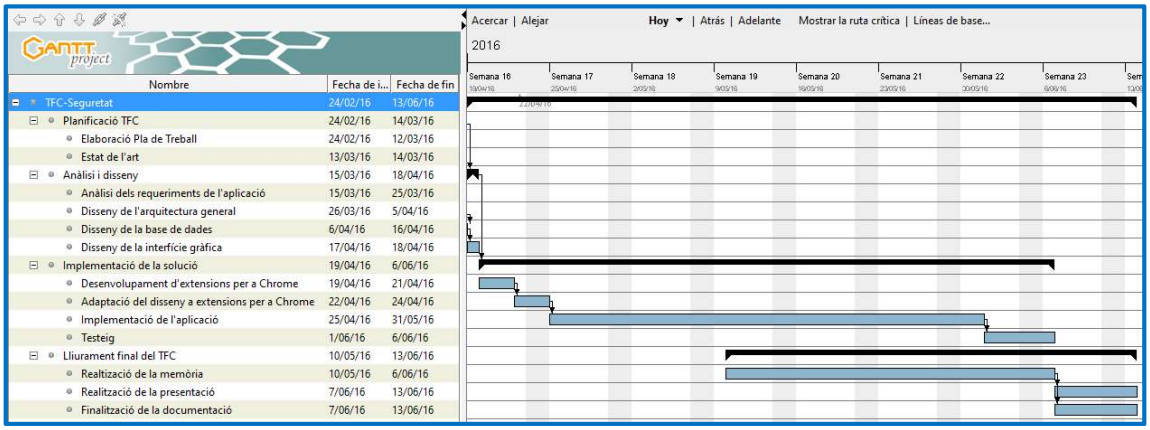
3. Implementació de la solució
   - Revisió documentació per desenvolupar extensions per a Chrome
   - Adaptació del disseny a les particularitats del desenvolupament d'extensions
   - Implementació de l'aplicació
   - Testeig

4. Lliurament final del TFC
   - Realització de la memòria
   - Realització de la presentació
   - Finalització de la documentació

Planificarem les diferents activitats segons el calendari marcat pel Pla Docent de l'assignatura. Això ens permetrà ajustar la durada de les activitats a les dades de lliurament de les diferents PAC's.



Nombre	Fecha de i...	Fecha de fin
TFC-Seguretat	24/02/16	13/06/16
Planificació TFC	24/02/16	14/03/16
Elaboració Pla de Treball	24/02/16	12/03/16
Estat de l'art	13/03/16	14/03/16
Anàlisi i disseny	15/03/16	18/04/16
Anàlisi dels requeriments de l'aplicació	15/03/16	25/03/16
Disseny de l'arquitectura general	26/03/16	5/04/16
Disseny de la base de dades	6/04/16	16/04/16
Disseny de la interfície gràfica	17/04/16	18/04/16
Implementació de la solució	19/04/16	6/06/16
Desenvolupament d'extensions per a Chrome	19/04/16	21/04/16
Adaptació del disseny a extensions per a Chrome	22/04/16	24/04/16
Implementació de l'aplicació	25/04/16	31/05/16
Testeig	1/06/16	6/06/16
Lliurament final del TFC	10/05/16	13/06/16
Realització de la memòria	10/05/16	6/06/16
Realització de la presentació	7/06/16	13/06/16
Finalització de la documentació	7/06/16	13/06/16



2.4 Producte obtingut

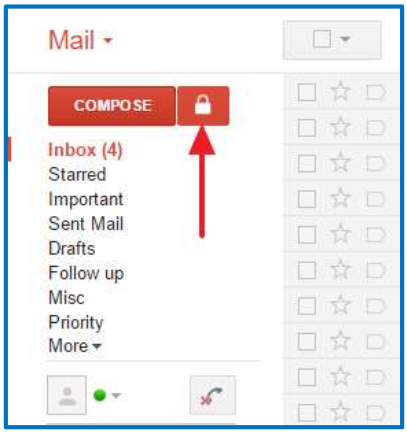
El resultat d'aquest projecte serà una extensió o plugin per a Google Chrome llesta per a instal·lar. Aquesta proporcionarà els elements necessaris per a poder intercanviar missatges de forma segura des de el correu web Gmail d'una manera fàcil i intuïtiva.

2.5 Estat de l'art

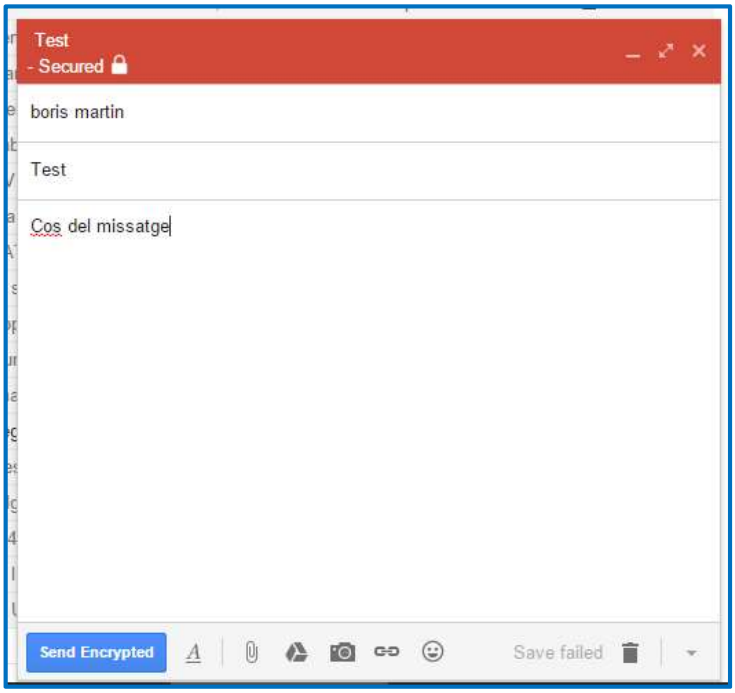
Abans de desenvolupar la nostra pròpia eina, revisarem si ja n'hi ha d'altres eines disponibles que puguin cobrir la mateixa necessitat, així com les diferents tecnologies o llibreries que ens permetran assolir el nostre objectiu.

SecureGmail (https://www.streak.com/securegmail)

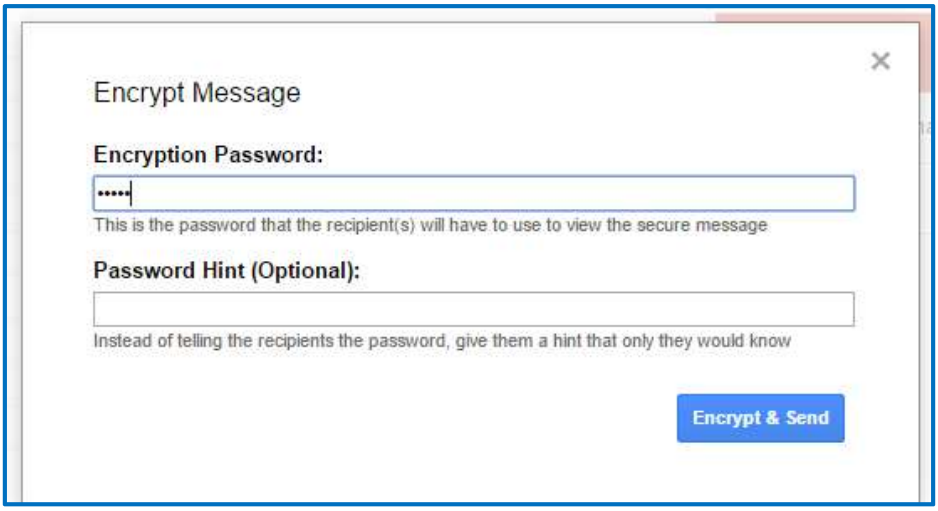
SecureGmail és una extensió per a Chrome que ofereix un xifrat simètric (la clau per xifrar i desxifrar missatges és la mateixa). La utilització d'aquesta extensió és molt senzilla. Primer s'ha d'instal·lar (un procés molt fàcil i molt ben documentat). Un cop instal·lat, apareix un cadenat a la vora del botó per redactar correus:



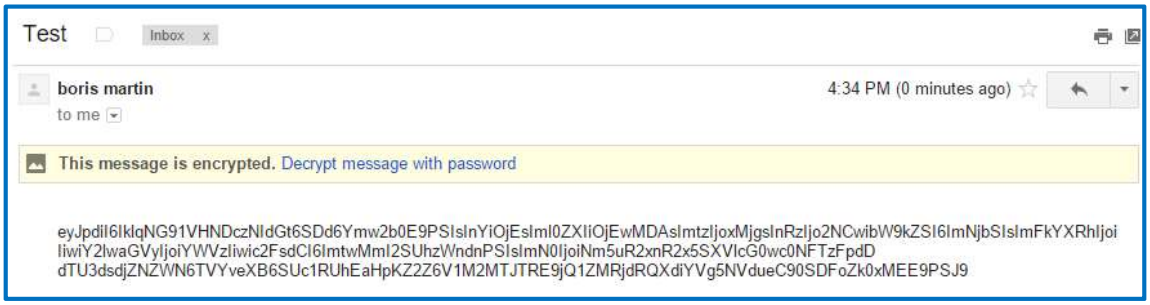
Si l'usuari vol enviar un correu xifrat, ha de polsar aquest botó i apareixerà la típica finestra d'edició

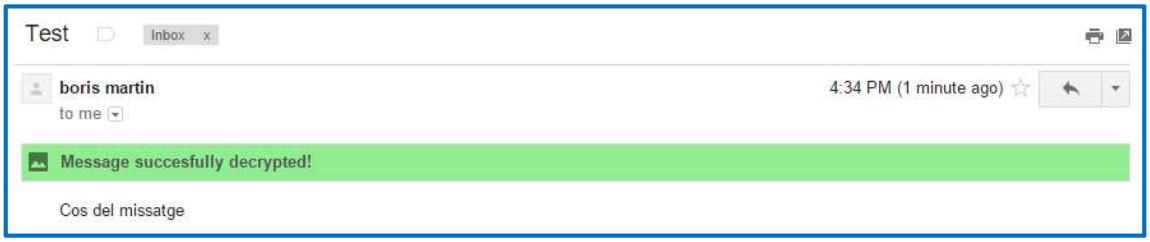


Just abans d'enviar el missatge, l'extensió demana el password de xifrat:



El receptor del missatge ho rep a la seva bústia i, si no hi introdueix el password correctament, no pot llegir el missatge:





Avantatges

1. Molt fàcil d'instal·lar i utilitzar.

Punts millorables

1. No permet gestionar les claus.
2. Utilitza un mecanisme de xifrat simètric. Per tant, emissor i receptor han d'utilitzar la mateixa clau per xifrar/desxifrar el missatge.
3. No proporciona cap mecanisme per a la transmissió de la clau de xifrat per un canal insegur

Mymail-Crypt for Gmail (http://prometheusx.net/)

Aquesta extensió implementa l'estàndard OpenPGP (Pretty Good Privacy) utilitzant la llibreria OpenPGP.js. Aquest estàndard utilitza un mecanisme de xifrat asimètric o de clau pública. Cada emissor disposa d'un parell de claus:

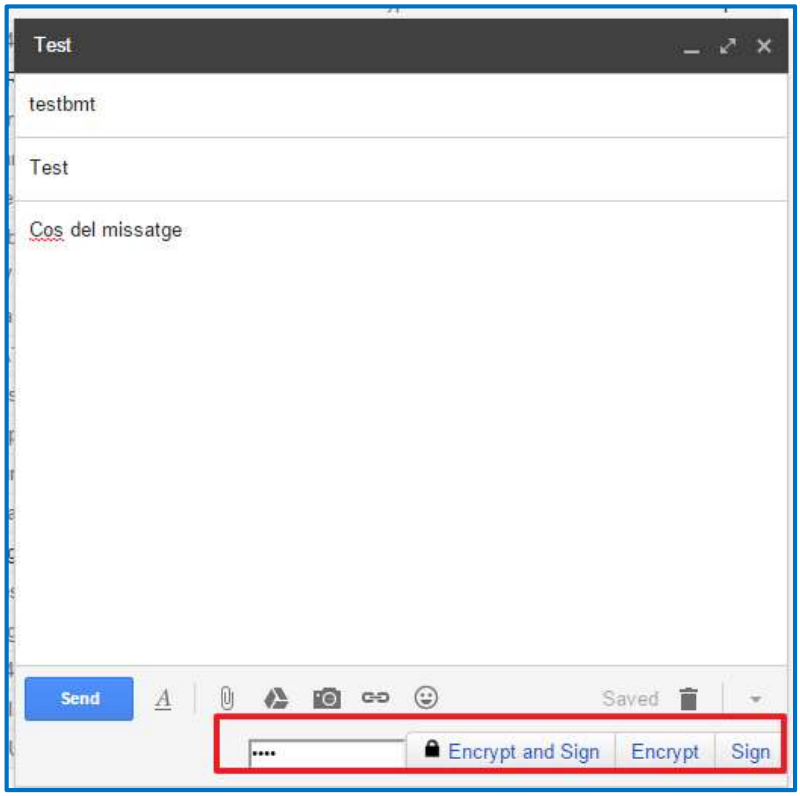
1. **Clau pública**: Clau que l'emissor pot enviar al receptor per un canal insegur sense perill que un tercer la pugui utilitzar per desxifrar el missatge.
2. **Clau privada**: Clau que l'emissor ha de mantenir en secret.

És una eina més completa que l'anterior ja que permet:

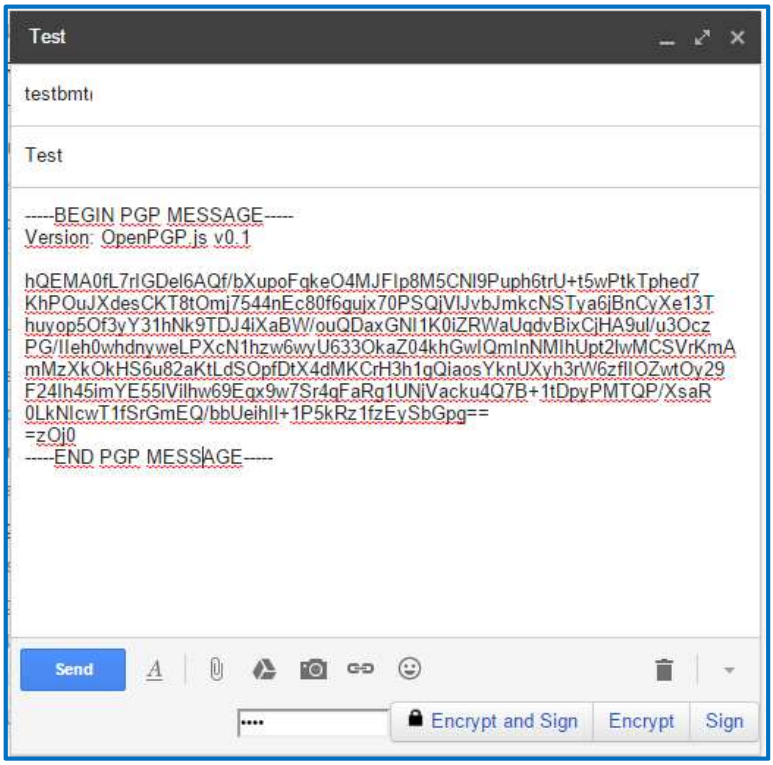
1. **Gestionar claus privades.**
2. **Gestionar claus públiques dels teus contactes.**

D'aquesta manera es soluciona el problema d'enviar la clau de xifrat per un canal insegur, ja que la clau pública la pot veure qualsevol.

La utilització d'aquesta extensió és una mica més complexa que l'anterior ja que requereix tenir cert coneixement del que significa el xifrat de clau pública. Tot i així, també n'és molt senzilla d'utilitzar. El primer que s'ha de fer és generar una clau per a l'emissor (la clau privada està protegida per contrasenya) i guardar la clau pública del destinatari a la pàgina de configuració. Un cop fet aquest pas previ, ja podem composar un missatge i veiem les opcions d'encriptació i signatura:



Per exemple, quan xifrem un missatge el receptor rebria un text amb el següent format:



Per tal de desxifrar el missatge, el receptor només ha de polsar el botó de desxifrat (prèviament ha de tenir la clau pública de l'emissor) i podrà accedir al cos del missatge en clar.

Avantatges

1. Utilització d'algoritmes de clau pública.
2. Permet el xifrat y signatura de missatges.
3. Permet gestionar les claus (generar i emmagatzemar).

Punts millorables

1. Interfície gràfica de configuració millorable.

3 Conceptes bàsics de criptografia

3.1 Una mica d'història

L'ús de la criptografia remunta a milers d'anys enrere. Des dels militars espartans de l'antiga Grècia, que utilitzaven un bastó o escítala per intercanviar missatges xifrats, fins als moderns sistemes de xifrat de clau pública actuals. L'avanç de l'electrònica i dels computadors, han permès passar de sistemes de xifrat senzills que utilitzaven paper i llapis a sistemes més elaborats d'una gran complexitat.

A continuació introduirem alguns del sistemes de xifrat més coneguts que s'han utilitzat al llarg dels anys.

3.1.1 Esteganografia

L'esteganografia tracta l'estudi i l'aplicació de tècniques que permeten ocultar missatges o objectes a dins d'uns altres, de manera, que la seva existència passi desapercebuda. Així, a diferència de la criptografia, si l'objecte o persona portadora del missatge és interceptat i el missatge és descobert, aquest n'és llegible directament.

Alguns exemples d'esteganografia són:

1. Heródoto, historiador i geògraf grec que va viure entre el 484 i el 425 a.C., relata en el seu llibre *Las Històrias* com un personatge havia rasurat el cabell d'un dels seus esclaus de confiança, li havia tatuat un missatge en el cuir cabellut, va esperar a que el cabell li tornès a créixer i el va enviar al receptor del missatge amb instruccions de que li havien de rasurar el cap. D'aquesta manera, si l'esclau era interceptat pel camí, el missatge estaria ocult sota el cabell i ningú no s'adonaria de la seva existència.

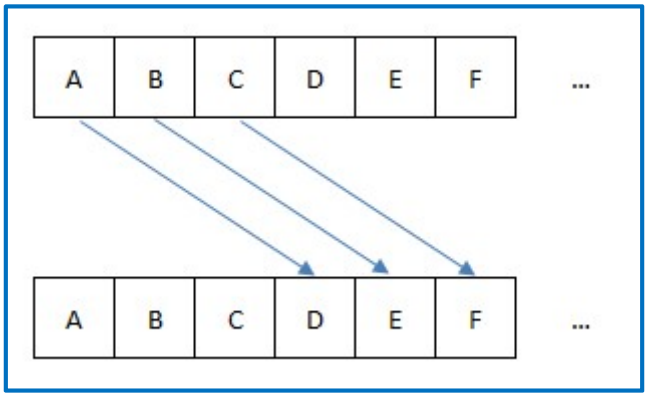
2. El científic italià Giovanni Battista della Porta (segle XV) va descobrir com ocultar un missatge dins un ou cuit. La tècnica consistia en escriure amb una tinta preparada amb alum i vinagre sobre la pela d'un ou. La tinta penetra i deixa un missatge a la superfície de l'albúmina de l'ou dur, que solament es pot llegir si es pela.

3. Al llarg de la història s'han utilitzat diferents tipus de tintes invisibles, com el suc de llimona o taronja, l'orina o la llet que, en escalfar la superfície on es va escriure el missatge, aquest n'apareix.

Actualment també s'utilitzen aquest tipus de tècniques per ocultar missatges en continguts digitals. Per exemple, es poden enviar missatges ocults en arxius de text, cançons, fotografies i vídeos.

3.1.2 Xifrat Cèsar

Aquest mètode de xifrat deu el seu nom a l'emperador romà Julio César, que l'utilitzava per comunicar-se amb els seus generals. Aquest sistema de xifrat mono alfabètic de substitució consistia en escriure el missatge amb un alfabet que estava format per les lletres de l'alfabet normal desplaçades tres posicions a la dreta.



D'aquesta manera, el missatge ABC seria transmès com DEF.

Quan el receptor del missatge el rebia, com que coneixia la clau secreta (l'alfabet desplaçat tres posicions a la dreta) podia fer el desplaçament invers i obtenir el missatge en clar.

3.1.3 Xifrat de Vigenère

El xifrat de Vigenère és un sistema de xifrat polí alfabètic de substitució. Utilitza com a alfabets les 26 permutacions circulars de l'alfabet al seu ordre habitual com es pot veure a la següent taula:

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Per xifrar un missatge es procedeix de la següent manera:

1. Es tria una paraula clau fàcil de recordar.
2. S'escriu la paraula clau sota el missatge a xifrar tantes vegades com sigui necessari.
3. Cada lletra del missatge a xifrar es codifica amb l'alfabet de la taula marcat per la lletra de la paraula clau.

D'aquesta manera si el missatge a xifrar és "Això és una prova":

1. La paraula clau serà TFC.
2. Escrivim la paraula clau sota el missatge.
3. Es substitueix cada lletra segons l'alfabet marcat per la paraula clau.

Missatge:	A	I	X	O	E	S	U	N	A	P	R	O	V	A
Clau:	T	F	C	T	F	C	T	F	C	T	F	C	T	F
Xifrat:	T	N	Z	H	J	U	N	S	C	I	W	Q	O	F

3.1.4 Màquina Enigma

Al 1918, els inventors alemanys Arthur Scherbius i Richard Ritter volien substituir els inadequats sistemes criptogràfics empleats durant la Primera Guerra Mundial. D'aquesta manera van inventar una màquina electromecànica que van denominar Enigma.

Aquesta màquina deu la seva fama a que fou adoptada per les forces militars alemanyes des de 1930 i molt intensament durant la Segona Guerra Mundial.

La màquina Enigma era composta en els seus inicis de tres parts fonamentals:

1. Teclat on era escrit el missatge a enviar.
2. Una unitat modificadora.
3. Un taulell on era mostrat el missatge xifrat.

Cada lletra del text a xifrar es polsava en el teclat i la unitat modificadora la transformava abans de mostrar-la en el taulell. Cada vegada que es polsava una lletra la unitat modificadora girava 1/26 voltes (per a un alfabet de 26 lletres). D'aquesta manera cada lletra introduïda seria xifrada amb un alfabet diferent de l'anterior.

Aquesta primera versió era equivalent a un xifrat de Vigenère de 26 lletres el qual era relativament fàcil de desxifrar. Per incrementar el nombre de claus per xifrar, es va afegir una segona unitat modificadora que girava una posició quan el primer disc donava una volta completa. Aquesta modificació donava a l'Enigma $26 \cdot 26 = 676$ claus per xifrar. Més tard se li va afegir una tercera unitat modificadora dotant-li de $26 \cdot 26 \cdot 26 = 17.576$ claus.

Per desxifrar els missatge rebuts, l'Enigma disposava d'un element més, el Reflector. Quan el missatge xifrat arribava al receptor, aquest disposava d'una altra màquina amb els rotors col·locats en la mateixa posició que la màquina emissora i, a través del Reflector, es desxifrava el missatge.

Posteriorment, se li van afegir dues característiques més que feien que l'Enigma oferís bilions de claus:

1. Rotors intercanviables, de manera que, en haver 6 formes possibles de col·locar els tres rotors, el nombre de claus augmenta.
2. Es va introduir un panell que permetia intercanviar parells de lletres en grups de sis.

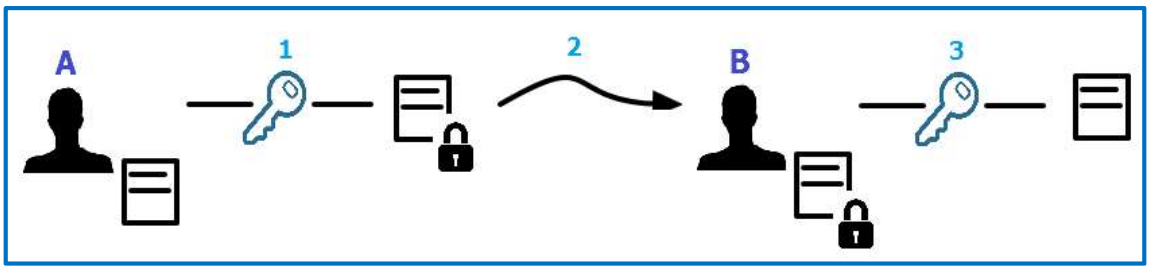
La màquina Enigma semblava indesxifrable però, degut a un error en l'enviament d'una màquina Enigma de Berlín a Varsòvia, els polonesos varen interceptar la màquina proporcionant una molt bona font d'informació. Més tard, davant de la manca de recursos dels polonesos per intentar desxifrar-la, els polonesos van compartir els seus avanços amb els francesos i els britànics, els quals, més tard, aconseguirien trencar el xifrat de l'Enigma.

3.2 Criptografia de clau simètrica

La criptografia de clau simètrica es basa en la utilització d'una sola clau per xifrar i desxifrar el missatge. El concepte de xifrat és molt senzill, donat un missatge en clar al què se li aplica un algoritme de xifrat, es genera un missatge xifrat que solament podrà ser desxifrat per aquells que coneixen l'algoritme i la clau de xifrat.

Els exemples comentats anteriorment com el xifrat Cèsar, el Vigenère o el proposat per la màquina Enigma, són xifrats de clau simètrica.

El procés de xifrat amb un algoritme de clau simètrica seria el següent:



1. L'usuari A envia un missatge xifrat a l'usuari B, xifrant el missatge.
2. L'usuari A envia el missatge i la clau perquè l'usuari B el pugi desxifrar.
3. L'usuari B desxifra el missatge amb la clau que ha rebut de l'usuari A i obté el missatge sense xifrar.

Exemples moderns de xifrat de clau simètrica són:

1. **DES**: L'any 1977, el *National Bureau of Standards* (NBS), una secció del Departament de Defensa dels EEUU, va publicar un criptosistema estàndard creat amb la finalitat de protegir qualsevol tipus de dades: el DES (*Data Encryption Standard*) amb la col·laboració de l'empresa IBM i la NSA *(National Security Agency*). Aquest criptosistema xifra blocs de dades de 64 bits de llargada mitjançant una clau de 56 bits.

2. **IDEA**: Més tard, a l'any 1990, J. Massey i X. Lai van desenvolupar el criptosistema IDEA. Aquests sistema xifra blocs de text en clar de 64 bits de llargada mitjançant una clau de 128 bits. El seu funcionament es basa en vuit iteracions idèntiques seguides d'una transformació de sortida.

3. **AES**: A l'any 2000 el NIST (*National Institute of Standards and Technology*) va escollir el criptosistema Rijndael com a AES (*Advanced Encryption Standard*) per la seva combinació de seguretat, rendiment, eficiència, flexibilitat i facilitat d'implementació. El criptosistema de Rijndael xifra blocs de text en clar de 128, 192 o 256 bits de longitud, mentre que la longitud de les claus de xifratge també pot variar de 128, 192 o 256 bits.

Els principals inconvenients de la criptografia de clau simètrica són:

1. **La distribució de claus**: Dos usuaris han d'escollir una clau secreta abans de començar a comunicar-se entre ells. En aquest cas, o bé s'han trobat personalment o bé han de confiar en un canal segur per distribuir les claus.

2. **La gestió de claus:** En una xarxa de N usuaris, cada parella d'usuaris ha de tenir la seva clau compartida particular, la qual cosa implica un total de N(N-1)/2 claus per a tota la xarxa.

3. **No hi ha signatura digital:** La signatura digital és l'equivalent a les signatures manuals. En un sistema de clau simètrica no hi possibilitat de signar els missatges pel fet de que totes les claus són compartides almenys per dos usuaris.

3.3 Criptografia de clau pública o asimètrica

El concepte de criptografia de clau pública, que permet superar els inconvenients comentats anteriorment, va ser proposat per W. Diffie i M.E. Hellman, l'any 1976. La idea era permetre un intercanvi segur de missatges entre emissor i receptor sense, ni tan sols, haver de trobar-se prèviament per acordar una clau secreta compartida.

La criptografia de clau pública o asimètrica basa el seu funcionament en què cada usuari ha de tenir una parella de claus:

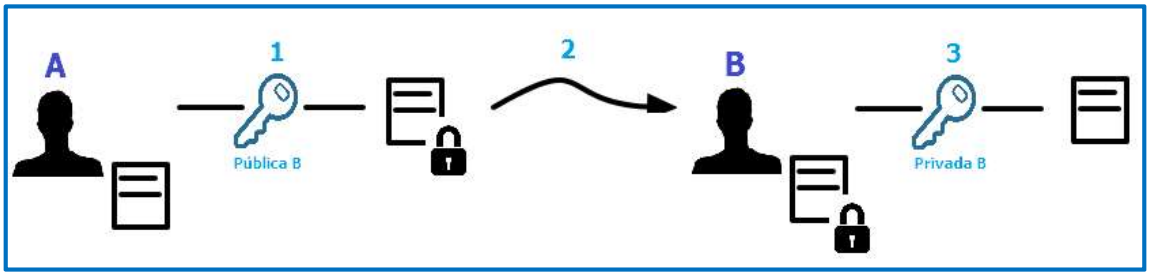
- **Clau pública**: Aquesta clau serà coneguda per tots els usuaris.

- **Clau privada**: Aquesta clau serà guardada pel seu propietari i no l'haurà de conèixer ningú altre.

Els criptosistemes de clau pública es basen en l'existència d'alguns tipus de funcions que són difícils d'invertir. És a dir, funcions que fàcilment es pot calcular la seva imatge per a un valor determinat, mentre que és difícil calcular aquest valor coneixent la seva imatge.

D'aquesta manera es pot calcular fàcilment la clau pública a partir de la clau privada però, és computacionalment molt costós trobar la clau privada a partir de la pública. Això vol dir, que si disposéssim d'un ordinador amb una potència de càlcul molt gran, aquests sistemes no funcionarien ja que seria relativament fàcil conèixer la clau privada de l'usuari. Ara bé, com que la potència de càlcul dels ordinadors actuals és limitada, el temps necessari per trobar la clau privada és molt gran en relació a la duració de la clau (per exemple, si s'utilitza un parell de claus que es canvien cada poc temps, calcular la clau privada a partir de la pública, costaria X anys, està clar que això no és una limitació).

El procés de xifratge amb aquest sistema és el següent:



1. L'usuari A vol enviar un missatge xifrat a l'usuari B. Per això, xifra el missatge amb la clau pública de l'usuari B.
2. L'usuari A envia el missatge xifrat per un canal insegur
3. L'usuari B rep el missatge xifrat amb la seva clau pública i el desxifra amb la seva clau privada, obtenint així, el missatge en clar.

Alguns exemples de criptosistemes de clau pública són:

- **RSA**: El criptosistema RSA va ser publicat per Rivest, Shamir i Adleman el 1978 en l'article "*A method for obtaining digital signatures and públic/key cryptosystems*". Aquest criptosistema basa la seva seguretat en el problema de la factorització. La clau pública i privada es calculen mitjançant l'elecció de dos nombres primers de manera que la seva factorització sigui el més difícil possible.

- **ElGamal**: A l'any 1985 T. ElGamal, va publicar aquest criptosistema de clau pública basat en l'exponenciació discreta sobre un grup multiplicatiu Z_p^* on p és un nombre primer gran (almenys 400 dígits). La seguretat d'aquest mètode de xifrat es basa en el problema del logaritme discret.

3.4 Signatura digital

Com hem comentat abans la criptografia de clau simètrica tenia l'inconvenient de que no es podia utilitzar per signar missatges, ja que la clau era compartida per almenys dos usuaris. Així, la criptografia de clau pública permet que un usuari signi un missatge de tal manera que la signatura pot ser verificada més tard per qualsevol persona.

Per signar un missatge l'usuari fa servir la seva clau privada. D'altra banda, per verificar una signatura, qualsevol pot fer servir la clau pública del signatari. A més, amb aquest procediment aconseguim:

1. **Autenticació**: La firma digital és equivalent a la firma física d'un document.

2. **Integritat**: El missatge no podrà ser modificat pel camí. Qualsevol modificació del missatge farà que la signatura calculada pel destinatari no coincideixi per l'enviada pel signatari.

3. **No repudi**: El signatari no pot repudiar més tard el fet d'haver signat el missatge, ja que ningú tret del signatari no té la clau privada necessària per produir la signatura.

4 Conceptes bàsics del desenvolupament de plugins per a Google Chrome utilitzats al treball

Els plugins o extensions són petits programes que permeten modificar i millorar la funcionalitat del navegador Google Chrome. Les tecnologies involucrades en el desenvolupament de plugins per a Chrome són HTML, Javascript i CSS.

Google ofereix el Chrome Web Store per poder publicar i distribuir les extensions escrites pels usuaris.

Cada extensió té els següents arxius:

- L'arxiu de manifest
- Un o més fitxers HTML
- Opcional: Un o més fitxers Javascript
- Opcional: Qualsevol altre arxiu que l'extensió necessiti (imatges, llibreries, etc)

4.1 Arxiu de manifest

L'arxiu de manifest dóna informació sobre l'extensió, com per exemple els fitxers més importants i les capacitats del navegador que l'extensió pot utilitzar. El format d'aquest fitxer és JSON.

Per a més informació sobre l'arxiu de manifest es pot consultar el següent enllaç:

https://developer.chrome.com/extensions/manifest

4.2 Opcions del plugin

Per permetre personalitzar el comportament de l'extensió als usuaris, l'extensió pot proporcionar una pàgina d'opcions. Si s'especifica una pàgina d'opcions a l'arxiu de manifest, l'opció de configuració apareixerà a l'extensió, obrint en una nova pestanya la pàgina HTML especificada.

Per a més informació sobre la pàgina d'opcions de les extensions es pot consultar el següent enllaç:

https://developer.chrome.com/extensions/options

4.3 Content Scripts

Els anomenats *Content Scripts* són fitxers Javascript que s'executen en el context de pàgines web. Utilitzant l'estàndard *Document Object Model* (DOM) aquests fitxers poden llegir i/o modificar les pàgines que visita el navegador.

Per exemple els *Content Scripts* poden:

- Trobar URLs sense enllaçar a les pàgines web i convertir-los en híper enllaços.
- Augmentar la mida de la lletra perquè el text sigui més llegible o modificar el color o la imatge de fons.
- Afegir contingut HTML dinàmic en funció de certa lògica.

Per ampliar la informació sobre els *Content Scripts* es pot consultar el següent enllaç:

https://developer.chrome.com/extensions/content_scripts

4.4 Background o Event Pages

Les pàgines *Background* o *Event* són scripts que s'executen en fons i permeten gestionar tasques o l'estat de l'extensió. La diferència principal entre una *Event page* i una de *Background* és que les primeres solament es carreguen quan es necessiten. Quan una *Event page* no està executant alguna tasca activament, la pàgina és descarrega alliberant memòria i recursos del sistema. Per aquest motiu, són especialment interessants per al seu ús en dispositius de baix consum d'energia.

Per a més informació sobre aquest tipus d'elements es pot consultar el següent enllaç:

https://developer.chrome.com/extensions/event_pages

5 Anàlisi i disseny funcional del plugin

Un cop hem definit la planificació del TFC, analitzarem els requeriments del nostre plugin. L'anàlisi contindrà tots els requeriments desitjables del nostre plugin. Els classificarem per prioritats per tal de poder implementar un plugin amb les funcionalitats bàsiques i ampliar-lo posteriorment si hi ha temps.

Després d'analitzar els requeriments passarem a definir el disseny del plugin per tal de satisfer tots els requeriments. Descriurem detalladament els elements necessaris per tal de poder gestionar l'enviament de missatges xifrats.

5.1 Anàlisi dels requeriments

Per tal de poder prioritzar els requeriments pensant en la seva implementació, assignarem una prioritat a cadascun dels requeriments. Bàsicament, hi haurà dues prioritats:

Prioritat	Descripció
1	Funcionalitat bàsica i imprescindible.
2	Funcionalitat addicional no necessària per al funcionament bàsic

Un cop definides les prioritats, recollim en una llista els requeriments:

Prioritat	Identificador	Requeriment
1	R1	Gestió de claus
1	R2	Xifrat de missatges
1	R3	Desxifrat de missatges
2	R4	Signatura de missatges
2	R5	Verificació de la signatura

5.1.1 R1 – Gestió de Claus

El tipus de xifrat que implementarà el plugin estarà basat en criptografia de clau pública o asimètrica. Aquest tipus de xifrat, a part d'assegurar la privacitat del nostre missatge, facilita l'autenticació del missatge mitjançant la signatura digital. Per tant, l'aplicació haurà de permetre:

1. **Generació de claus pública i privada**: Haurà de permetre generar parells de claus per poder xifrar i desxifrar missatges. Generalment aquesta opció servirà perquè l'emissor del missatge pugui començar a utilitzar l'intercanvi segur de missatges o també per poder crear parells de claus per a diferents usuaris i després distribuir-les (per un canal segur evitant així que algú pugui interceptar la clau privada).

2. **Importació de claus públiques**: Haurà de permetre importar la clau pública dels diferents receptors. D'aquesta manera quan xifrem un missatge, s'utilitzarà la clau corresponent al receptor.

5.1.2 R2 – Xifrat de missatges

Per dur a terme l'intercanvi de missatges de forma segura, l'aplicació haurà de tenir l'opció de xifrar un missatge. L'usuari podrà xifrar un missatge abans d'enviar-lo.

5.1.3 R3 – Desxifrat de missatges

Quan l'usuari rebi un missatge xifrat, tindrà l'opció de desxifrar-lo per poder llegir-lo en text clar.

5.1.4 R4 – Signatura de missatges

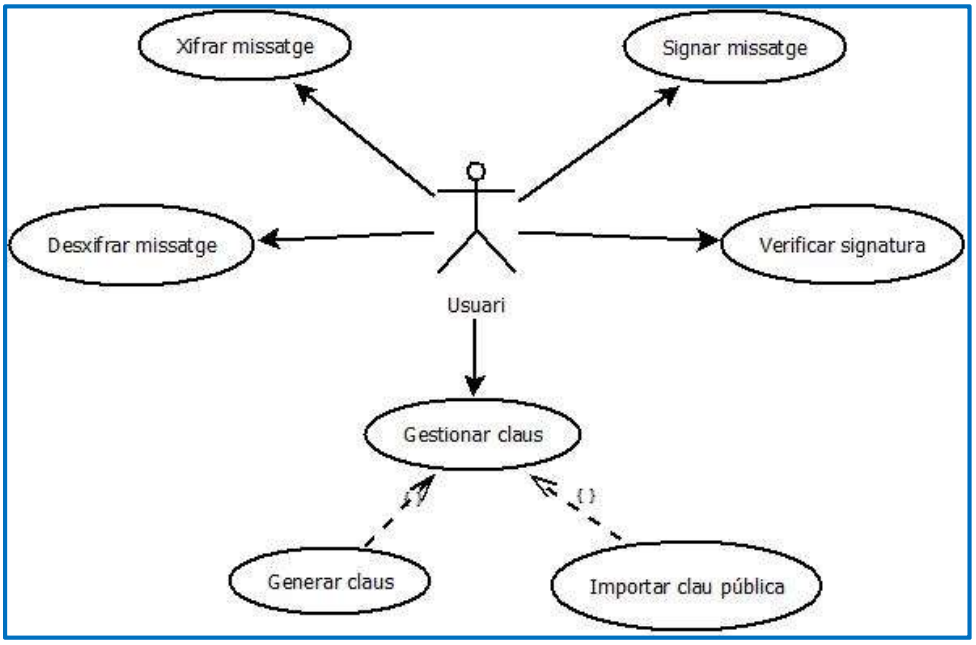
Per tal de poder assegurar l'autenticitat i la integritat del missatge, l'aplicació donarà l'opció de signar-lo digitalment.

5.1.5 R5 – Verificació de la signatura

L'aplicació permetrà verificar la signatura del missatge rebut. D'aquesta manera es podrà verificar que l'emissor és realment qui diu que és (no repudi) y que el missatge no ha estat modificat pel camí (integritat).

5.2 Diagrama de casos d'ús

El següent diagrama de casos d'ús descriu les diferents accions que l'usuari podrà fer un cop s'hagi identificat a l'aplicació de Gmail.



Xifrar missatge

Cas d'ús	Xifrar missatge
Actors	Usuari
Precondició	1. S'ha d'haver emplenat un receptor 2. S'ha d'haver emplenat el cos del missatge
Postcondició	1. El cos del missatge és xifrat amb la clau corresponent al receptor
Propòsit	
Xifrar el missatge abans de ser enviat	
Resum	
L'usuari tindrà l'opció d'enviar el missatge xifrat polsant el botó corresponent	

Desxifrar missatge

Cas d'ús	Desxifrar missatge
Actors	Usuari
Precondició	1. S'ha d'haver rebut un missatge xifrat
Postcondició	1. El missatge es desxifra amb la clau corresponent al remitent
Propòsit	
Desxifrar missatges rebuts	
Resum	
L'usuari tindrà l'opció de desxifrar un missatge polsant el botó corresponent	

Signar Missatge

Cas d'ús	Signar missatge
Actors	Usuari
Precondició	1. S'ha d'haver emplenat el cos del missatge
Postcondició	1. El missatge es signa amb la clau privada de l'emissor
Propòsit	

Signar missatges per assegurar la integritat i l'autenticitat del missatge
Resum
L'usuari tindrà l'opció de signar els missatges per tal d'assegurar la seva integritat i autenticitat

Verificar signatura

Cas d'ús	Verificar signatura missatge
Actors	Usuari
Precondició	1. S'ha d'haver rebut un missatge signat
Postcondició	1. Es verifica la signatura amb la clau pública de l'emissor
Propòsit	
Verificar la signatura d'un missatge per tal d'assegurar la integritat i l'autenticitat del missatge	
Resum	
L'usuari tindrà l'opció de verificar la signatura del missatge rebut polsant el botó corresponent.	

Gestionar claus

Cas d'ús	Generar claus
Actors	Usuari
Precondició	1. Emplenar formulari amb els següents camps: - Correu electrònic - Paraula clau per a la clau privada - Longitud de la clau
Postcondició	1. Es genera un parell de claus (privada i pública) associades al correu electrònic introduït
Propòsit	
Generar parells de claus i associar-les a un correu electrònic	
Resum	
Es podran generar parells de claus i associar-les a un correu electrònic per tal de poder intercanviar missatges de forma segura.	

Cas d'ús	Importar clau pública
Actors	Usuari
Precondició	1. Emplenar camp amb la clau pública del receptor
Postcondició	1. Es guarda la clau pública associada al mail del receptor
Propòsit	
Generar parells de claus i associar-les a un correu electrònic	
Resum	
Es podran generar parells de claus i associar-les a un correu electrònic per tal de poder intercanviar missatges de forma segura.	

5.3 Disseny de la base de dades

Per tal d'evitar afegir complexitat al TFC, s'utilitzarà l'emmagatzematge al client (utilitzant HTML5 Local Storage). D'aquesta manera les claus quedaran emmagatzemades al navegador de l'usuari. Aquesta aproximació té les següents avantatges i inconvenients:

Avantatges:

1. S'evita la necessitat d'instal·lar i dissenyar una base de dades, disminuint així la complexitat de la solució.
2. Les dades emmagatzemades al Local Storage no surten mai del client (a diferència de las cookies).

Inconvenients:

1. És l'opció més insegura. Les claus privades queden emmagatzemades al navegador de l'usuari. Aquestes claus podrien ser consultades per qualsevol amb un script.
2. No es cobreix la distribució de les claus privades. S'hauran de buscar alternatives segures per poder distribuir aquestes claus (en cas que vulguem gestionar claus centralitzadament).

5.4 Disseny de la interfície gràfica

La interfície gràfica de la nostra aplicació estarà dividida en dues parts:

1. **Content Script**: Aquest element, propi del desenvolupament de plugins per a Chrome, són fitxers JavaScript que s'executen en el context d'una pàgina web. Proporcionant, així, accés a l'arbre DOM (Document Object Model) podent llegir o modificar les seves propietats. El plugin desenvolupat contindrà un content script que afegirà la funcionalitat requerida, així com els elements gràfics (botons, capses de text, etc) a la pàgina de Gmail.

2. **Pàgina de configuració del plugin**: Els plugins per a Chrome, poden disposar d'una pàgina de configuració per tal de configurar certes funcionalitats del plugin. El plugin desenvolupat contindrà una pàgina de configuració que s'utilitzarà per a la gestió de claus.

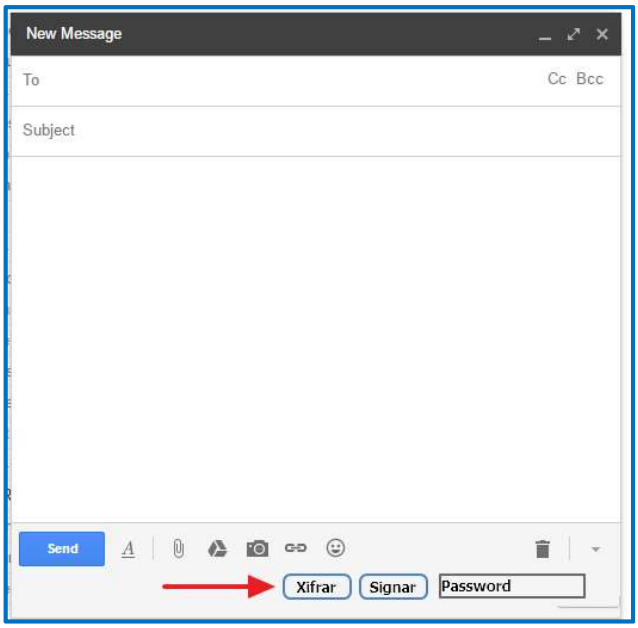
Content Script

Xifrar i signar: Per poder xifrar i signar els missatges enviats, afegirem els següents elements a la pàgina de Gmail:

1. Botó per xifrar el missatge.
2. Botó per signar el missatge.

3. Capsa de text per introduir la paraula clau per poder accedir a la clau privada de l'emissor.

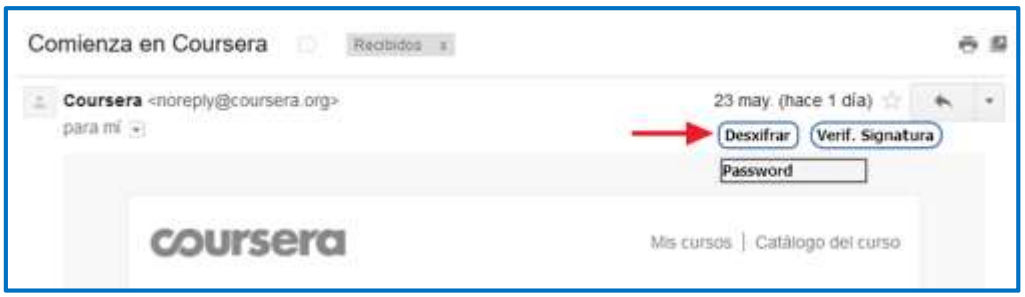
La disposició aproximada dels elements serà la següent:



Desxifrar i verificar signatura: Per poder desxifrar i verificar la signatura dels missatges rebuts, afegirem els següents elements a la pàgina de Gmail:

1. Botó per desxifrar el missatge
2. Botó per verificar la signatura del missatge

La disposició aproximada dels elements serà la següent:



Pàgina de configuració del plugin

En la pàgina de configuració del plugin es podran gestionar les claus dels diferents contactes. Per això, es disposarà d'una pàgina amb el següent menú

1. **Inici**: En aquest apartat s'introduirà l'objectiu de la pàgina de configuració i una breu descripció del què es pot fer.

2. **Gestió de claus**: Aquesta secció mostrarà un llistat de les claus guardades prèviament. A més disposarà de tres opcions:

    a. **Generar claus**: Permetrà generar un parell de claus nou. Per crear-la serà necessari omplir un petit formulari amb els camps següents:

        i. Nom
        ii. Correu electrònic
        iii. Paraula clau
        iv. Longitud de la clau

    Un cop generada la clau s'afegirà al llistat comentat anteriorment.

    b. **Importar clau pública**: Permetrà afegir la clau pública d'un contacte mitjançant un camp de text.

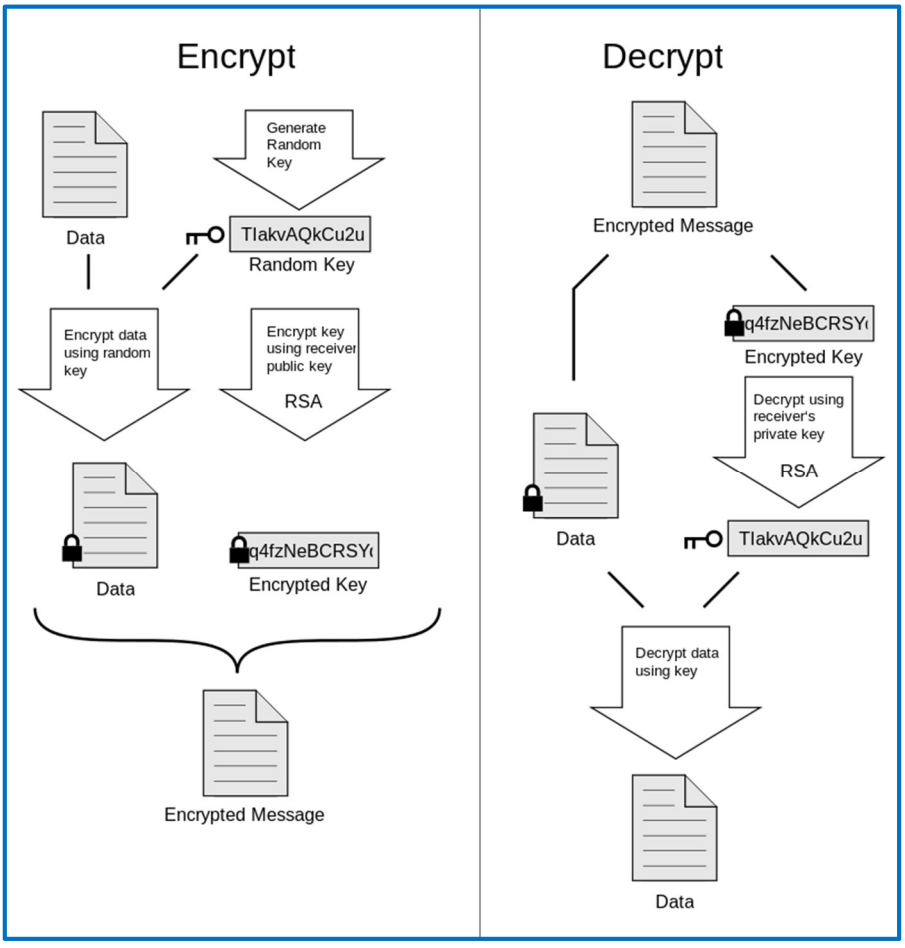
6 Disseny tècnic de la solució

6.1 Funcionament del xifrat escollit (OpenPGP)

El xifrat escollit per al plugin desenvolupat a aquest TFC és OpenPGP. Aquest criptosistema està basat en el PGP (*Pretty Good Privacy*) que va ser dissenyat i desenvolupat per Phil Zimmermann al 1991. Degut a l'àmplia acceptació d'aquest sistema per intercanviar informació de forma segura, es va proposar a la IETF (*Internet Enginnering Task Force*) l'estàndard OpenPGP.

Aquest criptosistema combina tècniques de criptografia simètrica i asimètrica per aprofitar els avantatges de cadascuna d'elles. El xifrat simètric és més ràpid que el asimètric, mentre que el segon, soluciona el problema de la distribució de la clau de forma segura i garanteix l'autenticitat i la integritat del missatge.

El procés de xifrat i desxifrat d'un missatge amb aquest criptosistema és el següent:



Font: https://es.wikipedia.org/wiki/Pretty_Good_Privacy

Xifrat

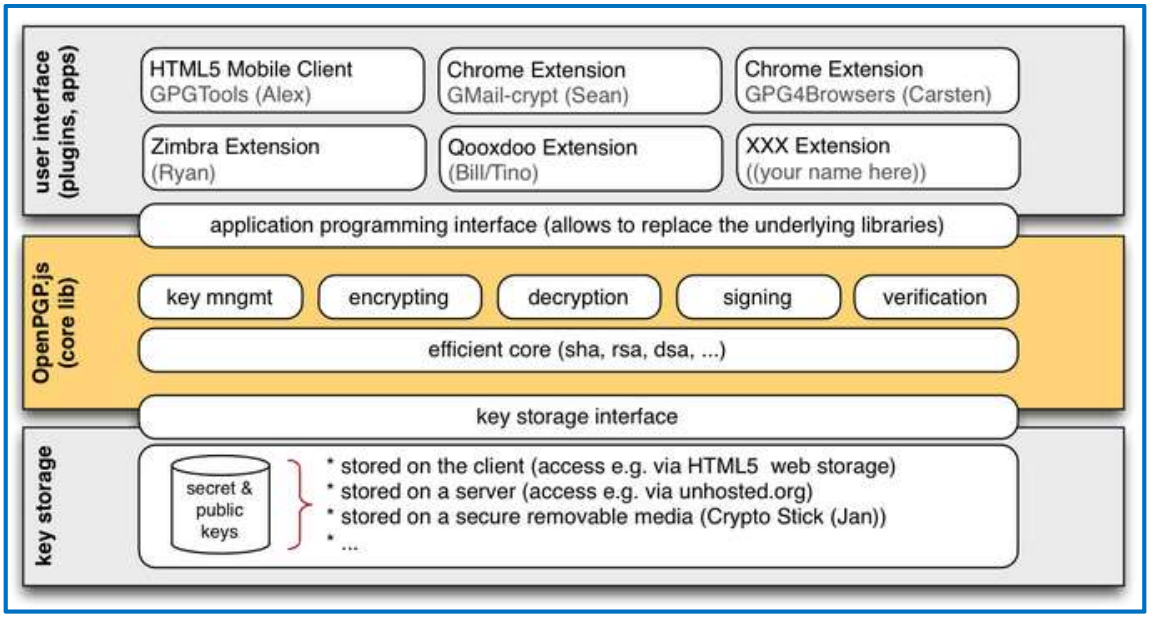
1. Es genera una clau aleatòria.
2. Es xifra el missatge a enviar amb un algoritme simètric (Triple DES, IDEA) utilitzant la clau generada al pas anterior.
3. Es xifra la clau utilitzada per xifrar el missatge amb la clau pública del receptor.
4. S'envia el missatge (missatge xifrat + clau xifrada) al receptor.

Desxifrat

1. El receptor separa la clau simètrica del missatge xifrat.
2. Utilitza la seva clau privada per obtenir la clau simètrica utilitzada per xifrar el text.
3. Un cop calculada la clau simètrica, pot desxifrar el text i obtenir-ne el text en clar.

6.2 OpenPGP.js: Implementació Javascript de codi obert

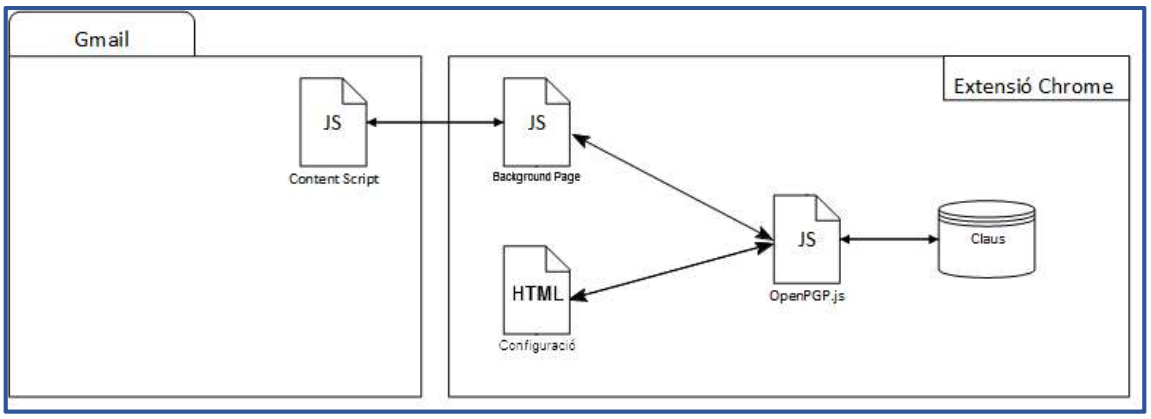
La llibreria Javascript OpenPGP.js (https://github.com/openpgpjs/openpgpjs) proporciona una implementació de codi obert del criptosistema OpenPGP. Com es pot veure a la següent figura:



Font: https://github.com/openpgpjs/openpgpjs/wiki/Introduction#overview

Aquesta llibreria proporciona tota la funcionalitat requerida per a la nostra extensió.

6.3 Arquitectura del plugin



Tal y com podem observar a la figura anterior, l'extensió està composta dels següents elements:

1. **Content Script**: S'encarrega d'afegir tots els elements HTML necessaris a la pàgina de Gmail i de manegar els seus events. Es comunica amb la pàgina de background mitjançant l'API de Chrome chrome.extension.sendRequest.

2. **Background Page**: S'encarrega d'inicialitzar i carregar els elements necessaris de OpenPGP.js per a poder gestionar el xifrat, desxifrat i la signatura de missatges.

3. **Pàgina de configuració**: Eina que permet gestionar les claus dels diferents contactes. Emmagatzema aquestes claus al LocalStorage del navegador.

4. **LocalStorage**: Aquesta característica del navegador permet emmagatzemar grans quantitats de dades localment al navegador, evitant transferir les dades al servidor. Aquí es guarden les claus públiques i privades (xifrades per un password que es demana quan es genera la clau).

Addicionalment, s'utilitzen les següents llibreries de codi obert per a facilitar diferents aspectes del desenvolupament:

JQuery

Aquesta llibreria JQuery facilita la manipulació dels elements HTML mitjançant una API molt fàcil d'utilitzar que funciona a tots els navegadors. Principalment s'ha fet servir per manipular l'arbre DOM (Document Object Model) als tres elements principals de l'extensió.

Lodash

Aquesta llibreria Javascript facilita el treball amb arrays, nombres, strings, objectes, etc.

Sanitize-html

Llibreria que permet netejar el codi HTML d'elements o etiquetes no vàlides. La fem servir per a netejar el resultat de xifrar/desxifrar el missatge per evitar etiquetes no vàlides.

Bootstrap

És un framework que utilitza HTML, CSS y Javascript per a desenvolupar aplicacions web responsives (adaptables a tot tipus de dispositius). S'ha fet servir sobretot en el disseny de la pàgina de configuració tot i que s'han fet servir algunes característiques aïllades al content script per a mostrar missatges modals per exemple.

7 Testeig del plugin

NOTA: La signatura digital de missatges i la posterior verificació de la signatura no s'ha pogut implementar per manca de temps. D'aquesta manera solament s'ha testejat la funcionalitat bàsica de xifrar i desxifrar missatges.

Un cop s'ha desenvolupat l'extensió, s'ha passat una bateria de proves per assegurar el bon funcionament de tots els components. Per tal de facilitar la realització de les proves les separarem per funcionalitat. Tot seguit, podem veure els passos de test executats i el seu resultat. A l'apartat d'annexos es poden veure les captures de pantalla corresponents a cada pas.

7.1 Xifrat de missatges

Pas	Descripció	Resultat esperat	Resultat obtingut	Estat OK/NOK
1	Botó de xifrat	Al redactar un correu en Gmail, ha d'aparèixer el botó de xifrat a la barra d'eines de la finestra de redacció	Apareix el botó correctament	OK
2	Xifrar un missatge per a un destinatari que no tenim la seva clau pública	Missatge d'error advertint de que no es pot trobar la clau del destinatari	Missatge d'error correcte	OK
3	Xifrat d'un missatge per a un destinatari que tenim la seva clau pública	El contingut del missatge és xifrat i substituït per un missatge PGP	El missatge és xifrat	OK

7.2 Desxifrat de missatges

Pas	Descripció	Resultat esperat	Resultat obtingut	Estat OK/NOK
4	Botó de desxifrat	Al llegir un correu, ha d'aparèixer un botó per a desxifrar i una capsa de text per introduir la contrasenya de la clau privada de l'usuari	Apareix el camp per introduir la contrasenya i el botó per a desxifrar	OK
5	Desxifrat d'un missatge no xifrat	Missatge d'error advertint que no s'ha pogut trobar un missatge PGP	Missatge d'error apareix correctament	OK
6	Desxifrat d'un	El missatge és	Missatge desxifrat	OK

	missatge xifrat introduint la contrasenya correcta	desxifrat correctament i es pot veure el text en clar	correctament	
7	Desxifrat d'un missatge xifrat introduint una contrasenya incorrecta	Missatge d'error advertint de que no s'ha pogut accedir a la clau privada de l'usuari	Missatge correcte	OK

7.3 Gestió de claus

Pas	Descripció	Resultat esperat	Resultat obtingut	Estat OK/NOK
8	Accés a la pàgina de configuració de l'extensió visible	Al clicar sobre la icona de l'extensió, ha de aparèixer habilitada la opció de configuració	Apareix l'opció habilitada	OK
9	La pàgina de configuració s'ha d'obrir al polsar el botó de configuració	La pàgina de configuració s'obre en una nova pestanya.	La pàgina s'obre en una nova pestanya	OK
10	Menú de la pàgina de configuració	Han d'aparèixer dues opcions, "Inici" i "Gestió de claus"	Opcions apareixen correctament	OK
11	Pàgina inici	Ha d'aparèixer una breu explicació del funcionament de la gestió de claus	Apareix l'explicació	OK
12	Pàgina gestió de claus	Ha d'aparèixer una taula, amb les claus per a cada usuari, i dos botons, generar parell de claus i importar clau pública	Apareix la taula i els dos botons	OK
13	Generar parell de claus	Si no s'omplen tots els camps del formulari (nom, email, contrasenya) ha d'aparèixer missatge de error	Apareix el missatge d'error	OK
14	Generar parell de claus	S'introdueix un email que no estigui ben format, ha d'aparèixer un missatge d'error	Apareix el missatge d'error	OK
15	Generar parell de claus	S'introdueix un password de menys de 8 caràcters,	Apareix el missatge d'error	OK

		missatge d'error		
16	Generar parell de claus	Introduïm totes les dades correctament. Ha d'aparèixer un missatge advertint de que s'ha generat un nou parell de claus i s'ha d'afegir a la taula	La taula de claus es refresca correctament	
17	Importar clau pública	S'introdueix una clau pública no vàlida, ha d'aparèixer missatge d'error	Apareix missatge d'error correcte	OK
18	Importar clau pública	Al introduir una clau pública vàlida, s'ha d'afegir un registre a la taula amb el nom i email corresponents	La taula es refresca correctament	OK

8 Conclusions i línies de treball futur

Aquest Treball Final de Carrera ens ha permès participar en un projecte des de la fase de presa de requeriments inicial fins a la fase de testeig. En concret ens ha permès:

1. **Inici de projecte:** Hem pogut definir el projecte i establir el seu abast.

2. **Planificació:** Hem pogut descompondre el projecte en activitats i planificar la seva execució temporal, establint fites assolibles. D'aquesta manera el seguiment posterior del projecte ha estat més fàcil.

3. **Anàlisi i disseny:** Hem pogut analitzar les necessitats funcionals de la nostra extensió, definir el comportament i aparença que hauria de tenir i, un cop revisada tota la documentació sobre el desenvolupament d'extensions per a Chrome, hem pogut establir l'arquitectura tècnica necessària de la nostra extensió.

4. **Implementació:** Ens ha permès afermar els coneixements en HTML, CSS i Javascript, així com també la utilització de llibreries Javascript molt utilitzades en el desenvolupament web (Jquery, Bootstrap, Lodash, etc). A més, hem pogut combinar totes aquestes eines en l'elaboració de l'extensió, obtenint així el producte requerit.

5. **Testeig:** Ens ha permès definir i executar els testejos necessaris per assegurar el correcte funcionament de la nostra extensió.

Com a contrapunt, la manca de temps per a la realització del projecte no ens ha permès implementar totes les funcionalitats definides a l'inici del projecte. Tot i que, preveient aquesta situació, vam assignar prioritats a cadascun dels requeriments. Això ens ha permès construir l'extensió des de les funcionalitats més bàsiques per assegurar un funcionament mínim.

En quant a les línies de treball futur, podem veure els següents punts millorables:

1. **Implementar la signatura digital i la seva verificació:** Tal i com hem comentat anteriorment, no hem disposat del temps necessari per a implementar la signatura digital de missatges i la seva verificació. És per això, que la primera línia de treball seria acabar d'implementar aquestes funcionalitats.

2. **Configuració de la llibreria OpenPGP per al xifrat de missatges:** Actualment la nostra extensió utilitza la configuració per defecte d'OpenPGP.js. Aquesta llibreria suporta diferents algoritmes de xifrat que poden ser configurats. Es podria afegir una pàgina de configuració per tal de que l'usuari pugui establir la configuració del xifrat desitjada.

3. **Emmagatzematge de les claus en un servidor de claus:** Actualment la nostra extensió fa servir HTML Local Storage per emmagatzemar tant la clau pública com la clau privada. Una possible millora d'aquest sistema seria la

implementació de la cerca i publicació de les claus públiques dels usuaris en un servidor de claus. D'aquesta manera l'intercanvi de les claus públiques entre els usuaris d'aquesta extensió seria transparent i milloraria la usabilitat de l'extensió.

4. **Xifrat d'imatges:** Actualment l'extensió suporta solament text (amb formats bàsics com negreta, cursiva, etc). Si inserim al missatge una imatge, aquesta es perd. Es podria estudiar la forma d'enviar les imatges xifrades i desxifrar-les correctament al destinatari.

9 Bibliografia

https://es.wikipedia.org/wiki/Historia_de_la_criptograf%C3%ADa

https://es.wikipedia.org/wiki/Esc%C3%ADtala

https://es.wikipedia.org/wiki/Esteganograf%C3%ADa

https://es.wikipedia.org/wiki/Her%C3%B3doto

http://www.egov.ufsc.br/portal/sites/default/files/la_criptografia_desde_la_antigua_grecia_hasta_la_maquina_enigma1.pdf

http://www.dma.fi.upm.es/recursos/aplicaciones/matematica_discreta/web/aritmetica_modular/cesar.html

http://roble.pntic.mec.es/jgad0020/cripto/vigenere.php

https://es.wikipedia.org/wiki/Enigma_%28m%C3%A1quina%29

https://developer.chrome.com/extensions

https://es.wikipedia.org/wiki/Pretty_Good_Privacy

https://tools.ietf.org/html/rfc4880

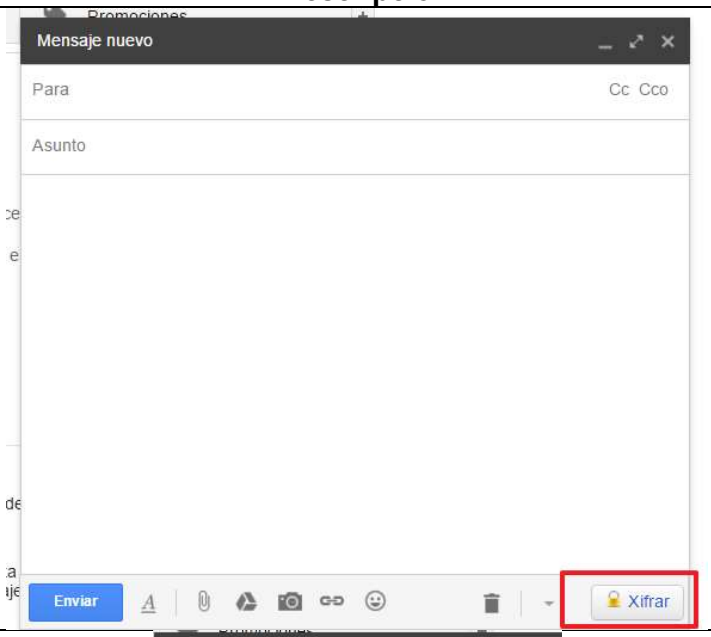
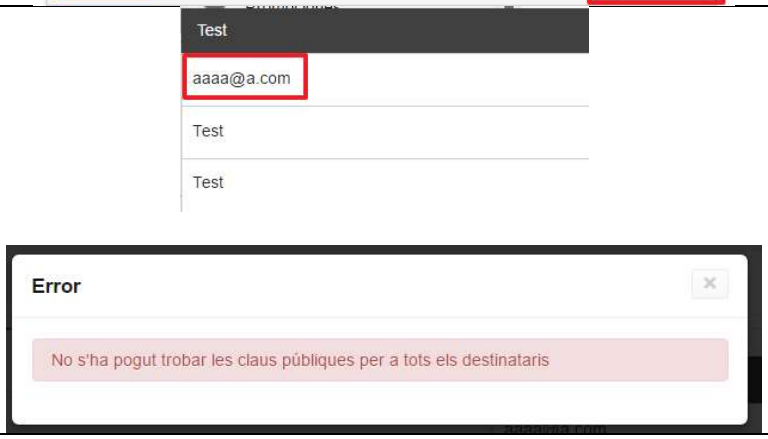
http://www.pgpi.org/doc/pgpintro/

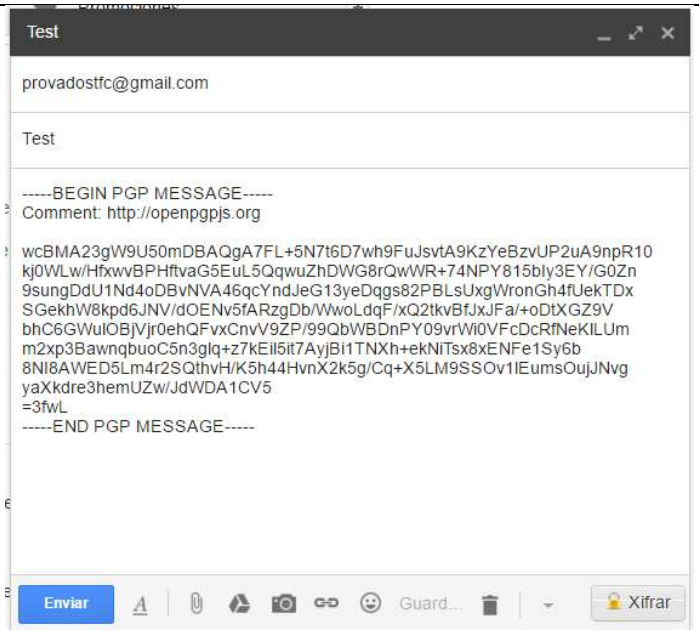
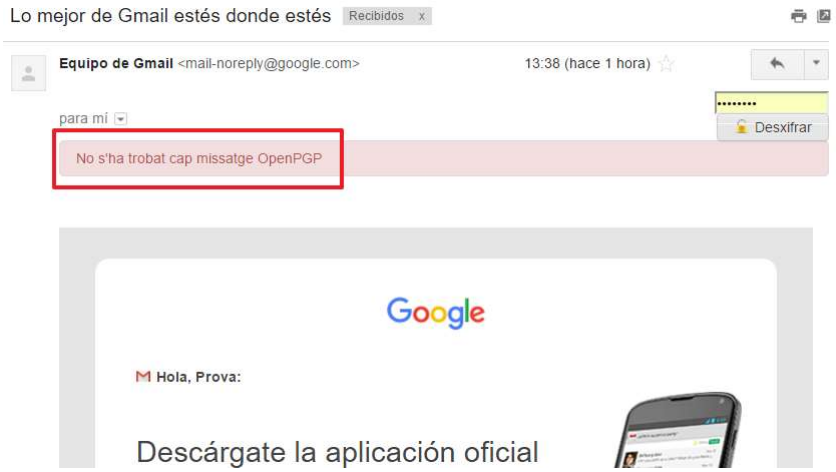
Jordi Herrera Joancomartí (UOC). "Xifres de clau compartida: xifres de bloc".

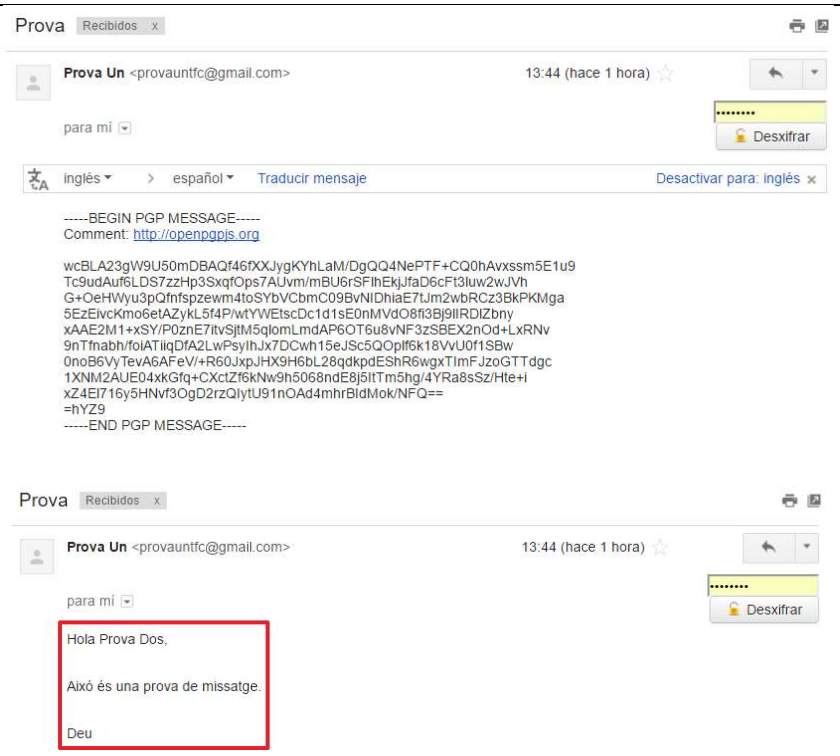
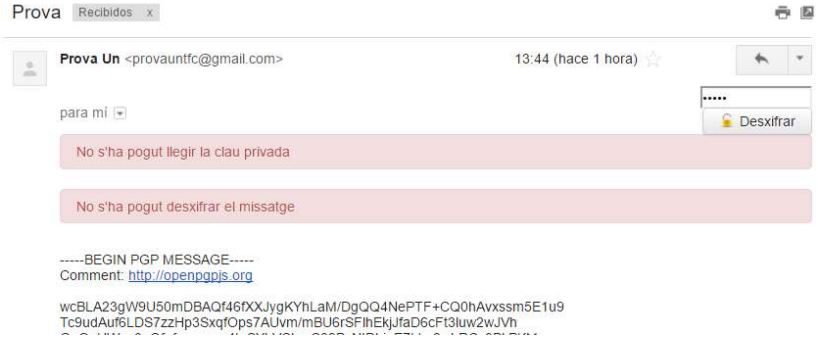
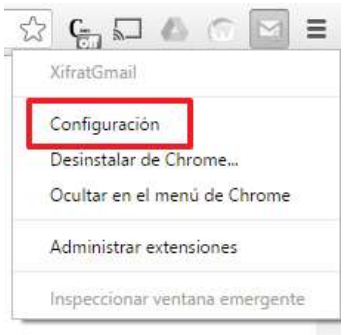
Josep Domingo Ferrer (UOC). "Xifres de clau pública".

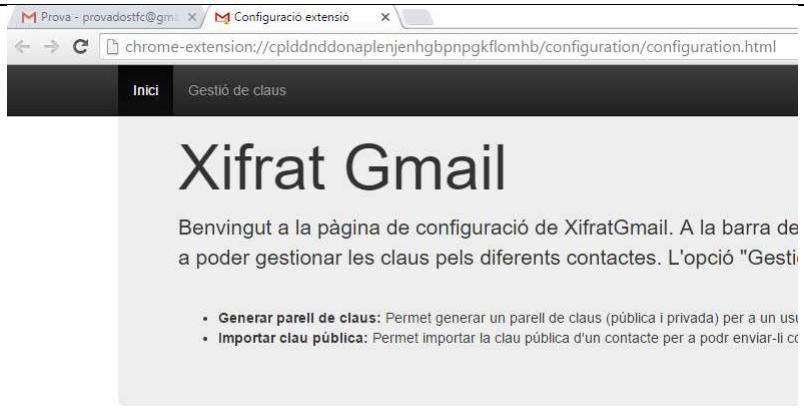
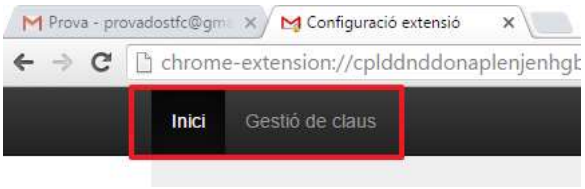
10 Annexos

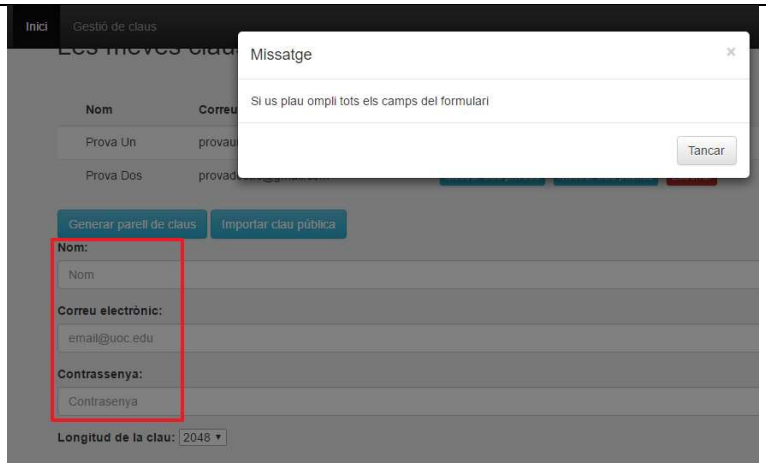
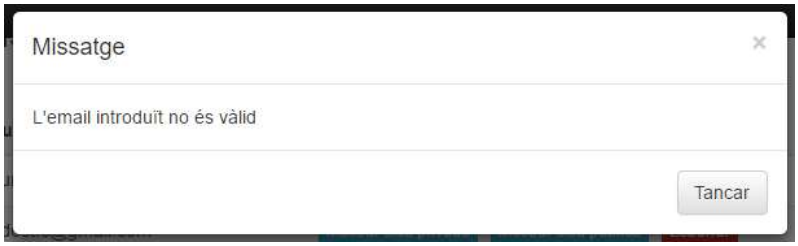
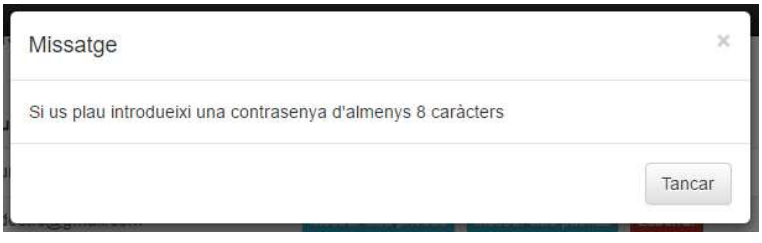
10.1 Captures de pantalla resultants del testeig

Pas	Descripció
1	
2	
3	

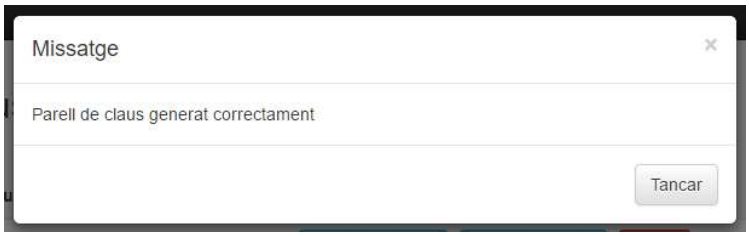
	 Test provadostfc@gmail.com Test -----BEGIN PGP MESSAGE----- Comment: http://openpgpjs.org wcBMA23gW9U50mDBAQgA7FL+5N7t6D7wh9FuJsvtA9KzYeBzvUP2uA9npR10 kj0WLw/HfxwvBPHftvaG5EuL5QqwuZhDWG8rQwWR+74NPY815bIy3EY/G0Zn 9sungDdU1Nd4oDBvNVA46qcYndJeG13yeDqgs82PBLsUxgWronGh4fUekTDx SGekhW8kpd6JNV/dOENv5fARzgDb/WwoLdqF/xQ2tkvBfJxJFa/+oDtXGZ9V bhC6GWulOBjVjr0ehQFvxCnvV9ZP/99QbWBDnPY09vrWi0VFcDcRfNeKILUm m2xp3BawnqbuoC5n3glq+z7kEil5it7AyjBi1TNXh+ekNiTsx8xENFe1Sy6b 8NI8AWED5Lm4r2SQthvH/K5h44HvnX2k5g/Cq+X5LM9SSOv1IEumsOujJNvg yaXkdre3hemUZw/JdWDA1CV5 =3fwL -----END PGP MESSAGE----- Enviar Guard... Xifrar
4	 Prova Recibidos Prova Un <provauntfc@gmail.com> 13:44 (hace 1 hora) para mí Desxifrar inglés español Traducir mensaje Desactivar para: inglés
5	 Lo mejor de Gmail estés donde estés Recibidos Equipo de Gmail <mail-noreply@google.com> 13:38 (hace 1 hora) para mí Desxifrar No s'ha trobat cap missatge OpenPGP Google Hola, Prova: Descárgate la aplicación oficial
6	

	 Prova Recibidos x Prova Un <provauntfc@gmail.com> 13:44 (hace 1 hora) para mí Desxifrar inglés español Traducir mensaje Desactivar para: inglés -----BEGIN PGP MESSAGE----- Comment: http://openpgpjs.org wcBLA23gW9U50mDBAQf46fXXJygKYhLaM/DgQQ4NePTF+CQ0hAvxssm5E1u9 Tc9udAuf6LDS7zzHp3SxqfOps7AUvm/mBU6rSFlhEkjJfaD6cFt3luw2wJVh G+OeHWyu3pQfnfspzewm4toSYbVCbmC09BvNIDhiaE7tJm2wbRCz3BkPKMga 5EzEivcKmo6etAZykL5f4P/wtYWEtscDc1d1sE0nMVdO8fi3Bj9IIRDIZbny xAAE2M1+xSY/P0znE7itvSjtM5qlomLmdAP6OT6u8vNF3zSBEX2nOd+LxRNv 9nTfnabh/foIATiiqDfA2LwPsyIhJx7DCwh15eJSc5QOplf6k18VvU0f1SBw 0noB6VyTevA6AFeV/+R60JxpJHX9H6bL28qdkpdEShR6wgxTImFJzoGTTdgc 1XNM2AUE04xkGfq+CXctZf6kNw9h5068ndE8j5ItTm5hg/4YRa8sSz/Hte+I xZ4El716y5HNvf3OgD2rzQIytU91nOAd4mhrBldMok/NFQ== =hYZ9 -----END PGP MESSAGE----- Prova Recibidos x Prova Un <provauntfc@gmail.com> 13:44 (hace 1 hora) para mí Desxifrar Hola Prova Dos, Això és una prova de missatge. Deu
7	 Prova Recibidos x Prova Un <provauntfc@gmail.com> 13:44 (hace 1 hora) para mí Desxifrar No s'ha pogut llegir la clau privada No s'ha pogut desxifrar el missatge -----BEGIN PGP MESSAGE----- Comment: http://openpgpjs.org wcBLA23gW9U50mDBAQf46fXXJygKYhLaM/DgQQ4NePTF+CQ0hAvxssm5E1u9 Tc9udAuf6LDS7zzHp3SxqfOps7AUvm/mBU6rSFlhEkjJfaD6cFt3luw2wJVh
8	 XifratGmail Configuración Desinstalar de Chrome... Ocultar en el menú de Chrome Administrar extensiones Inspeccionar ventana emergente
9	

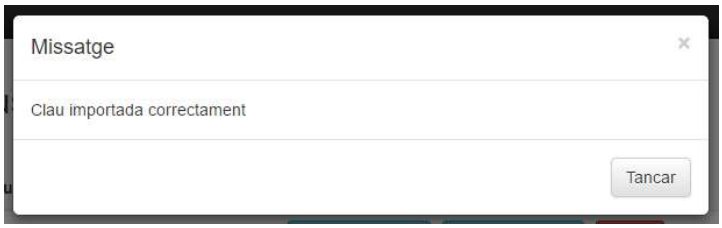
	 Prova - provadostfc@gm Configuració extensió chrome-extension://cpldndnddonaplenjenhgbpnpgkflomhb/configuration/configuration.html Inici Gestió de claus Xifrat Gmail Benvingut a la pàgina de configuració de XifratGmail. A la barra de a poder gestionar les claus pels diferents contactes. L'opció "Gesti • Generar parell de claus: Permet generar un parell de claus (pública i privada) per a un us • Importar clau pública: Permet importar la clau pública d'un contacte per a podr enviar-li c
10	 Prova - provadostfc@gm Configuració extensió chrome-extension://cpldndnddonaplenjenhgb Inici Gestió de claus
11	 Inici Gestió de claus Xifrat Gmail Benvingut a la pàgina de configuració de XifratGmail. A la barra de navegació superior es troba el menú per a poder gestionar les claus pels diferents contactes. L'opció "Gestió de claus" permet: • Generar parell de claus: Permet generar un parell de claus (pública i privada) per a un usuari mitjançant un formulari • Importar clau pública: Permet importar la clau pública d'un contacte per a podr enviar-li correus electrònics xifrats
12	 Inici Gestió de claus Les meves claus Nom Correu electrònic Prova Un provauntfc@gmail.com Mostrar clau privada Mostrar clau pública Esborrar Prova Dos provadostfc@gmail.com Mostrar clau privada Mostrar clau pública Esborrar Generar parell de claus Importar clau pública
13	

	 Inici Gestió de claus Missatge Si us plau ompli tots els camps del formulari Tancar Nom Correu Prova Un Prova Dos Generar parell de claus Importar clau pública Nom: Nom Correu electrònic: email@uoc.edu Contrassenya: Contrasenya Longitud de la clau: 2048
14	 Nom: Nom1 Correu electrònic: nom.com Contrassenya: Longitud de la clau: 2048  Missatge L'email introduït no és vàlid Tancar
15	 Nom: Nom1 Correu electrònic: nom1@test.com Contrassenya: Longitud de la clau: 2048  Missatge Si us plau introdueixi una contrasenya d'almenys 8 caràcters Tancar
16	

<table>
<tr><td></td><td> 




</td></tr>
<tr><td>17</td><td> 
</td></tr>
<tr><td>18</td><td> 
</td></tr>
</table>


Missatge
Clau importada correctament
Tancar


Nom
Correu electrònic
Prova Un
provauntfc@gmail.com
Mostrar clau privada
Mostrar clau pública
Esborrar
Prova Dos
provadostfc@gmail.com
Mostrar clau privada
Mostrar clau pública
Esborrar
Nom1
nom1@test.com
Mostrar clau privada
Mostrar clau pública
Esborrar
Nom2
nom2@test.com
Mostrar clau pública
Esborrar