UOCrypt:
Gestor de contrasenyes d'escriptori amb funcions de sincronització.

Carles Suria Marquez.
Enginyeria Tècnica d'Informàtica de Sistemes.

Consultor: Cristina Pérez Solà.
13/06/2014

A la meva família i amics, per tot el temps que els he robat.

A l'Antònia, per la seva col·laboració durant
la fase de transició d'aquest projecte.

A tots els consultors i tutor, per la seva paciència i ajuda
que durant tots aquests anys m'han donat.

Resum del projecte.

Aquest projecte correspon a un Treball Final de Carrera d'Enginyeria Tècnica d'Informàtica de Sistemes, àrea de Seguretat Informàtica, corresponent a la realització d'un gestor de contrasenyes d'escriptori amb funcions de sincronització.

Al llarg d'aquest text s'analitzarà que és un gestor de contrasenyes així com les principals característiques i funcions que aquests solen oferir per a continuació, desenvolupar-ne un seguint totes les etapes del cicle de vida d'un programari.

S'estudiarà també el concepte de xifrat i diferents criptosistemes, especialment l'AES, que serà l'utilitzat en aquest projecte.

Començarem elaborant el pla de treball on definirem els objectius, la metodologia i la planificació temporal a més d'estudiar quines tecnologies i altres treballs similars existeixen a l'actualitat.

Seguirem amb la fase d'elaboració on es recolliran els requisits del programari, tot elaborant els diagrames necessaris (diagrames de casos d'ús i de classes), s'estudiaran quines llibreries seran necessàries per implementar el xifrat/desxifrat així com el mecanisme de sincronització i es dissenyarà la interfície d'usuari.

Continuarem amb la descripció de la implementació realitzada, centrant-nos en les parts fonamentals com són les funcions criptogràfiques, la generació de contrasenyes segures, l'anàlisi de contrasenyes per a determinar-ne la seva qualitat, la sincronització de la base de dades perquè pugui estar actualitzada quan s'empra des de més d'un equip i la gestió de la interfície d'usuari.

Per acabar, explicarem les proves realitzades per a verificar el funcionament correcte de l'aplicació i les millores introduïdes a partir de la fase de transició, tot extraient les conclusions oportunes.

Paraules clau: Seguretat Informàtica, Criptografia, Xifrat, Desxifrat, AES, Contrasenya, Criptosistema.

Índex de continguts

Índex de figures

1 Introducció.

1.1 El gestor de contrasenyes.

Començarem aquest projecte definint que és un gestor de contrasenyes i descrivint els dos tipus principals que existeixen.

1.1.1 Definició.

Un gestor de contrasenyes és un programari que s'utilitza per desar parelles usuari/contrasenya mitjançant una base de dades xifrada amb una clau mestra, de manera que aquesta és l'única que l'usuari ha de memoritzar. Això facilita l'administració de les contrasenyes permetent als usuaris triar-ne de més complexes sense por de no recordar-les més endavant.

Sovint els gestors de contrasenyes ofereixen l'opció de generar-ne d'aleatòries, la qual cosa ajuda a evitar que s'utilitzi una mateixa clau per a accedir a diferents recursos, pràctica que és molt poc recomanable.

En el cas de que l'usuari opti per assignar la seva pròpia clau, els gestors de contrasenyes acostumen a incorporar un analitzador de la seva fortalesa. Cal remarcar que la clau mestra triada ha de ser suficient forta per assegurar que és difícil de trencar ja que si això es produís un atacant tindria accés a totes les contrasenyes desades en la base de dades.

Els gestors de contrasenyes també són útils com a mesura de defensa contra el "Phishing" degut a que una màquina mai confondrà dues pàgines semblants però amb diferent domini, garantint així que només s'introduiran les credencials en pàgines legítimes.

1.1.2 Tipus.

Existeixen dos tipus principals de gestors de contrasenyes: d'escriptori i en línia, cada un dels quals aporta els seus avantatges.

Amb els gestors en línia es pot accedir a les credencials des de qualsevol lloc amb l'únic requeriment d'un dispositiu que implementi un navegador web i tingui accés a Internet. En cas de caiguda de la xarxa la informació no estarà disponible.

Els gestors d'escriptori sempre tenen accés a la informació (la base de dades és local) però requereixen la instal·lació del programari i a més, en cas d'utilització des de més d'un dispositiu, la informació pot quedar fragmentada, incompleta i desactualitzada. Per evitar aquest problema, se solen implementar funcions de sincronització mitjançant la xarxa.

Per aquest treball optarem per desenvolupar una aplicació d'escriptori implementant les pertinents funcions de sincronització.

1.2 Objectius.

A continuació descriurem els objectius que pretenem assolir a la finalització d'aquest projecte.

1.2.1 Objectiu principal.

A la finalització d'aquest projecte s'espera tenir desenvolupat i totalment funcional un gestor de contrasenyes d'escriptori que implementi les funcions més habituals en aquest tipus de programari tal i com s'ha descrit en l'apartat anterior. El xifratge es farà mitjançant AES, permetent a l'usuari triar la longitud de la clau entre les tres possibles (128, 192 o 256 bits). Les contrasenyes en clar no podran estar allotjades en cap moment a la memòria persistent de l'ordinador (disc dur, memòries usb, etc.) per a evitar possibles intents de recuperació. L'aplicació haurà de permetre utilitzar la base de dades des de més d'un dispositiu (sincronització).

1.2.2 Objectius secundaris.

- Dissenyar una interfície gràfica amb una bona usabilitat.
- Treballar les llibreries de criptografia de Java.
- Treballar funcions de sincronització.

1.3 Productes obtinguts.

A la finalització d'aquest projecte s'ha obtingut UOCrypt, un gestor de contrasenyes plenament funcional que implementa les característiques principals d'aquest tipus de programari com ara el xifrat de la base de dades quan es desa al disc, generació de contrasenyes automàtiques, anàlisi de contrasenyes i sincronització de la base dades quan aquesta s'empra des de més d'un equip.

1.4 Breu descripció dels altres capítols de la memòria.

En els capítols que seguiran a continuació podrem trobar, en primer lloc, el pla de treball on explicarem la metodologia emprada per al desenvolupament d'aquest projecte, definirem les tasques que caldrà realitzar i la seva planificació temporal, i descriurem l'estat de l'art.

Continuarem explicant en detall les fases d'elaboració (recollida de requisits i elaboració del diagrama de casos d'ús i la documentació textual), disseny (diagrama de classes i disseny de la interfície d'usuari), implementació (procediments de xifrat i sincronització), construcció (desenvolupament i joc de proves) i transició.

Seguirem amb la descripció de les conclusions extretes de l'elaboració d'aquest projecte i acabarem amb la inclusió d'un glossari amb la definició dels termes més importants i la bibliografia consultada per a l'elaboració d'aquest Treball Final de Carrera.

2 Pla de treball.

2.1 Metodologia.

Per a dur a terme aquest projecte s'optarà per un un cicle de vida Rational Unified Process on distingirem les següents fases:

Inici: En aquesta fase s'ha delimitat l'abast del projecte.

Elaboració: S'estudiarà el domini del problema essent la recollida de requisits junt amb l'anàlisi i disseny els components principals d'aquesta fase.

Construcció: Durant aquesta fase es desenvoluparà el producte de manera iterativa i incremental satisfent les necessitats de l'arquitectura obtinguda en la fase anterior. El components principals seran la realització i la prova.

Transició: Es lliurarà el producte a un client fictici per a la seva avaluació. Pot ser que calgui fer retocs com a conseqüència d'errors o afegir noves funcions.

2.2 Llistat de tasques a realitzar.

Tot seguit detallarem el conjunt de tasques a realitzar en cada una de les etapes anteriors:

2.2.1 Fase d'elaboració.

- Analitzar diferents programaris ja existents per a obtenir un llistat de funcions necessàries.
- Crear el diagrama de casos d'us per satisfer els requisits obtinguts.
- Elaborar la documentació textual dels casos d'ús.
- Especificar les classes d'anàlisi.
- Cercar les llibreries criptogràfiques necessàries.
- Cercar un mecanisme de sincronització.
- Cercar les llibreries necessàries per a la sincronització.
- Dissenyar la interfície d'usuari.

2.2.2 Fase de construcció.

- Implementar el disseny anterior.
- Realitzar un conjunt de proves per a verificar el funcionament correcte del programari.

2.2.3 Fase de transició.

- Lliurar una versió preliminar del programari a un client fictici per a que pugui avaluar-lo.
- Seguint les indicacions del client solucionar els errors detectats i implementar possibles millores.

2.3 Planificació temporal.

Presentem ara la planificació temporal del projecte:

Nombre de tarea	Duración	Comienzo	Fin
Elaborar pla de treball	12 días	vie 28/02/14	lun 17/03/14
Fase d'elaboració	20 días	mar 18/03/14	lun 14/04/14
Analitzar gestors de contrasenyes existents i recollida de requisits	2 días	mar 18/03/14	mié 19/03/14
Elaborar diagrama de casos d'ús	2 días	jue 20/03/14	vie 21/03/14
Elaborar la documentació textual	2 días	sáb 22/03/14	lun 24/03/14
Especificar les classes d'anàlisi	3 días	mar 25/03/14	jue 27/03/14
Cercar i documentar llibreries criptogràfiques	4 días	vie 28/03/14	mié 02/04/14
Cercar un mecanisme de sincronització	3 días	jue 03/04/14	dom 06/04/14
Cercar i documentar les llibreries de sinronització	3 días	lun 07/04/14	mié 09/04/14
Dissenyar la interficie d'usuari	3 días	jue 10/04/14	lun 14/04/14
Fase de Construcció	25 días	mar 15/04/14	lun 19/05/14
Implementar el disseny	22 días	mar 15/04/14	mié 14/05/14
Proves	3 días	jue 15/05/14	lun 19/05/14
Fase de transició	19 días	mar 20/05/14	vie 13/06/14
Elaborar presentació	6 días	sáb 14/06/14	vie 20/06/14
Elaborar memòria	76 días	vie 28/02/14	vie 13/06/14

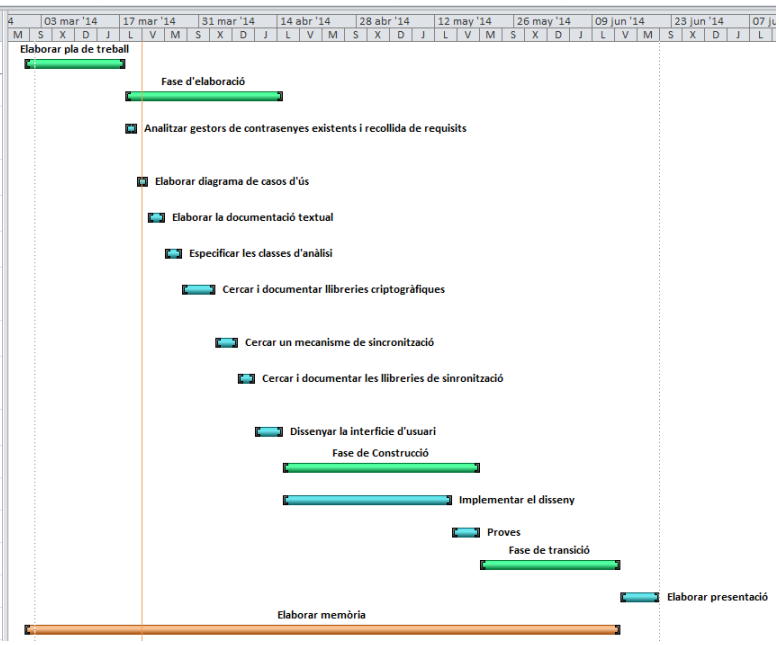


Figura 1: Planificació temporal.

2.4 Estat de l'art.

2.4.1 El sistema de xifratge.

Entenem per xifratge el procés per al qual un text en clar és transforma en un text xifrat de manera que només coneixent la clau criptogràfica (que és secreta) serem capaços de recuperar el missatge original. En aquest sentit cal dir que que tot el mecanisme de xifratge, excepte la clau secreta, és conegut. Així que, la seguretat d'una xifra ha de residir totalment en la clau secreta (suposició de Kerckhoffs). Existeixen dos tipus principals de xifres: de clau compartida i de clau pública:

2.4.1.1 Xifres de clau compartida.

Els criptosistemes de clau compartida són aquells en els quals l'emissor i el receptor comparteixen una mateixa clau per a xifrar i desxifrar missatges.
Aquest tipus de xifra presenta tres inconvenients: la distribució de claus (abans de començar la comunicació dos usuaris han d'elegir una clau secreta trobant-se personalment o confiant en un canal segur, cosa que no sempre serà possible), la gestió de claus (cada parella d'usuaris ha de tenir la seva clau compartida particular) i no hi ha signatura digital (totes les claus son compartides almenys per dos usuaris).
Tot i així, són àmpliament utilitzades degut a que són més ràpides que les xifres de clau pública i requereixen menys recursos.

2.4.1.1.1 Xifra de clau compartida AES.

Per a aquest projecte no ens cal cap distribució de claus ni tampoc cap funció de signatura digital així que és més adequat utilitzar un criptosistema de clau compartida com AES que fa servir claus de xifratge de 128, 192 i 256 bits i xifra blocs de text en clar

de les mateixes longituds (tot i que l'estàndard aprovat pel NIST només fa servir blocs de 128 bits). Podeu obtenir més informació sobre aquest estàndard a:
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf [1]

El funcionament d'AES consisteix en una transformació inicial del text en clar seguida d'un nombre d'iteracions que varien entre 10 i 14 depenent de les longituds anteriors, cada una de les quals aplica al bloc quatre funcions de transformació com es pot veure en la imatge següent:

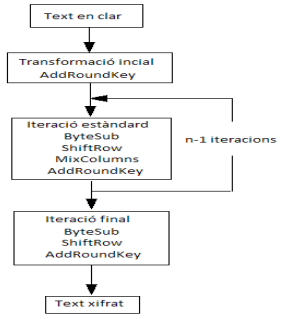


Figura 2: Funcionament d'AES.

AES treballa amb diferents subclaus en cada iteració. Aquestes subclaus s'obtenen per l'aplicació d'una funció d'ampliació a la clau de xifratge inicial.

Vegem ara breument el funcionament de la resta de funcions:

Transformació inicial:

Es transformen els bytes del text en clar en una matriu d'estat 4x4, és a dir, blocs per xifrar de 128 bits (estàndard NIST).
Sobre aquesta matriu s'aplica la funció AddRoundKey que fa una suma XOR de la matriu d'estat amb cada byte de la subclau k(i) corresponent.

Funció ByteSub:

Aquesta funció aplica una substitució no lineal dels bytes de la matriu d'estat.

Funció ShiftRow:

La funció ShiftRow desplaça les files de la matriu d'estat de manera que la fila zero es deixa igual, la fila 1 es desplaça C1 bytes l'esquerra, la fila 2 es desplaça C2 bytes a l'esquerra i la fila 3, C3 bytes a l'esquerra. Els valors C1, C2 i C3 depenen de la longitud del bloc N_b.

Funció MixColumns:

La funció MixColumns barreja les columnes de la matriu d'estat a partir d'operacions polinomials.

El lector interessat en els detalls de l'algorisme pot consultar:
http://ca.wikipedia.org/wiki/Advanced_Encryption_Standard [2].

2.4.1.2 Xifres de clau pública.

Per superar els inconvenients dels criptosistemes de clau compartida, varen sorgir les xifres de clau pública on cada usuari disposa d'una parella de claus, una pública coneguda per tothom i una privada. Un text xifrat amb una d'elles només pot ser desxifrat amb l'altre. Així doncs, un missatge xifrat amb la clau publica d'un usuari només podrà desxifrat per ell mateix (només ell coneix la clau privada) i davant d'un missatge xifrat amb la clau privada d'un usuari tothom podrà estar segur de que realment ell n'és l'autor (signatura digital).

2.4.2 Gestors de contrasenyes.

Existeix una gran varietat de gestors de contrasenyes tant de codi obert com propietari. Una petita mostra, amb les característiques més rellevants, podria ser la següent:

KeePass

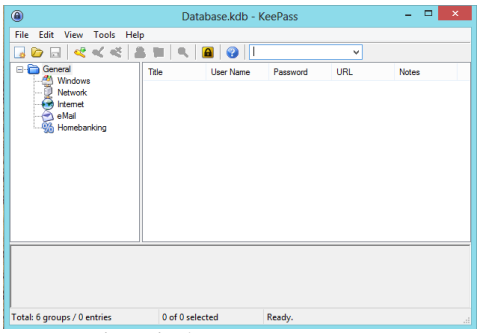


Figura 3: Interfície gràfica de KeePass.

- Encriptació AES.
- Utilització d'un fitxer de claus opcional per a desxifrar la base de dades (a més de la clau mestra).
- Sincronització mitjançant Dropbox (versió registrada).
- Bloqueig ràpid de l'espai de treball.
- Implementació d'un generador de contrasenyes.
- Implementació d'un analitzador de contrasenyes.

Password Safe

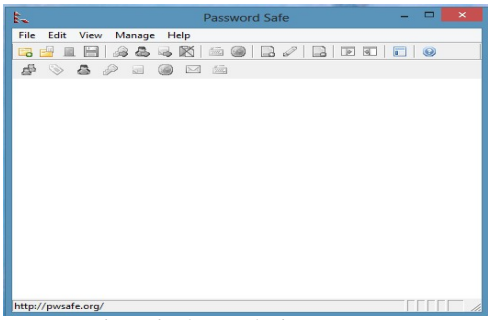


Figura 4: Interfície gràfica de Pasword Safe.

- Encriptació Twofish.
- Bloqueig ràpid de l'espai de treball.
- Implementació d'un generador de contrasenyes.

PINs

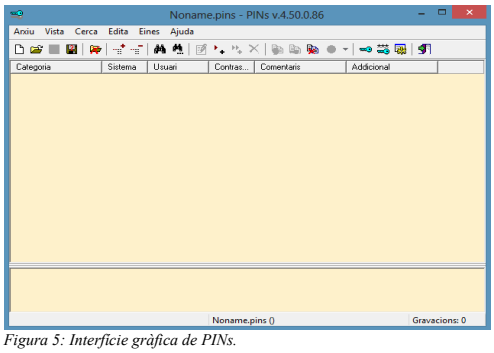


Figura 5: Interfície gràfica de PINs.

- Encriptació Blowfish.
- Bloqueig ràpid de l'espai de treball.
- Implementació d'un generador de contrasenyes.

3 Fase d'elaboració.

3.1 Anàlisi de requisits.

En aquesta fase analitzarem els requeriments mínims que haurà de complir la nostra aplicació per a poder satisfer el objectius marcats anteriorment.

3.1.1 Recollida de requisits.

3.1.1.1 Funcionament general de l'aplicació.

Les contrasenyes i noms d'usuari es desaran xifrades en un fitxer al disc. Per tal de poder-les recuperar, serà necessari utilitzar una clau de xifrat derivada a partir d'una clau mestra i uns bits aleatoris (bits de sal) desats en un fitxer (veure apartat 3.3.1.4). D'aquesta manera, l'usuari tindrà opció de desar aquest fitxer clau en un suport extern afegint un nivell més de seguretat (caldrà una cosa que l'usuari sap a més d'una cosa que l'usuari té).
Una vegada la base de dades estigui desxifrada (a la memòria volàtil) l'usuari podrà començar a utilitzar les funcions de l'aplicació.

3.1.1.2 Crear / obrir base de dades.

Al iniciar l'aplicació es podrà triar entre o bé obrir una base de dades existent o bé crear-ne una de nova. En el primer dels casos caldrà escriure la clau mestra i seleccionar el fitxer clau per a poder-la desxifrar i en el segon, serà necessari omplir un formulari amb les dades requerides: Nom, clau mestra, ruta del fitxer clau i la longitud de la clau de xifratge. D'aquest procés en resultaran dos fitxers: un amb la base de dades que es desarà en un subdirectori del directori de treball i un segon amb el fitxer clau, podent l'usuari triar el directori on es desarà.

3.1.1.3 Crear / eliminar categories.

Les entrades de la base de dades estaran organitzades per categories fent possible funcions de filtratge, ordenació, etc. L'usuari tindrà opció de crear-ne de noves i també d'eliminar-ne fent servir els formularis corresponents.

3.1.1.4 Crear /eliminar entrades.

Es podran afegir i eliminar entrades a la base de dades. En el primer cas, caldrà introduir les dades necessàries: títol, URL, nom d'usuari, contrasenya i notes. S'avaluarà la seguretat de la clau i s'oferirà la possibilitat de generar-ne una de forma automàtica. A més, quedarà registrada la data de creació.

3.1.1.5 Editar configuració.

L'usuari podrà editar la configuració (clau mestra, ubicació del fitxer clau, etc.) mitjançant el formulari adient.

3.1.1.6 Editar una entrada.

Serà possible editar una entrada i es registrarà la data de la darrera modificació.

3.1.1.7 Copiar dades al portapapers.

Els camps de les entrades de la base de dades es podran copiar al portapapers. Si el camp és la contrasenya, es registrarà la data d'ús i després de 20 segons el portapapers es buidarà.

3.1.1.8 Obrir l'URL.

Es podrà obrir l'URL que consta al camp apropiat d'una entrada.

3.1.1.9 Mostrar / ocultar contrasenyes en pantalla.

L'usuari podrà triar si els camps nom d'usuari i contrasenya són visibles o s'emmascaren amb asteriscs.

3.1.1.10 Bloqueig de l'espai de treball.

S'esborraran les dades de la taula, es xifrarà la base de dades, es minimitzarà l'aplicació i s'esborrarà la clau mestra de la memòria, essent necessari introduir-la novament avanç de poder tornar a desxifrar la base de dades.

3.1.1.11 Enllaçar amb servidor.

S'enllaçarà l'aplicació amb un servidor (tipus Dropbox o Google Drive). Es configuraran tots els paràmetres necessaris per a fer possible que l'aplicació pugui accedir a la informació emmagatzemada al servidor.

3.1.1.12 Sincronitzar amb servidor.

Quan s'instal·li aquest programari en un segon dispositiu, podrem sincronitzar-lo amb una base de dades ja existent al servidor tot utilitzant un fitxer de sincronització.

3.1.1.13 Crear fitxer de sincronització.

Es crearà un fitxer amb les dades necessàries per poder sincronitzar automàticament des d'un altre equip amb una base de dades ja existent.

3.1.1.14 Desar base de dades.

Es desarà la base de dades al disc després de xifrar els camps nom d'usuari i contrasenya.

3.1.2 Diagrama de casos d'us.

Com es pot veure hi haurà dos actors: Temporitzador, que serà l'encarregat de buidar el portapapers i Usuari, que engegarà la resta de casos d'ús.

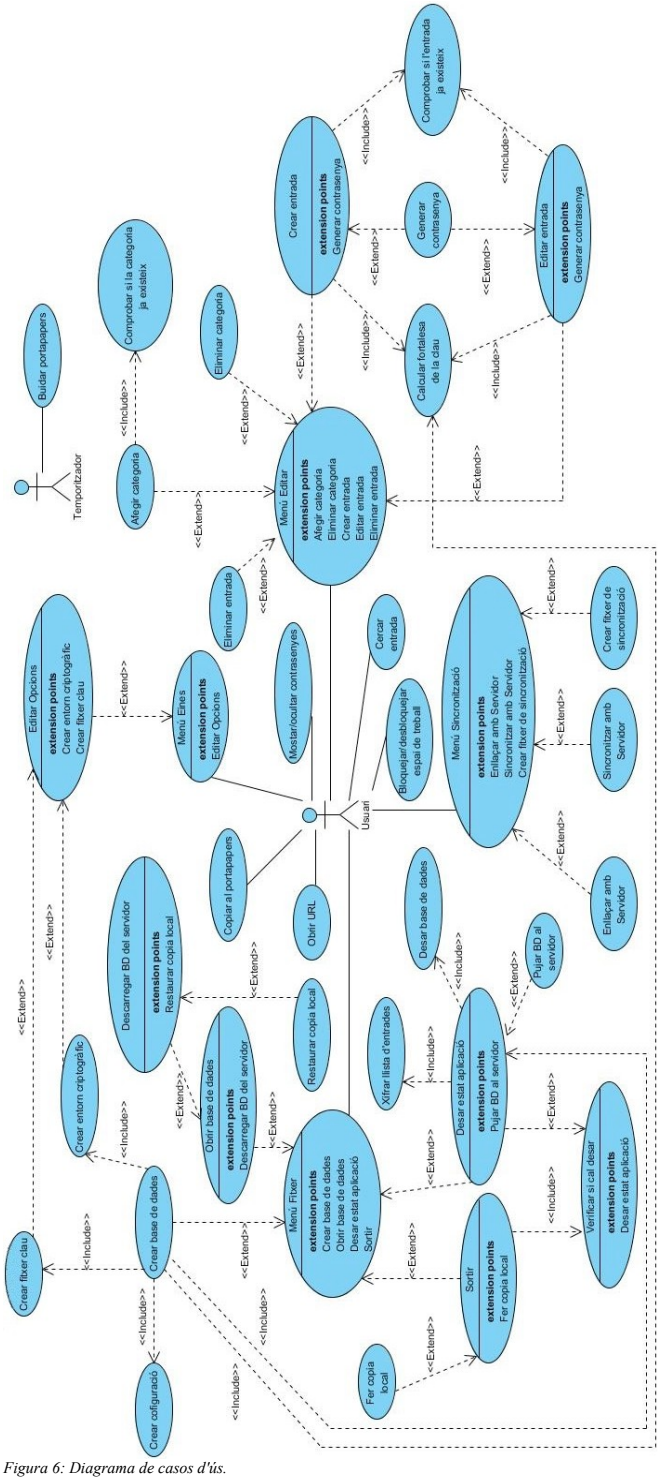


Figura 6: Diagrama de casos d'ús.

3.1.3 Documentació textual dels casos d'ús.

A continuació s'elaborarà la documentació textual dels principals casos d'us.

Cas d'ús número 1: "Menú fitxer"

Resum de la funcionalitat: mostra el menú "Fitxer".

Paper dins el treball de l'usuari: És la primera passa i la darrera que s'ha de realitzar en la utilització normal de l'aplicació (normalment obrir i tancar la base de dades).

Actors: **usuari**.

Casos d'ús relacionats: Crear base de dades, Obrir base de dades, Desar base de dades, Sortir de l'aplicació.

L'**usuari** tria entre una d'aquestes quatre opcions del menú: Crear base de dades Obrir base de dades, Desar base de dades o Sortir de l'aplicació.

Cas d'ús número 2: "Crear base de dades"

Resum de la funcionalitat: crea una nova base de dades.

Paper dins el treball de l'usuari: el fan servir els usuaris una única vegada avanç de poder començar a desar les seves contrasenyes.

Actors: **usuari**.

Casos d'ús relacionats: Menú fitxer, Crear fitxer clau, Crear configuració, Crear entorn criptogràfic.

Precondició: la base de dades no existeix.

Postcondició: s'ha creat una nova base de dades.

L'**usuari** omple un formulari proporcionant la següent informació, a partir de la qual es crearan un nou fitxer de dades (que inclou la llista de d'entrades i la configuració) i un fitxer clau amb els bits de sal:

- Nom de la base de dades.
- Ubicació on desar el fitxer de clau (bits de sal).
- Clau mestre.
- Bits de xifratge (128, 192 o 256).

Per defecte, els dos fitxers es creen dins el subdirectori "Dades" del directori de treball de l'aplicació tot i que és possible desar el fitxer de clau en una ubicació diferent per tal de permetre fer-la portable (per exemple dins una memòria USB).

Aquest procés comprova també la fortalesa de la clau mestra introduïda, crea l'entorn criptogràfic necessari, verifica que les dades introduïdes són correctes i desa l'estat de l'aplicació.

Alternatives de procés i excepcions: Si la base de dades ja existeix se li demana a l'usuari si la vol sobreescriure. Es poden produir excepcions d'entrada/sortida i criptogràfiques.

Cas d'ús número 3: "Crear fitxer clau"

Resum de la funcionalitat: Crea un fitxer amb els bits de sal.

Casos d'ús relacionats: Editar opcions, Crear base de dades.

Precondició: Els bits de sal i la ubicació on desar-los estan disponibles.

Postcondició: S'ha creat un fitxer amb els bits de sal a la ubicació escollida.

Es crea un fitxer amb els bits de sal a la ubicació indicada a la configuració.

Alternatives de procés i excepcions: Si el fitxer de clau ja existeix se li demana a l'usuari si el vol sobreescriure. Es poden produir excepcions d'entrada/sortida.

Cas d'ús número 4: "Crear entorn criptogràfic"

Resum de la funcionalitat: configura l'entorn criptogràfic.

Casos d'ús relacionats: Crear base de dades, Editar opcions.

Es configura l'aplicació per treballar amb AES segons la mida triada de la clau de xifrat, s'obtenen els bits de sal i amb aquests se'n deriva la clau criptogràfica partir de la clau mestra.

Alternatives de procés i excepcions: Es poden produir excepcions d'entrada/sortida i criptogràfiques.

Cas d'ús número 5: "Obrir base de dades"

Resum de la funcionalitat: es llegeix la base de dades i la configuració.

Paper dins el treball de l'usuari: el fan servir els usuaris cada vegada que volen començar a treballar amb una base de dades ja existent.

Actors: **usuari**.

Casos d'ús relacionats: Menú fitxer, Descarregar BD de Dropbox, Restaurar copia local.

Precondició: la base de dades existeix.

Postcondició: s'ha llegit la base de dades i la configuració.

L'**usuari** selecciona la base de dades que vol obrir explorant l'arbre de directoris i es recupera la llista d'entrades junt amb la configuració.

Alternatives de procés i excepcions: Si l'opció de sincronització està activa, es descarrega el fitxer emmagatzemat al servidor i si es produeix algun error es segueix treballant amb la còpia local. Es poden produir excepcions d'entrada/sortida.

Cas d'ús número 6: "Desar estat aplicació"

Resum de la funcionalitat: es desa l'estat actual de l'aplicació.

Paper dins el treball de l'usuari: el fan servir els usuaris cada vegada que volen fer persistent l'estat actual de l'aplicació.

Actors: **usuari**.

Casos d'ús relacionats: Menú Fitxer, Xifrar base de dades, Desar base de dades, Verificar si cal desar.

Es xifra la llista d'entrades i després es desa la base de dades (que inclou aquesta llista més la configuració).

Alternatives de procés i excepcions: si la sincronització està activa es desa una copia al servidor. Es poden produir excepcions d'entrada/sortida i criptogràfiques.

Cas d'ús número 7: "Xifrar llista entrades"

Resum de la funcionalitat: es xifra la llista d'entrades mitjançant AES.

Casos d'ús relacionats: Desar estat aplicació.

Es xifren els camps "usuari" i "contrasenya" de la llista d'entrades utilitzant AES amb la clau derivada a partir de la clau mestra i els bits de sal. Cada vegada es calcula un nou vector d'inicialització.

Precondició: S'ha inicialitzat l'entorn criptogràfic.

Alternatives de procés i excepcions: Es poden produir excepcions criptogràfiques.

Cas d'ús número 8: "Desar base de dades"

Resum de la funcionalitat: es desa la base de dades al disc.

Casos d'ús relacionats: Desar estat aplicació.

Es desen en un fitxer al disc la llista d'entrades i la configuració.

Alternatives de procés i excepcions: Es poden produir excepcions d'entrada/sortida.

Cas d'ús número 9: “Sortir”

Resum de la funcionalitat: es tanca l'aplicació.

Paper dins el treball de l'usuari: el fan servir els usuaris quan han acabat de treballar amb l'aplicació i la volen tancar.

Actors: **usuari**.

Casos d'ús relacionats: Menú Fitxer, Verificar si cal desar.

Es desa l'estat de l'aplicació si és necessari i es tanca l'aplicació.

Alternatives de procés i excepcions: si la sincronització està activa es fa una còpia del fitxer de dades a una ubicació local diferent per si passés que, durant la descàrrega des del servidor, es produís algun error i aquest quedés corrupte. Es poden produir excepcions d'entrada/sortida.

Cas d'ús número 10: “Menú editar”

Resum de la funcionalitat: mostra el menú “Editar”.

Paper dins el treball de l'usuari: és el cas d'ús principal del treball dels usuaris.

Actors: **usuari**.

Casos d'us relacionats: Afegir categoria, Eliminar categoria, Crear entrada, Eliminar entrada, Editar entrada.

L'**usuari** tria entre una d'aquestes cinc opcions del menú: Afegir categoria, Eliminar categoria, Crear entrada, Eliminar entrada, Editar entrada.

Cas d'ús número 11: “Afegir categoria”

Resum de la funcionalitat: crea una nova categoria.

Paper dins el treball de l'usuari: el fan servir els usuaris cada vegada que volen crear una nova categoria.

Actors: **usuari**.

Casos d'ús relacionats: Menú editar.

Precondició: la categoria no existeix.

Postcondició: s'ha creat la nova categoria.

L'**usuari** introdueix el nom d'una nova categoria que servirà per classificar les diferents entrades de la base de dades i si aquesta no existeix, es crea.

Cas d'ús número 12: “Eliminar categoria”

Resum de la funcionalitat: elimina una categoria existent.

Paper dins el treball de l'usuari: el fan servir els usuaris cada vegada que volen eliminar una categoria existent.

Actors: **usuari**.

Casos d'ús relacionats: Menú editar.

Precondició: la categoria existeix i no té cap entrada associada.

Postcondició: s'ha eliminat la categoria.

L'**usuari** selecciona quina categoria vol eliminar i si no té cap entrada associada aquesta s'esborra.

Cas d'ús número 13: “Crear entrada”

Resum de la funcionalitat: es crea un nou objecte “Entrada” que representa una entrada de la base de dades.

Paper dins el treball de l'usuari: el fan servir els usuaris cada vegada que volen crear una nova entrada.

Actors: **usuari**.

Casos d'ús relacionats: Menú editar, Calcular fortalesa de la clau, Generar contrasenya.

Precondició: no existeix una altre entrada amb el mateix títol dins la mateixa categoria.

Postcondició: s'ha creat una nova entrada.

L'**usuari** emplena un formulari amb les dades relatives a un compte (títol, URL, usuari, contrasenya, i notes), es calcula la fortalesa de la clau i si les dades són correctes s'afegeix un nova entrada a la llista. La data de creació queda registrada.

Alternatives de procés i excepcions: l'usuari té l'opció de generar una contrasenya de forma automàtica.

Cas d'ús número 14: “Eliminar entrada”

Resum de la funcionalitat: s'elimina una entrada existent.

Paper dins el treball de l'usuari: el fan servir els usuaris cada vegada que volen eliminar una entrada existent.

Actors: **usuari**.

Casos d'ús relacionats: Menú editar.

Precondició: l'entrada existeix.

Postcondició: s'ha eliminat l'entrada.

L'**usuari** selecciona una entrada existent i l'elimina.

Cas d'ús número 15: "Calcular fortalesa de la clau"

Resum de la funcionalitat: es calcula la fortalesa d'una clau donada.

Casos d'ús relacionats: Crear entrada, Editar entrada.

Precondició: s'ha introduït una contrasenya.
Postcondició: s'ha calculat la fortalesa de la contrasenya.

Es calcula la fortalesa de la clau en funció de les següents característiques:

- Longitud de la contrasenya.
- Nombre de majúscules.
- Nombre de minúscules.
- Nombre de dígits.
- Nombre de símbols.
- Existència de caràcters repetits.
- Nombre de dígits o símbols en posicions intermèdies.
- Majúscules, minúscules o dígits consecutius.
- Longitud de seqüències de caràcters i dígits.

Cas d'ús número 16: "Generar contrasenya"

Resum de la funcionalitat: es genera una contrasenya de forma automàtica.

Paper dins el treball de l'usuari: el fan servir el usuaris cada vegada que volen generar una contrasenya automàticament.

Actors: **usuari**.

Casos d'ús relacionats: Crea entrada, Editar entrada.

L'**usuari** selecciona la mida de la clau i es genera una contrasenya aleatòria.

Cas d'ús número 17: "Editar entrada"

Resum de la funcionalitat: s'edita una entrada existent per modificar-la.

Paper dins el treball de l'usuari: el fan servir els usuaris cada vegada que volen modificar els camps d'una entrada.

Actors: **usuari**.

Casos d'ús relacionats: Menú editar, Calcular fortalesa de la clau, Generar contrasenya.

Precondició: l'entrada existeix.

Postcondició: s'ha modificat l'entrada.

L'**usuari** edita un formulari amb les dades relatives a una entrada (títol, URL, usuari, contrasenya i notes), es calcula la fortalesa de la clau i si les dades són correctes (mateixes restriccions que una entrada nova) es modifica. La data queda registrada.

Alternatives de procés i excepcions: l'usuari te l'opció de generar una contrasenya de forma aleatòria.

Cas d'ús número 18: "Menú sincronització"

Resum de la funcionalitat: Mostra el menú "Sincronització".

Paper dins el treball de l'usuari: el fan servir els usuaris cada vegada que volen que volen actuar damunt la sincronització.

Actors: **usuari**.

Casos d'ús relacionats: Enllaçar amb servidor, Sincronitzar amb servidor, Crear fitxer de sincronització.

L'**usuari** tria entre una de les següents opcions del menú: Enllaçar amb servidor, Sincronitzar amb servidor, Crear fitxer de sincronització.

Cas d'ús número 19: "Enllaçar amb servidor"

Resum de la funcionalitat: enllaça l'aplicació amb el servidor.

Paper dins el treball de l'usuari: el fan servir els usuaris una vegada per enllaçar l'aplicació amb el servidor.

Actors: **usuari**.

Casos d'ús relacionats: Menú sincronització.

Precondició: l'aplicació no està enllaçada amb el servidor.

Postcondició: l'aplicació s'ha enllaçat amb el servidor.

L'**usuari** tria aquesta opció i obté les dades de connexió amb el servidor i les configura a l'aplicació.

Alternatives de procés i excepcions: es poden produir excepcions d'entrada/sortida.

Cas d'ús número 20: “Crear fitxer de sincronització”

Resum de la funcionalitat: es crea un fitxer amb les dades necessàries per sincronitzar automàticament un altre equip amb el servidor.

Paper dins el treball de l'usuari: el fan servir els usuaris cada vegada que volen crear un fitxer de sincronització amb el servidor.

Actors: **usuari**.

Casos d'ús relacionats: Menú sincronització.

Precondició: l'aplicació està enllaçada amb el servidor.
Postcondició: s'ha creat el fitxer de sincronització.

L'**usuari** tria aquesta opció i crea un fitxer que podrà utilitzar des d'un equip diferent per a sincronitzar-lo automàticament amb el servidor.

Alternatives de procés i excepcions: es poden produir excepcions d'entrada/sortida.

Cas d'ús número 21: “Sincronitzar amb servidor”

Resum de la funcionalitat: es sincronitza l'aplicació amb el servidor.

Paper dins el treball de l'usuari: el fan servir els usuaris una vegada per sincronitzar un equip nou amb el servidor.

Actors: **usuari**.

Casos d'ús relacionats: Menú sincronització.

Precondició: l'aplicació no està sincronitzada amb el servidor.

Postcondició: l'aplicació s'ha sincronitzat amb el servidor.

L'**usuari** tria aquesta opció per obrir el fitxer creat en el cas d'ús anterior i sincronitzar automàticament l'aplicació amb el servidor.

Alternatives de procés i excepcions: es poden produir excepcions d'entrada/sortida.

Cas d'ús número 22: “Copiar al portapapers”

Resum de la funcionalitat: es copia una cel·la de la taula d'entrades al portapapers.

Paper dins el treball de l'usuari: el fan servir els usuaris cada vegada que volen copiar un camp d'una entrada al portapapers.

Actors: **usuari**.

Precondició: la posició del ratolí coincideix amb una cel·la de la taula.

Postcondició: s'ha copiat el valor de la cel·la al portapapers.

L'**usuari** prem el botó dret del ratolí damunt una cel·la i seleccionant l'opció corresponent del menú desplegable copia el seu contingut al portapapers. Si el que s'ha copiat és una contrasenya s'actualitza la data del darrer ús i s'engega un comptador de 20 segons després dels quals el contingut del portapapers es buidarà.

Cas d'ús número 23: "Obrir URL"

Resum de la funcionalitat: s'obre l'URL corresponent a una entrada.

Paper dins el treball de l'usuari: el fan servir els usuaris cada vegada que volen obrir l'URL d'una entrada determinada.

Actors: **usuari**.

Precondició: la posició del ratolí coincideix amb una filera de la taula la qual conté una URL en el camp corresponent.

Postcondició: s'ha obert l'URL.

L'**usuari** prem el botó dret del ratolí damunt una filera de la taula i seleccionant l'opció corresponent del menú desplegable obre l'URL que hi consta.

Cas d'ús número 24: "Mostrar/ocultar contrasenyes"

Resum de la funcionalitat: es mostren en clar o emmascarats amb asteriscs els continguts dels camps "usuari" i "contrasenya"

Paper dins el treball de l'usuari: el fan servir els usuaris cada vegada que volen canviar el mode de visualització dels camps referits.

Actors: **usuari**.

L'**usuari** marca o desmarca una casella de verificació per commutar entre els dos modes de visualització.

Cas d'us número 25: "Editar opcions"

Resum de la funcionalitat: s'editen les opcions de configuració.

Paper dins el treball de l'usuari: el fan servir els usuaris cada vegada que volen canviar alguna opció de configuració.

Actors: **usuari**.

Casos d'ús relacionats: Menú eines, Crear entorn criptogràfic, Crear fitxer clau.

L'**usuari** edita el formulari d'edició de la configuració per canviar la ubicació del fitxer de clau, la clau mestra o per activar/desactivar la sincronització.

Alternatives de procés i excepcions: si es canvia la clau mestra cal introduir la clau anterior i es crea un nou entorn criptogràfic. Es poden produir excepcions d'entrada/sortida i criptogràfiques.

Cas d'us número 26: "Bloquejar espai de treball"

Resum de la funcionalitat: es bloqueja l'espai de treball.

Paper dins el treball de l'usuari: el fan servir els usuaris cada vegada que volen bloquejar l'espai de treball.

Actors: **usuari**.

Precondició: l'espai de treball està desbloquejat.

Postcondició: s'ha bloquejat l'espai de treball.

L'**usuari** pressiona un botó i la llista d'entrades es xifra, la taula d'entrades s'esborra i l'aplicació es minimitza.

Alternatives de procés i excepcions: es poden produir excepcions criptogràfiques.

Cas d'us número 27: "Desbloquejar espai de treball"

Resum de la funcionalitat: es desbloqueja l'espai de treball.

Paper dins el treball de l'usuari: el fan servir els usuaris cada vegada que volen desbloquejar l'espai de treball.

Actors: **usuari**.

Precondició: l'espai de treball està bloquejat.

Postcondició: s'ha desbloquejat l'espai de treball.

L'**usuari** maximitza l'aplicació i després d'introduir la clau mestra es desxifra la llista d'entrades i es mostra per pantalla dins la taula.

Alternatives de procés i excepcions: es poden produir excepcions criptogràfiques.

Cas d'us número 28: "Buidar portapapers"

Resum de la funcionalitat: buida el portapapers.

Paper dins el treball de l'usuari: el fa servir el temporitzador després de que una contrasenya s'hagi copiat al portapapers.

Actors: **temporitzador**.

El **temporitzador** buida el contingut del portapapers 20 segons després de que una contrasenya s'hi hagi copiat.

Cas d'ús número 29: "Desxifrar llista entrades"

Resum de la funcionalitat: es desxifra la llista d'entrades mitjançant AES.

Casos d'ús relacionats: Obrir base de dades.

Es desxifren els camps "usuari" i "contrasenya" de la llista d'entrades utilitzant AES amb la clau derivada a partir de la clau mestra i els bits de sal.

Precondició: S'ha inicialitzat l'entorn criptogràfic.

Alternatives de procés i excepcions: Es poden produir excepcions criptogràfiques.

3.2 Disseny.

3.2.1 Especificació de les classes d'anàlisi.

Per a dur a terme aquest projecte s'utilitzaran cinc classes principals que inclouran els atributs i operacions necessàries per a poder desenvolupar el casos d'ús anteriors i una classe addicional per a cada formulari necessari.

A continuació s'ofereix una breu descripció de les classes principals seguit pel diagrama resultant, on s'han representat només els atributs i operacions més rellevants (s'han omès les operacions d'accés als atributs):

- **Principal**: és la classe que gestiona la interfície d'usuari. Té els atributs i operacions necessàries per gestionar els diferents components (formularis, menús, taules, etc.) requerits per a realitzar les accions d'usuari (gestionar categories, entrades, base de dades, ...).

- **AES**: ofereix les operacions necessàries per xifrar i desxifrar utilitzant el criptosistema AES.

- **Entrada**: representa una entrada de la base dades amb tots els atributs necessaris dels diferents comptes (títol, data creació, data modificació, usuari, contrasenya ...).

- **Configuració**: classe que permet desar la configuració de l'aplicació.

- **Útils**: es una classe estàtica que ofereix utilitats a la resta de classes del projecte com per exemple, generació de caràcters aleatoris, calcular la fortalesa d'una clau, etc.

La classe FormConnexioServidor està pendent d'especificar en funció del sistema de sincronització elegit més endavant.

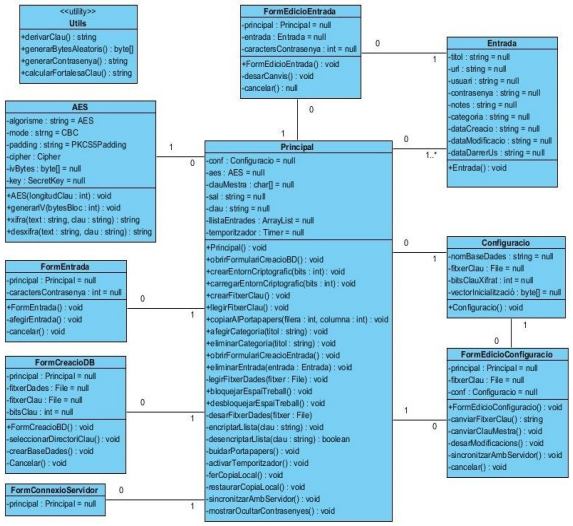
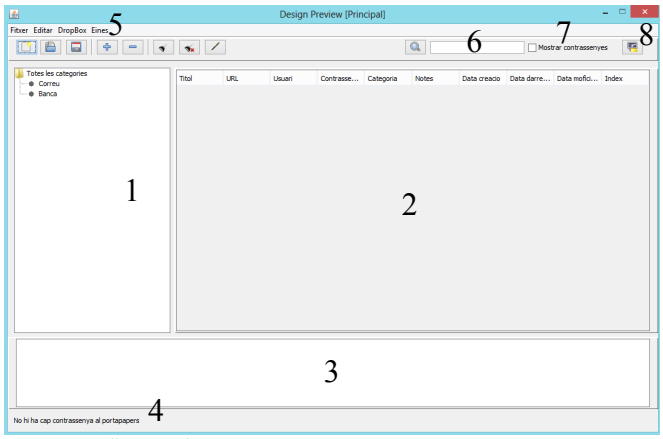


Figura 7: Diagrama de classes.

3.2.2 Disseny de la interfície d'usuari.

La interfície d'usuari constarà d'una pantalla principal des d'on, mitjançant una sèrie de botons i menús, s'aniran obrint els formularis necessaris per a realitzar totes les tasques requerides.

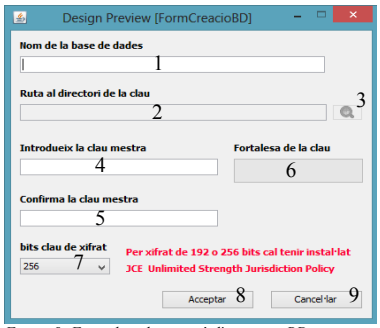
3.2.2.1 Pantalla principal.



1) Arbre de categories.
2) Taula d'entrades.
3) Informació addicional.
4) Estat de l'aplicació.
5) Botons i menús de funcions varies.
6) Cerca entrades.
7) Mostra/oculta contrasenyes.
8) Bloqueja l'espai de treball.

Figura 8: Pantalla principal.

3.2.2.2 Formulari de creació d'una nova base de dades.



1) Nom de la base de dades.
2) Ruta al directori del fitxer clau.
3) Obre un explorador de directoris.
4) Clau mestra.
5) Confirmació de la clau mestra.
6) Mostra la fortalesa de la clau.
7) Bits de la clau de xifrat.
8) Acceptar i crear la base de dades.
9) Cancel·lar i tornar a la pantalla principal.

Figura 9: Formulari de creació d'una nova BD

3.2.2.3 Formulari d'edició de la configuració.

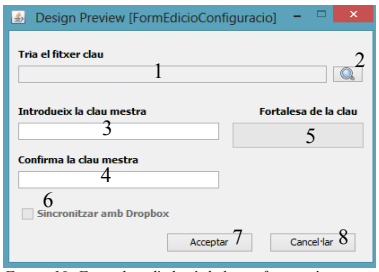


Figura 10: Formulari d'edició de la configuració.

1) Ruta al directori del fitxer clau.
2) Obre un explorador de directoris.
3) Clau mestra.
4) Confirmació de la clau mestra.
5) Mostra la fortalesa de la clau.
6) Activa la sincronització amb Dropbox.
7) Acceptar i desar modificacions.
8) Cancel·lar i tornar a la pantalla principal.

3.2.2.4 Formulari de creació/edició d'una entrada.

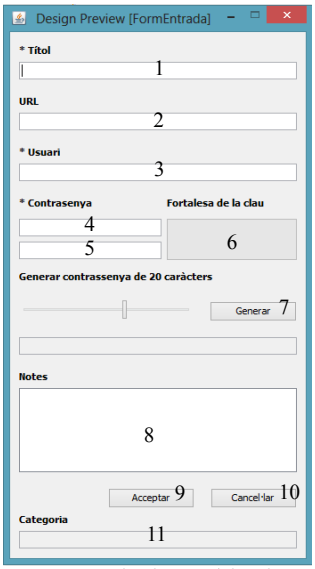
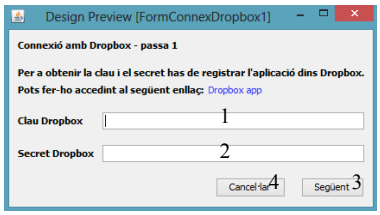


Figura 11: Formulari de creació/edició d'una entrada.

1) Títol de l'entrada.
2) URL.
3) Nom d'usuari del compte.
4) Contrasenya del compte.
5) Confirmació de la contrasenya.
6) Mostra la fortalesa de la clau.
7) Genera contrasenya aleatòria.
8) Camp de notes.
9) Acceptar i crear entrada.
10) Cancel·lar i tornar a la pantalla principal.
11) Categoria de l'entrada.

3.2.2.5 Formularis de sincronització amb Dropbox.



1) Clau Dropbox.
2) Secret Dropbox.
3) Continuar el procés.
4) Cancel·lar i tornar a la pantalla principal.

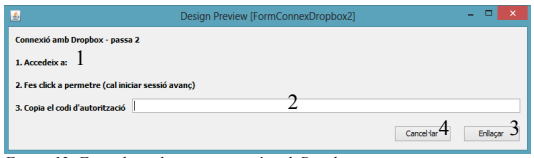


Figura 12: Formularis de sincronització amb Dropbox.

1) Enllaç al codi d'autorització.
2) Codi d'autorització.
3) Enllaçar amb Dropbox.
4) Cancel·lar.

3.3 Implementació.

3.3.1 Llibreries criptogràfiques de Java.

La realització d'aquest projecte requereix emprar funcions criptogràfiques que permetin treballar amb el criptosistema AES. Per a tal fi, s'ha triat la llibreria Java Cryptography Extension (JCE) ja que està inclosa en la distribució estàndard de Java, estant per aquest motiu molt estesa.
No obstant això, degut a les restriccions que alguns països apliquen, la versió del JCE inclosa al Java Runtime Environement (JRE) no permet el xifratge amb claus de 192 o 256 bits, així que per poder utilitzar claus AES d'aquestes longituds caldrà instal·lar prèviament el JCE Unlimited Strength Jurisdiction.

3.3.1.1 Funcionament de JCE.

El nucli del Java Cryptography Extension és la classe Cipher [3], la qual descriurem a continuació.

3.3.1.2 Creació d'objectes Cipher.

Per a crear un objecte d'aquesta classe cal cridar al mètode *getInstance*, passant com a paràmetre la transformació requerida, que indica l'algorisme a utilitzar, el mode d'operació i l'algorisme de farciment (per aquest treball: AES, CBC i PKCS5Padding).

CBC [4]:
Per assegurar que es generen textos xifrats diferents quan el mateix text en clar és encriptat vàries vegades amb la mateixa clau, abans de ser xifrat, a cada bloc de text se li aplica una operació XOR amb el bloc previ ja xifrat. D'aquesta manera, cada bloc xifrat depèn de tots els blocs de text en clar anteriors. A més, per fer cada missatge únic, es pot utilitzar un vector d'inicialització que ha de ser aleatori i no s'ha de repetir (tampoc cal mantenir-lo en secret). En aquest projecte generarem un nou vector d'inicialització per a cada operació de xifrat.

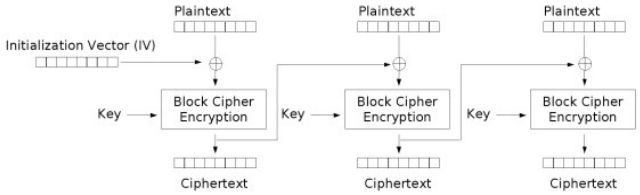


Figura 13: Funcionament del mode CBC.

PKCS5Padding [5]:
Com ja s'ha dit anteriorment, AES actua sobre blocs de 16 bytes per tant, quan el darrer bloc té una mida inferior, cal completar-lo. Amb aquest algorisme de farciment cada byte que falta s'omple amb el nombre de bytes de farciment que cal generar. Per exemple, si es necessiten 4 bytes, el farciment serà: {4,4,4,4}.

Exemple de creació d'una instància Cipher: `cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");`

3.3.1.3 Xifrat/desxifrat.

Per al xifrat/desxifrat d'un text cal cridar a dos mètodes de la classe Cipher: *init* i *doFinal*. Amb *init* preparem l'operació i amb *doFinal* la realitzem. La sintaxi seria la següent:

init (mode_operació, clau, vector d'inicialització);
doFinal (text);

Per exemple, per desxifrar un text xifrat hauríem d'executar les següents instruccions:

```
cipher.init(Cipher.DECRYPT_MODE, key, new IvParameterSpec(iv));
byte[] decrypted = cipher.doFinal(dec);
```

3.3.1.4 Derivació de les claus de xifrat.

Per a poder xifrar/desxifrar necessitem obtenir una clau de mida fixa (128, 192 o 256 bits) a partir d'una contrasenya o paraula de pas de mida arbitraria utilitzant una funció de derivació de claus. En aquest projecte utilitzarem PBKDF2 [6] que aplica una funció pseudoaleatòria a la contrasenya o paraula de pas combinant-la amb bits de sal i repetint el procés varies vegades per obtenir una clau derivada, la qual podrà ser utilitzada com a clau criptogràfica.
Afegint aquests bits de sal a la contrasenya es redueixen les expectatives d'èxit d'atacs que utilitzin resums precalculats (rainbow tables [7]) fent que s'hagin de provar individualment múltiples contrasenyes i no totes a l'hora.

3.3.2 Implementació de la sincronització.

3.3.2.1 Descripció.

Com s'ha dit anteriorment, quan s'actualitzi la base de dades des d'un dispositiu, cal que qualsevol canvi realitzat quedi replicat automàticament a tots els altres equips on estigui instal·lat el programari.

Per aconseguir-ho es mantindrà una còpia de la base de dades actualitzada a un compte de Dropbox, de manera que tots els dispositius hi tinguin accés. S'ha triat Dropbox ja que el seu ús està molt estès i Java disposa de llibreries gratuïtes que permeten accedir-hi sense necessitat de tenir instal·lada l'aplicació.

El funcionament general serà el següent:

1) Després de desar la base de dades es pujarà una còpia al servidor Dropbox.
2) Al tancar l'aplicació es desarà una copia addicional de la base de dades en una ubicació diferent (local).
3) Al obrir la base de dades, primer s'intentarà descarregar la còpia actualitzada del compte de Dropbox. En el cas de que això no sigui possible (errors de comunicació, etc.) es treballarà amb la còpia local desada en l'apartat 2.

3.3.2.2 Llibreries de Dropbox per a Java.

En aquest projecte farem servir les següents llibreries per treballar amb Dropbox [8]:

- dropbox-core-sdk-1.7.6.jar
- jackson-core-2.2.3.jar

Per a poder enllaçar l'aplicació amb Dropbox primer cal registrar-la, acció que ens proporcionarà una clau i un secret amb el quals podrem obtenir una autorització d'accés. Les passes a seguir són les següents:

1.- Accedint al següent enllaç registrem l'aplicació i obtenim la clau i el secret necessaris: https://www.dropbox.com/login?cont=https%3A//www.dropbox.com/developers/apps

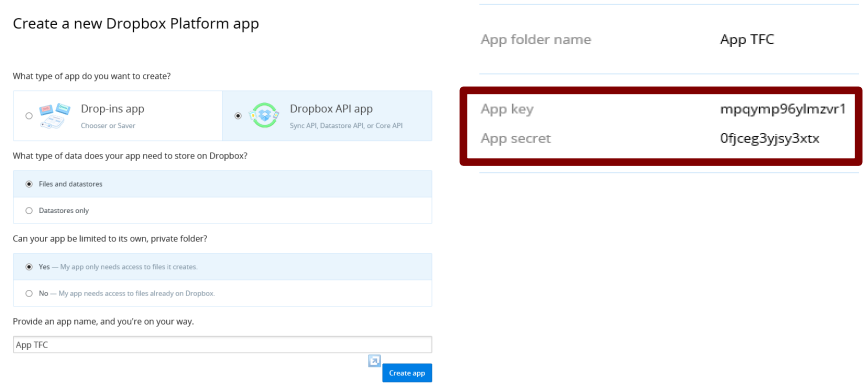


Figura 14: Obtenció de les dades per enllaçar amb Dropbox.

2.- Mitjançant un objecte de la classe DbxAppInfo que rep com a paràmetres la clau i el secret obtinguts a la passa anterior, generem un enllaç a la pàgina d'autorització:

3.- Accedint a l'enllaç permetem a la nostra aplicació crear carpetes a Dropbox i obtenim el codi d'autorització:

Figura 15: Autorització Dropbox.

4.- Per acabar, amb el codi obtingut, finalitzem el procés d'enllaç amb la creació d'un objecte de la classe DbxClient.

Tot aquest procés s'haurà de realitzar de la manera més automatitzada possible.

3.4 Estructura de dades.

En aquest projecte necessitem una estructura de dades que permeti desar les diferents entrades (associació d'un usuari i contrasenya junt amb altres dades d'interès) que es mostraran en una taula la qual ja te implementada la funció d'ordenació. No es preveu que l'aplicació hagi de gestionar grans quantitats d'informació de manera que quan calgui realitzar alguna cerca, un algorisme seqüencial serà prou eficient.
Per tant, l'estructura de dades més adequada per a dur a terme aquest projecte serà una llista que a més, presenta l'avantatge de que al ser serialitzable és molt fàcil implementar la seva persistència. Aquesta llista contindrà objectes de la classe Entrada.

4 Fase de construcció.

4.1 Desenvolupament.

El desenvolupament d'aquest projecte s'ha fet dividint el problema principal en cinc subproblemes: implementació del xifrat/desxifrat, generació de contrasenyes, anàlisi de contrasenyes, sincronització amb Dropbox i gestió de la interfície d'usuari. A continuació es farà una descripció de cada un d'ells.

4.1.1 Implementació del xifrat/desxifrat.

Per a la implementació de les funcions de xifrat i desxifrat s'ha creat la classe AES, basada en la classe Crypto de cryptojs.altervista.org [10] i que utilitza la llibreria JCE de Java. Aquesta classe s'ha hagut d'adaptar a les necessitats concretes d'aquest treball i corregir-hi alguns errors com la mida del vector d'inicialització que per AES no depèn de la mida de la clau de xifrat. Les seves dues funcions principals són les següents:

xifra: rep com a paràmetre el text en clar i retorna el text xifrat, tot recolzant-se en la funció cipher.init, la qual pren com arguments (a més del mode d'operació) la clau de xifrat i el vector d'inicialització.

desxifra: És la funció inversa de l'anterior. Rep com a paràmetre el text xifrat i retorna el text en clar.

Abans de poder utilitzar aquestes operacions, cal inicialitzar l'entorn criptogràfic cridant una de les següents funcions:

crearEntornCryptografic, crea una instància de la classe AES, genera uns nous bits de sal i a partir d'aquests i la clau mestra, en deriva la clau de xifrat.

carregarEntornCryptografic, igual que la anterior excepte que no genera uns nous bits de sal ja que n'utilitza els ja existents.

4.1.2 Generació de contrasenyes.

Una de les funcions imprescindibles que ha de tenir tot gestor de contrasenyes és que pugui generar-ne automàticament. Per a tal fi, s'ha creat la funció *generarContrasenya* que en crea una d'aleatòria, utilitzant els caràcters entre el 33 (!) i el 126 (~), podent triar la seva longitud entre 4 i 30 caràcters.

Per defecte, la mida de la clau s'ha establert en 20 caràcters que equival a una entropia [11] de 130,8 bits, donant per tant, una contrasenya molt segura:

Entropia de cada caràcter = log2(93) = 6,54 bits.
Entropia de la contrasenya = entropia de cada caràcter * longitud de la clau = 130,8.

4.1.3 Anàlisi de contrasenyes.

Una altra funció important que ha de tenir aquest tipus de programari és la capacitat d'analitzar les contrasenyes introduïdes per l'usuari i determinar-ne la seva fortalesa. Utilitzar l'entropia com a mètode de mesura només és correcte per a contrasenyes aleatòries, ja que aquesta només depèn de la longitud de la clau i de la mida del conjunt

de caràcters, no de la combinació d'aquests.

Així doncs, per a determinar la qualitat d'una contrasenya (les triades pels usuaris no seran necessàriament aleatòries) s'ha dissenyat la funció *calcularFortalesaClau* que n'analitza les característiques i retorna la seva fortalesa en funció de la puntuació obtinguda com s'explica a continuació:

4.1.3.1 Requeriments.

- Longitud de la contrasenya >= 8,
- Conté almenys una lletra majúscula.
- Conté almenys una lletra minúscula.
- Conté almenys un dígit.
- Conté almenys un símbol.

4.1.3.2 Puntuació.

- Puntuació += (longitud de la contrasenya * 2).
- Puntuació += ((longitud de la contrasenya – nombre de majúscules) * 2).
- Puntuació += ((longitud de la contrasenya – nombre de minúscules) * 2).
- Puntuació += (nombre de dígits * 4).
- Puntuació += (nombre de símbols * 6).
- Puntuació += (nombre de dígits o símbols en mig de la contrasenya * 2).
- Si el nombre dels requeriments assolits >3 llavors Puntuació += (nombre de requeriments assolits * 2).
- Si la contrasenya està formada només per lletres llavors Puntuació -= (longitud de la contrasenya).
- Si la contrasenya està formada només per dígits llavors Puntuació -= (longitud de la contrasenya).
- Si la contrasenya té caràcters repetits llavors Puntuació -= (nombre de caràcters repetits * (nombre de caràcters repetits -1)).
- Si la contrasenya té majúscules consecutives llavors Puntuació -= (nombre de majúscules consecutives * 2).
- Si la contrasenya té minúscules consecutives llavors Puntuació -= (nombre de minúscules consecutives * 2).
- Si la contrasenya té dígits consecutius llavors Puntuació -= (nombre de dígits consecutius * 2).
- Si la contrasenya té lletres en seqüencia llavors Puntuació -= (nombre de lletres en seqüència * 3).
- Si la contrasenya té dígits en seqüencia llavors Puntuació -= (nombre de dígits en seqüència * 3).

4.1.3.3 Avaluació.

- Puntuació [0,20) --> Molt insegura.
- Puntuació [20,40) --> Insegura.
- Puntuació [40,60) --> Acceptable.
- Puntuació [60,80) --> Segura.
- Puntuació [80,100] --> Molt segura.

Aquest procediment està basat en l'article “Password Strength Control” de Codeproject.com [12]. S'ha reduït el multiplicador de la longitud de la contrasenya de 4 a 2 per afavorir l'us de contrasenyes més llargues.

4.1.4 Sincronització amb Dropbox.

A l'apartat 3.3.2.2 ja em vist com enllaçar l'aplicació amb Dropbox però ara ens queda veure com donar accés des d'un segon equip a una base de dades ja existent. Tot el que cal per accedir a les dades d'una aplicació desades a Dropbox és conèixer la cadena de caràcters anomenada “access token” desada a l'objecte de configuració. Per tant, per a realitzar aquesta tasca, la llegirem cada vegada que sigui necessari:

La funció *crearFitxerSincronitzacio* s'encarrega de desar en un fitxer l'objecte amb la configuració (que entre altres dades conté l'access token), de manera que només caldrà obrir-lo des de'l nou equip amb l'opció “Sincronitzar amb Dropbox” perquè la informació necessària quedi actualitzada i la connexió amb el servidor Dropbox quedi establerta.

4.1.5 Gestió de la interfície d'usuari.

La gestió de la interfície d'usuari s'ha realitzat mitjançant un arbre per mostrar les diferents categories de les entrades, una taula per mostrar els camps de les entrades, un panell de text per mostrar informació addicional i diversos botons per a realitzar les funcions necessàries.

4.2 Proves i verificació de funcionament.

A continuació realitzarem una sèrie de proves per a verificar el funcionament correcte de les funcions principals de l'aplicació.

4.2.1 Creació d'una nova base de dades.

Creem una nova base de dades i triem desar el fitxer clau (amb els bits de sal) a una memòria USB.

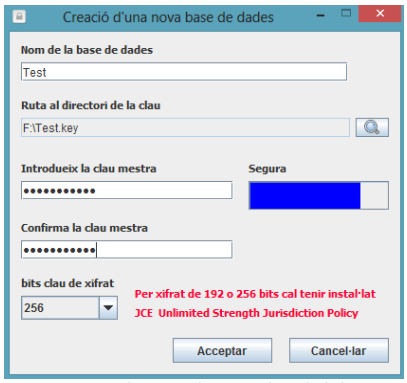
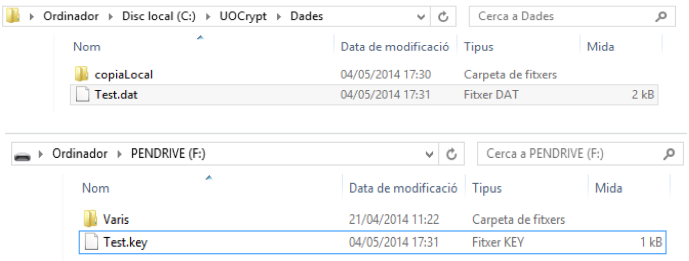


Figura 16: Prova de creació d'una nova base de dades.

Els fitxers corresponents (dades i clau) s'han creat i la qualitat de la clau s'ha avaluat correctament.



Si els fitxers ja existeixen s'informa l'usuari i se li demana si els vol sobreescriure.

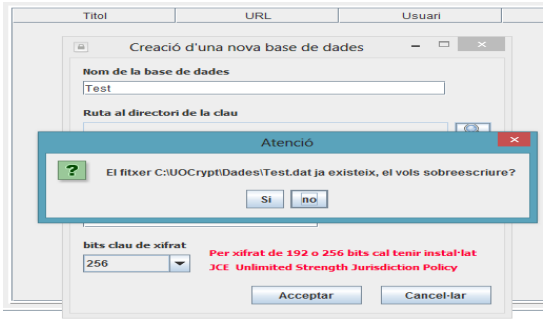


Figura 17: Prova de fitxer ja existent al crear una nova base de dades.

4.2.2 Creació d'una nova categoria.

Afegim una nova categoria (Xarxes Socials).

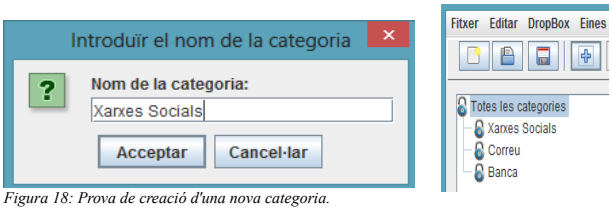


Figura 18: Prova de creació d'una nova categoria.

Veiem com la nova categoria s'ha creat correctament.

Si la categoria ja existeix, s'informa l'usuari i l'acció no és produeix.

Figura 19: Prova de categoria ja existent al crear-ne una de nova.

4.2.3 Eliminació d'una categoria existent.

Eliminem la categoria “Xarxes Socials”.

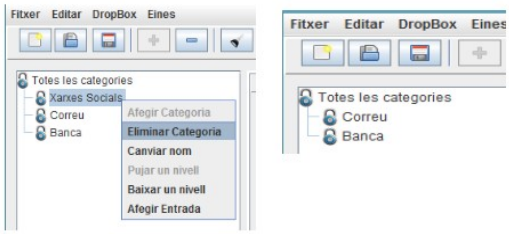


Figura 20: Prova d'eliminació d'un categoria.

Veiem com la categoria s'ha eliminat correctament.

Si la categoria té entrades associades s'informa l'usuari i no es permet l'operació.

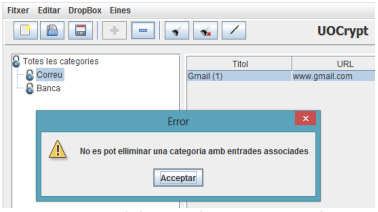


Figura 21: Prova d'elimiació d'una categoria amb entrades associades.

4.2.4 Creació d'una entrada de la base de dades.

Afegim una entrada a la base de dades.

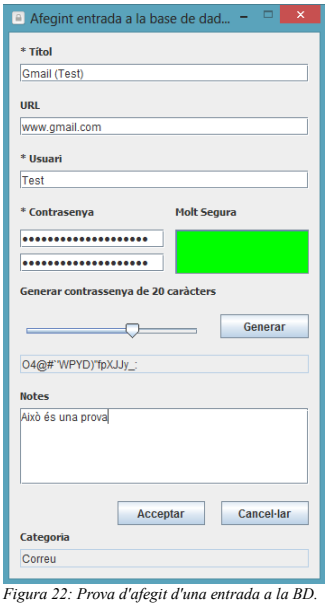


Figura 22: Prova d'afegit d'una entrada a la BD.

L'entrada s'ha creat correctament.

Títol	URL	Usuari	Contrasenya
Gmail (1)	www.gmail.com	**********	**********
Gmail (Test)	www.gmail.com	**********	**********

Veiem que s'ha generat una contrasenya molt segura automàticament i que la informació relativa a l'entrada s'ha actualitzat.

Títol: **Gmail (Test)**, URL: **www.gmail.com**, Usuari: **Test**, Contrassenya: ********, Categoria: **Correu**, Data creacio: **4/5/2014 17:47**,

Això és una prova

4.2.5 Eliminació d'una entrada de la base de dades.

Eliminem l'entrada que em afegit en l'apartat anterior.

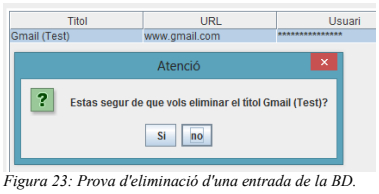


Figura 23: Prova d'eliminació d'una entrada de la BD.

Si l'usuari confirma que vol esborrar l'entrada, aquesta queda eliminada.

Títol	URL
Gmail (1)	www.gmail.com

4.2.6 Desat de la base de dades.

Aquesta és l'operació principal de l'aplicació i per a la qual s'ha dissenyat. La llista d'entrades que hi ha a la memòria volàtil s'ha de desar xifrada a la memòria persistent (disc dur).

Deixem dues entrades amb contrasenyes “2222” i “1111” per veure tot seguit com queden desades a la base de dades al disc.

Titol	URL	Usuari	Contrasenya
Gmail (1)	www.gmail.com	carles.suria	2222
Santander	www.gruposantander.es	carles	1111

Notifications | Output - UOCrypt (run)

```
run:
Contrasenya xifrada desada: 9Sh+98XghORshlPKDQT3oQ==
Contrasenya xifrada desada: wVWIfRcRVPQUJk3Nph58rw==
```

Figura 24: Prova de desat de la base de dades.

Veiem com efectivament les contrasenyes s'han desat al disc xifrades.

4.2.7 Edició d'una entrada de la base de dades.

Editem l'entrada “Santander” per assignar-li una contrasenya més segura.

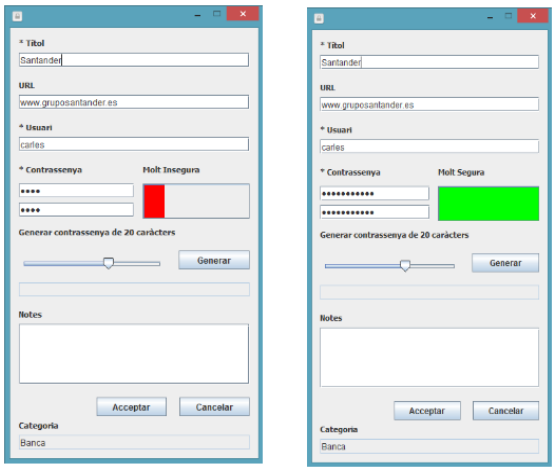


Figura 25: Prova d'edició d'una entrada de la BD (1).

El camp contrasenya s'ha modificat correctament i la informació relativa a l'entrada s'ha actualitzat.

Titol	URL	Usuari	Contrasenya
Santander	www.gruposantander.es	carles	C0ntR@s3ny@

Titol: **Santander**, URL: **www.gruposantander.es**, Usuari: **carles**, Contrassenya: ********, Categoria: **Banca**, Data creacio: **4/5/2014 17:58**, Data darrer us: **Mai**, Data modificació: **4/5/2014 18:13**

Figura 26: Prova d'edició d'una entrada de la BD (2).

4.2.8 Sortida de l'aplicació.

Si hi ha canvis pendents de desar, es demana a l'usuari si vol fer-ho abans de tancar l'aplicació.

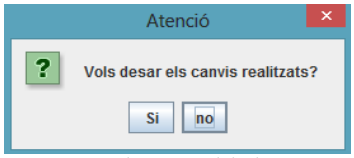


Figura 27: Prova de tancament de l'aplicació.

Si la resposta és afirmativa es desa la base de dades i després l'aplicació es tanca correctament.

4.2.9 Obertura de la base de dades.

Seleccionem la base de dades que volem obrir mitjançant l'arbre de directoris i si la clau mestra introduïda és correcte i el fitxer clau està disponible, aquesta s'obre i les dades es desxifren.

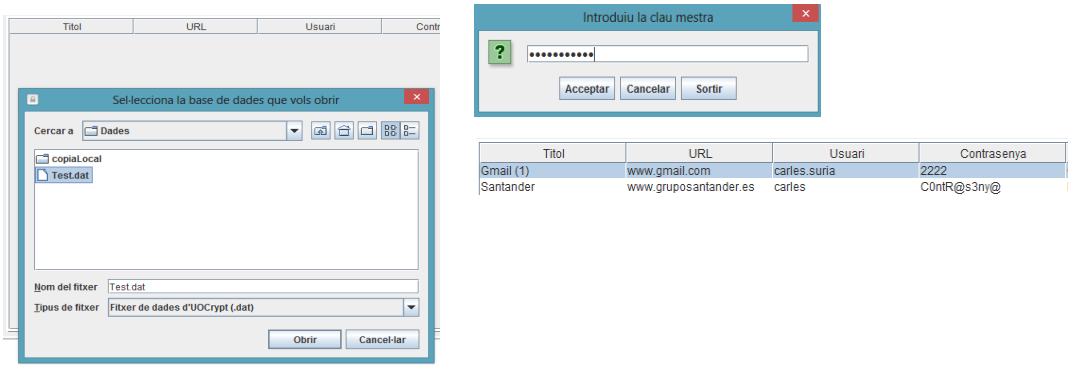


Figura 28: Prova d'obertura de la BD (1).

Si la clau mestra introduïda no és correcte, s'informa l'usuari i la base de dades no es desxifra.

Figura 29: Figura 28: Prova d'obertura de la BD (2).

En el cas de que el fitxer clau (bits de sal) no estigui disponible, s'informa l'usuari i la base de dades no es pot desxifrar. Es dona l'opció de cercar aquest fitxer mitjançant l'arbre de directoris.

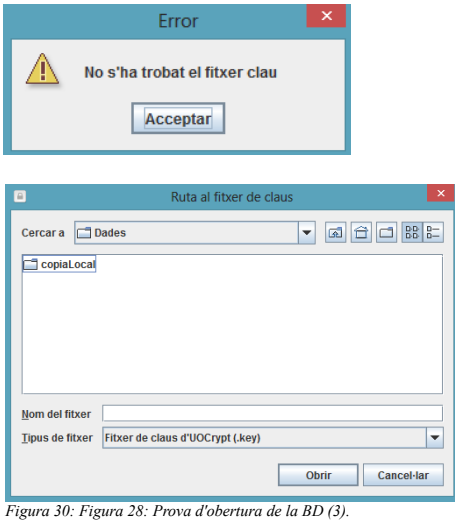


Figura 30: Figura 28: Prova d'obertura de la BD (3).

4.2.10 Mostrar/ocultar usuaris i contrasenyes.

Marquem o desmarquem la casella de comprovació Mostrar contrasenyes per alternar entre mostrar/ocultar els noms d'usuari i contrasenyes.

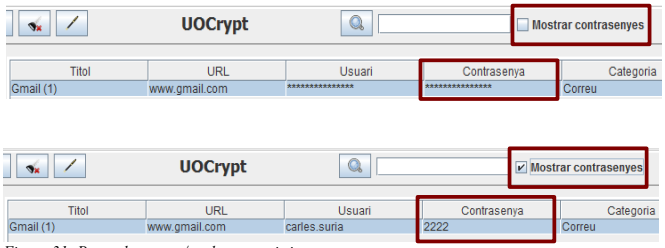


Figura 31: Prova de mostar/ocultar usuaris i contrasenyes.

4.2.11 Filtrat d'entrades per categoria.

Abans afegim algunes entrades a la base de dades.

Seleccionem una categoria de l'arbre, que serveix com a filtre de la taula:

- Es mostren les entrades de totes les categories.

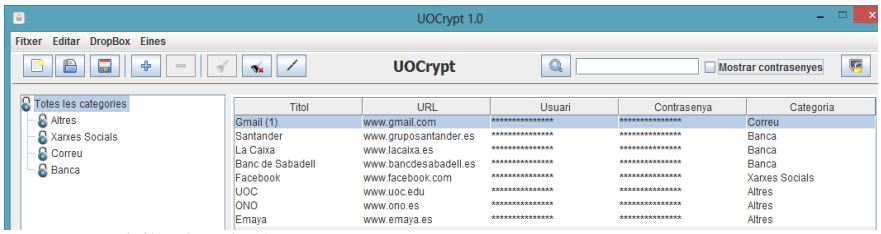


Figura 32: Prova de filtrat d'entrades (1).

- Filtrem per la categoria Correu.

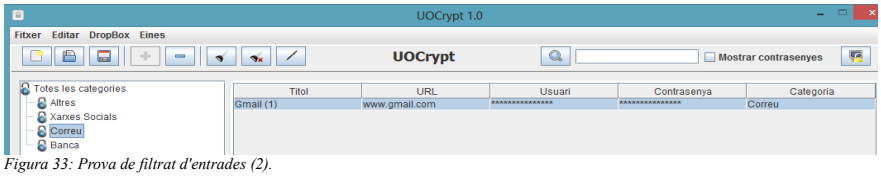


Figura 33: Prova de filtrat d'entrades (2).

- Filtrem per la categoria Altres.

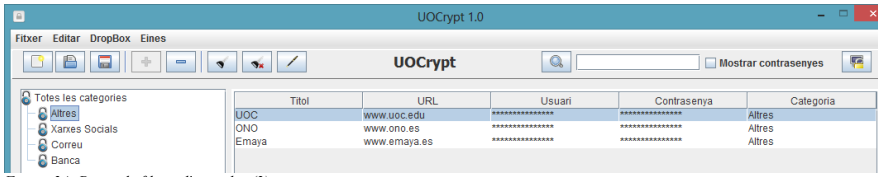


Figura 34: Prova de filtrat d'entrades (3).

4.2.12 Cerca d'una entrada pel seu nom.

Escrivim el nom (o part) d'una entrada al camp i després de prémer el botó amb la lupa o la tecla de retorn, a la taula només es mostren les entrades coincidents.

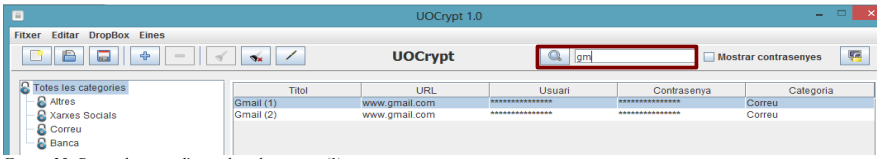


Figura 35: Prova de cerca d'entrada pel seu nom (1).

Si deixem el camp en blanc es mostren totes les entrades.

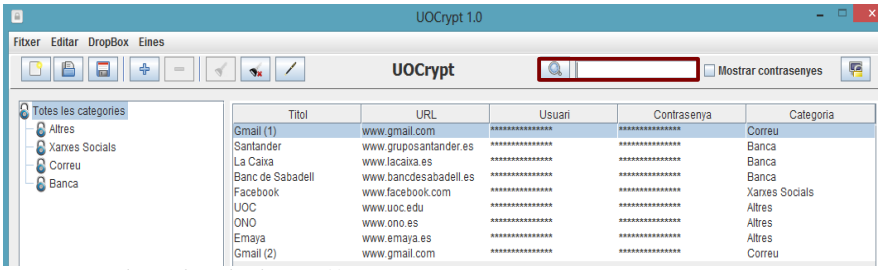


Figura 36: Prova de cerca d'entrada pel seu nom (2).

4.2.13 Bloqueig/desbloqueig de l'espai de treball.

Premem el botó  i l'aplicació es minimitza després de xifrar la llista d'entrades i esborrar les variables criptogràfiques a més de la taula.

Figura 37: Prova de bloqueig/desbloqueig de l'espai de treball (1).

Si ara volem maximitzar l'aplicació, avanç cal que tornem a introduir la clau mestra per generar de nou la clau de xifrat.

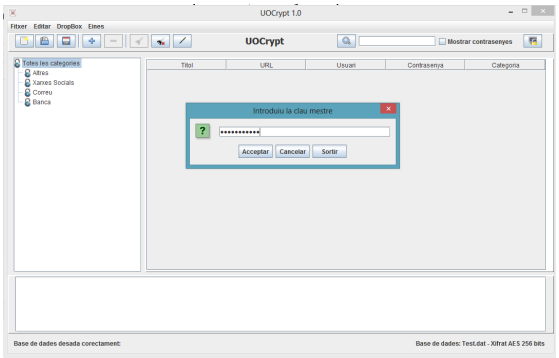


Figura 38: Prova de bloqueig/desbloqueig de l'espai de treball (2).

Si introduïm una clau errònia tres vegades l'aplicació es tanca.

Figura 39: Prova de bloqueig/desbloqueig de l'espai de treball (2).

Si introduïm la contrasenya correcta, es desbloqueja l'espai de treball.

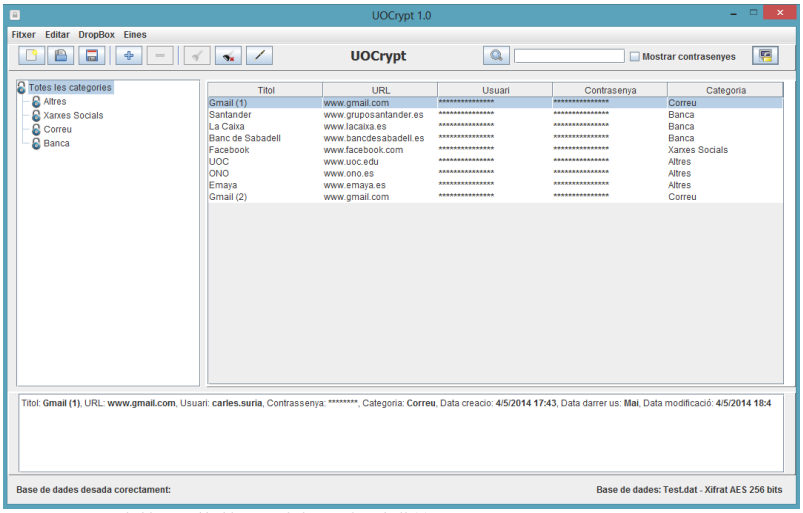


Figura 40: Prova de bloqueig/desbloqueig de l'espai de treball (3).

4.2.14 Enllaç amb Dropbox.

Seleccionem del menú “Dropbox” l'opció “Enllaçar amb Dropbox” i comencem el procés:

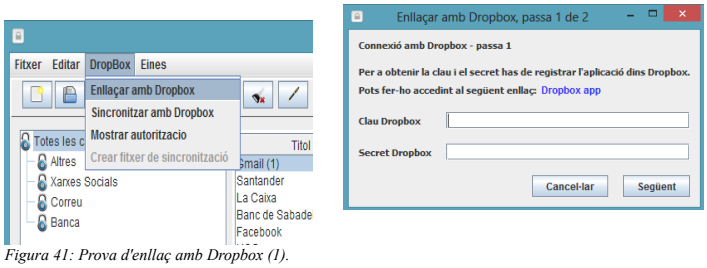


Figura 41: Prova d'enllaç amb Dropbox (1).

Accedim al enllaç 'Dropbox app' per registrar l'aplicació.

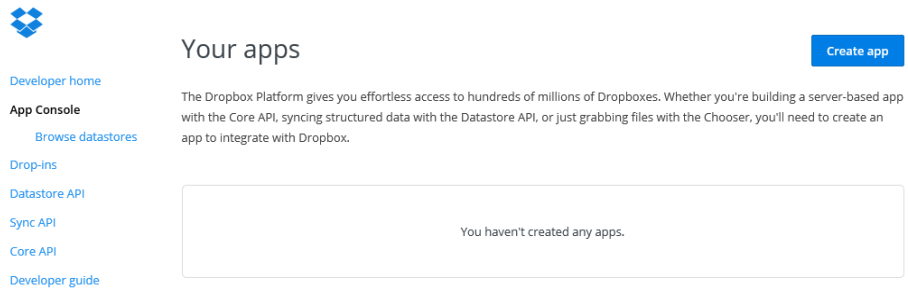


Figura 42: Prova d'enllaç amb Dropbox (2).

Creem una nova aplicació.

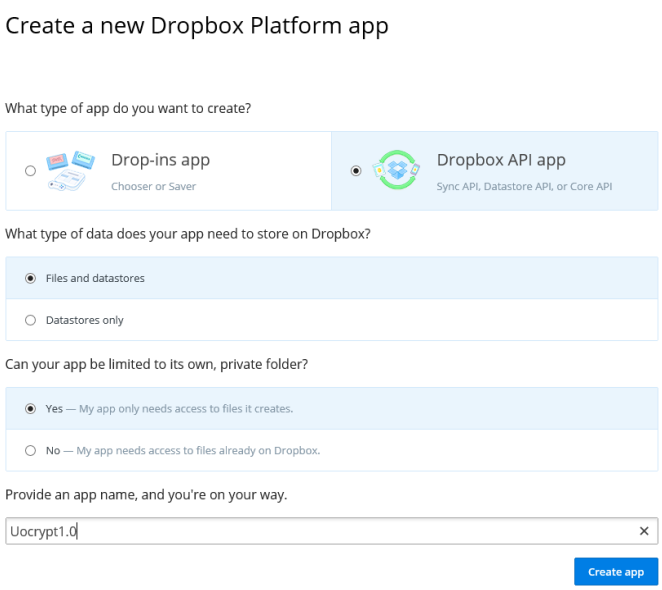


Figura 43: Prova d'enllaç amb Dropbox (3).

Així obtenim la clau i el secret.

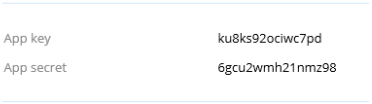


Figura 44: Prova d'enllaç amb Dropbox (4).

Els escrivim als camps corresponents i premem “Següent”.

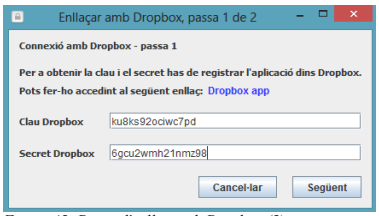


Figura 45: Prova d'enllaç amb Dropbox (5).

Accedim a l'enllaç per autoritzar l'aplicació.

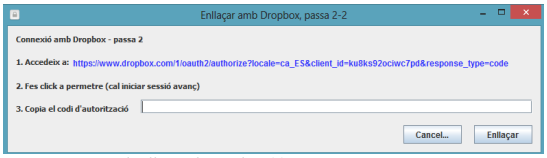


Figura 46: Prova d'enllaç amb Dropbox (6).

Permetem a l'aplicació accedir a les dades.

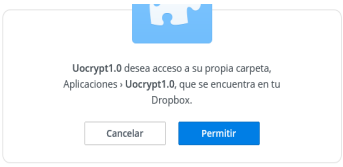


Figura 47: Prova d'enllaç amb Dropbox (7).

Copiem l'autorització i premem enllaçar.

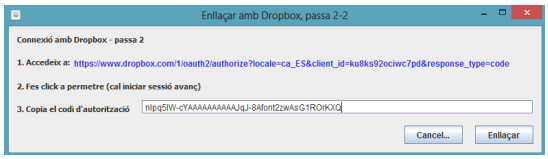
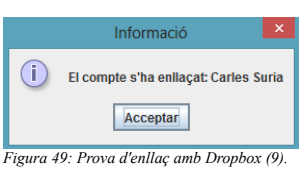


Figura 48: Prova d'enllaç amb Dropbox (8).

Així l'aplicació ha quedat enllaçada amb Dropbox.



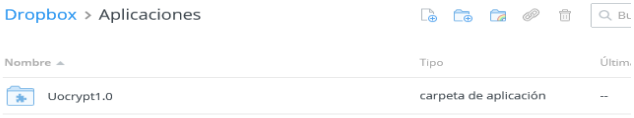
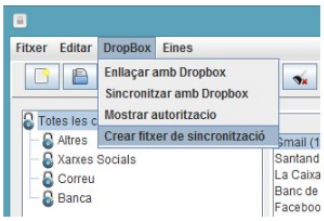
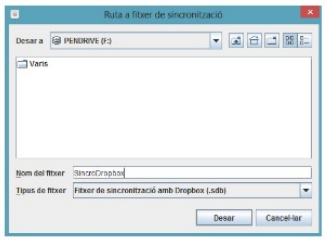


Figura 49: Prova d'enllaç amb Dropbox (9).

4.2.15 Creació del fitxer de sincronització.

Seleccionem del menú “Dropbox” l'opció “Crear fitxer de sincronització” i després de triar el nom i la ubicació, el fitxer és creat.





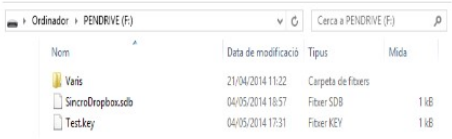
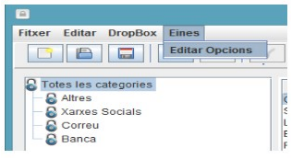


Figura 50: Prova de creació del fitxer de sincronització (1).

Des del menú “Eines – Editar opcions” habilitem la sincronització.



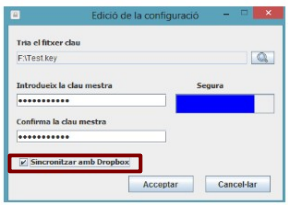


Figura 51: Prova de creació del fitxer de sincronització (2).

4.2.16 Sincronització amb Dropbox.

Des d'un equip diferent seleccionem del menú Dropbox l'opció “Sincronitzar amb Dropbox” i explorant l'arbre de directoris cerquem el fitxer de sincronització creat anteriorment.

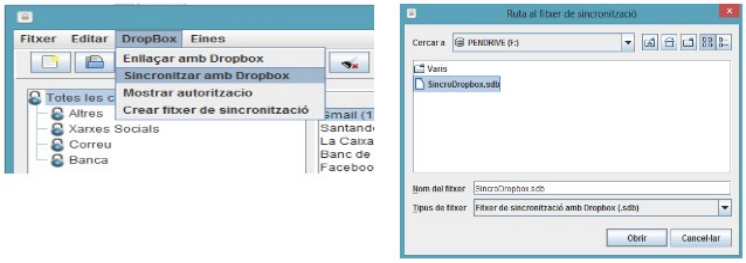


Figura 52: Prova de sincronització amb Dropbox (1).

Després de prémer damunt el botó “Obrir” i introduir la clau mestra, l'aplicació queda sincronitzada.

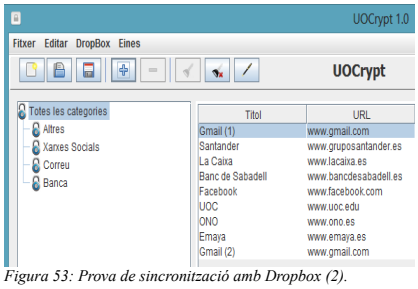


Figura 53: Prova de sincronització amb Dropbox (2).

A partir d'aquest moment podem veure com els canvis realitzats des d'un dels equips estan sincronitzats al accedir-hi des de l'altre.

4.2.17 Copiat dels camps de la taula al portapapers.

Premem el botó dret del ratolí damunt d'un dels camps de la taula i seleccionem l'opció “Copiar”. El seu valor es copia al portapapers i si el camp copiat és la contrasenya, s'actualitza la data del darrer ús.

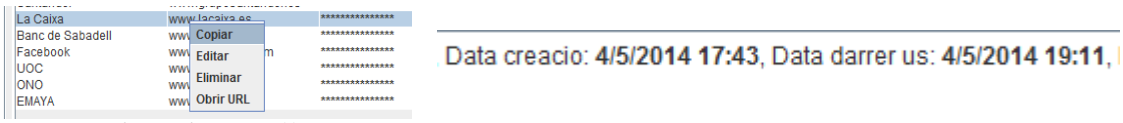


Figura 54: Prova de copiat al portapapers (1).

Ara podem enganxar-lo, per exemple, damunt d'un document de text.

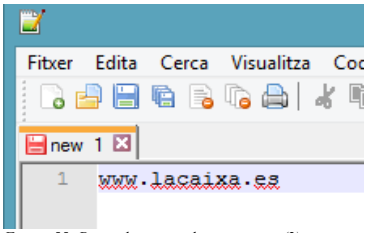


Figura 55: Prova de copiat al portapapers (2).

En el cas de que el camp copiat sigui la contrasenya, també s'activa el temporitzador i quan aquest arriba a 0, el contingut del portapapers s'elimina.

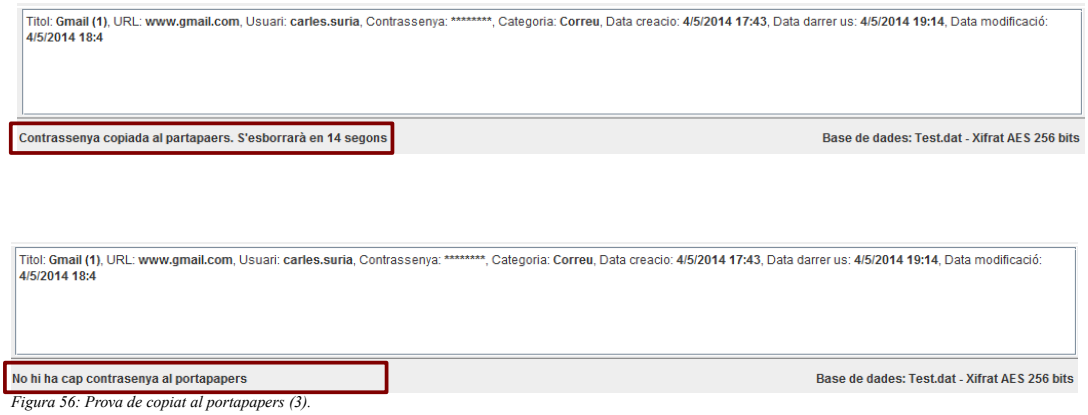


Figura 56: Prova de copiat al portapapers (3).

4.2.18 Obertura d'una URL.

Premem el botó dret del ratolí damunt una filera de la taula i si l'URL està disponible, seleccionem l'opció “Obrir URL”.

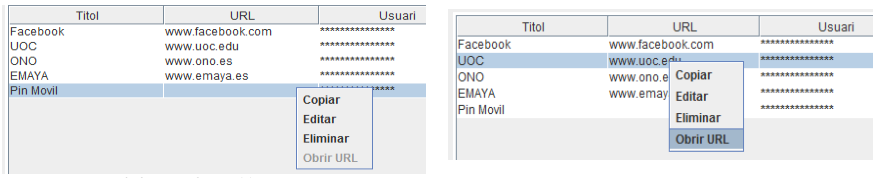


Figura 57: Prova d'obertura d'URL (1).

L'URL s'obre correctament.

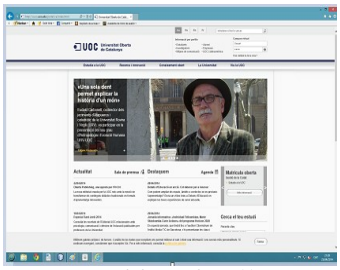


Figura 58: Prova d'obertura d'URL (2).

4.2.19 Obertura de la base de dades sense accés a la xarxa.

Per a realitzar aquesta prova es deshabilitaran totes les interfícies de xarxa de l'ordinador.

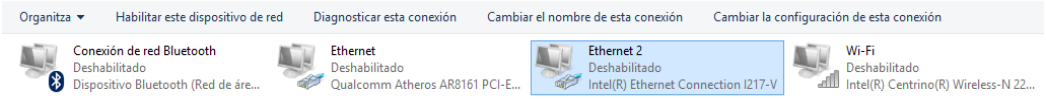


Figura 59: Prova d'obertura de la BD sense accés a la xarxa (1).

Si al obrir la base de dades amb l'opció de sincronització activada l'equip no té accés a Internet, s'adverteix l'usuari i es treballa amb la copia local.

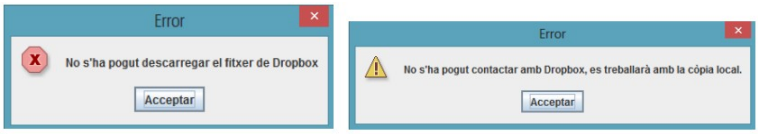


Figura 60: Prova d'obertura de la BD sense accés a la xarxa (2).

Si en aquesta situació es realitzen canvis i es volen desar, s'informa l'usuari que això podria comportar pèrdua d'informació i se li demana confirmació.

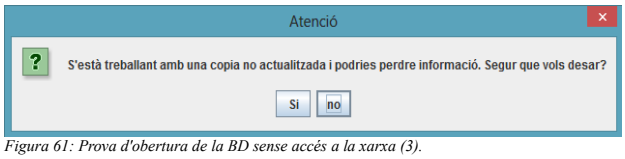
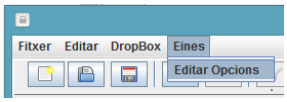


Figura 61: Prova d'obertura de la BD sense accés a la xarxa (3).

4.2.20 Edició de la configuració.

Accedim al menú “Eines – Editar opcions” per canviar la clau mestra.



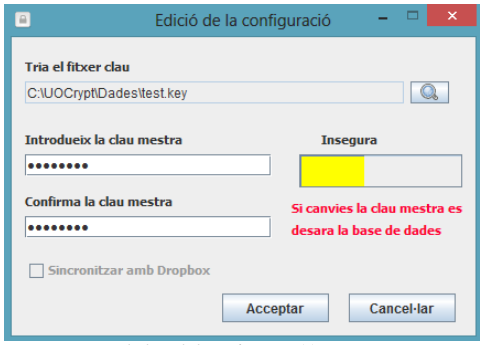


Figura 62: Prova d'edició de la configuració (1).

Introduïm la nova clau mestra.

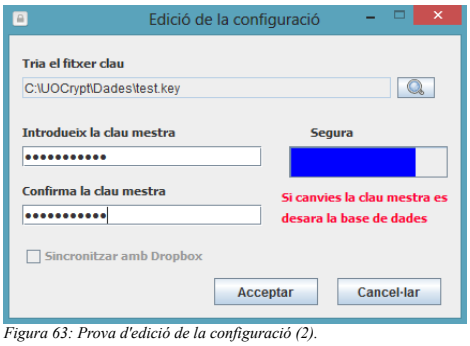


Figura 63: Prova d'edició de la configuració (2).

Escrivim la clau anterior.

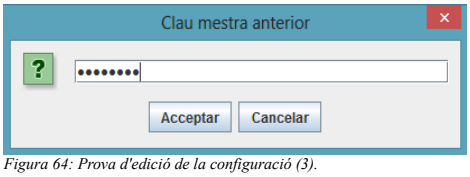


Figura 64: Prova d'edició de la configuració (3).

I comprovem que podem desxifrar correctament la base de dades amb la nova clau mestra.

També s'ha verificat que el canvi d'ubicació del fitxer clau i la sincronització amb Dropbox funciona correctament.

5 Fase de Transició.

Per a dur a terme aquesta fase, s'ha lliurat la primera versió acabada del programari a un usuari per que el provi i pugui informar-nos dels possibles errors que es vagi trobant així com fer suggerències de millora. Després d'utilitzar l'aplicació uns quants dies, l'usuari ha trobat una sèrie d'errors (un potencialment greu) i ha fet el suggeriment d'algunes millores:

5.1 Error en el sistema de xifrat.

S'ha trobat que després de canviar la clau mestra, si l'usuari sortia de l'aplicació sense desar la base de dades, ja no era possible tornar-la a recuperar.

La causa de l'error era que després del canvi de la clau mestra es tornen a generar els bits de sal i al no desar-se després la base de dades (procés que l'encripta), al intentar-la reobrir, ens trobàvem amb un fitxer xifrat amb una clau diferent (ja que estava derivada a partir d'uns bits de sal diferents).

Per solucionar aquest problema s'ha fet que al final del procés de canvi de la clau mestra, l'estat de l'aplicació es desi automàticament.

5.2 Doble xifrat al bloquejar l'espai de treball.

En equips lents, era possible prémer el botó de bloqueig vàries vegades abans de que l'aplicació es minimitzés i això provocava que les dades xifrades es tornessin a xifrar. Al desxifrar-les (només una vegada), les dades obtingudes ja no eren les correctes. Per a solucionar aquest problema s'ha fet que aquest botó es deshabiliti fins que la base de dades es torni a desencriptar.

5.3 Menús visibles en cada moment.

S'ha corregit la visualització dels menús de manera que en cada moment només estiguin habilitades les opcions possibles.

5.4 Afegir la possibilitat de canviar l'ordre de l'arbre de categories.

L'usuari ha proposat que es pugui canviar l'ordre de les categories a l'arbre. Per tant, s'han afegit les respectives opcions al menú.

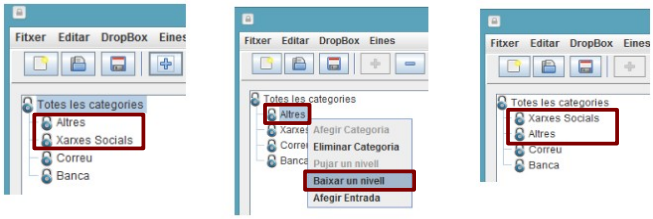


Figura 65: Canvi de l'ordre de l'arbre de categories.

5.5 Afegir la possibilitat de canviar el nom de les categories.

Una altra proposta de l'usuari ha estat afegir la possibilitat de canviar el nom de les categories la qual cosa s'ha considerat adequada i per tant, s'ha implementat.

Figura 66: Canvi del nom d'una categoria.

5.6 Ruta del fitxer clau per defecte.

S'ha afegit una ruta per defecte del fitxer clau (el directori de treball) al formulari de creació d'una nova base de dades.

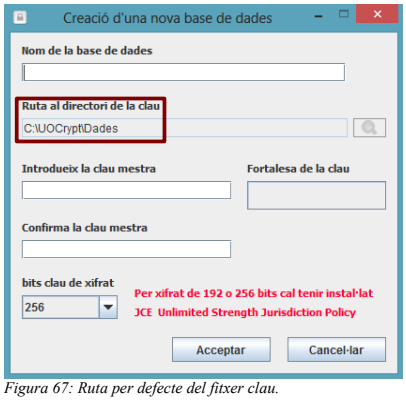


Figura 67: Ruta per defecte del fitxer clau.

6 Conclusions.

Avui dia és força comú haver de gestionar un nombre elevat de contrasenyes com, per exemple, de correu electrònic, banca electrònica, xarxes socials, tendes virtuals, subscripcions a serveis diversos, etc. El fet d'haver-les de recordar, sovint fa que adoptem actituds poc segures com contrasenyes massa curtes, utilització de paraules del diccionari, repetides per a diferents comptes, etc.

Una possible solució per a resoldre aquest problema pot ser mantenir totes les contrasenyes desades en un fitxer però això suposa que si algú altre aconsegueix accedir-hi, podrà conèixer totes les nostres credencials i suplantar-nos (accedir als nostres comptes bancaris, llegir els nostres correus, etc.). Aquest problema el podem solucionar mitjançant la criptografia, xifrant aquest fitxer amb una clau mestra (la única que cal recordar) coneguda només per nosaltres. Veiem doncs, que la criptografia pot tenir aplicacions directes a la nostra vida quotidiana encara que no sempre en siguem conscients (altres exemples podrien ser els pagaments segurs a Internet, la utilització de certificats digitals, etc.).

Per tal de facilitar la gestió del xifrat/desxifrat del fitxer que conté totes les nostres credencials, sorgiren els gestors de contrasenyes, que a més, ofereixen tota una sèrie d'utilitats com poden ser la generació automàtica de contrasenyes o l'avaluació de la fortalesa de les triades per nosaltres mateixos. Cal recordar que si algú pogués llegir aquest fitxer coneixeria totes les nostres credencials i per tant, és imprescindible triar una clau mestra el més segura possible, evitant les conductes poc segures esmentades anteriorment. Això no ha de suposar cap problema ja que com s'ha dit, aquesta és la única contrasenya que ens cal memoritzar.

En aquest projecte s'ha desenvolupat UOCrypt, un gestor de contrasenyes on s'han inclòs les principals funcions que tot programari d'aquest tipus ha d'oferir, xifrant la base de dades de credencials utilitzant el criptosistema AES. Podem afirmar que s'han assolit tots els objectius; les credencials mai es desen en clar a la memòria persistent (disc dur, memòria USB, ...), s'ha dissenyat una interfície d'usuari amb una bona usabilitat i s'han desenvolupat les funcions de sincronització amb Dropbox, tot complint els terminis establerts.

Tot i l'èxit del projecte, no ha estat exempt de dificultats, les majors de les quals han estat relacionades amb el desenvolupament de la primera aplicació amb una interfície gràfica d'usuari havent d'aprendre a utilitzar formularis i tot tipus de controls com ara botons, arbres, taules, etc. (fins al moment només s'havien creat aplicacions de consola) i per altre banda, amb la transició entre la fase de disseny i la de construcció, on per manca d'experiència s'ha hagut d'invertir molt temps i esforços, demostrant la importància de preparar detingudament i a consciència el disseny, la qual cosa ens estalviarà molta feina i maldecaps en les fases posteriors del projecte.

Malgrat que UOCrypt és una aplicació força completa, en un futur podríem afegir-hi algunes funcions més, com per exemple, la introducció automatitzada de les credencials a les URL o la gestió de mòduls per integrar-se amb altres aplicacions però això, ja serà un altre projecte ...

7 Glossari.

AES: Advanced Encryption Standard. Criptosistema Rijndael, que xifra blocs de 128 bits per mitjà d'una clau que pot variar la longitud entre 128, 192 o 256 bits.

Bits de sal: Bits aleatoris que són usats en una funció derivadora de claus, junt amb la contrasenya, per a derivar una clau criptogràfica. Aquesta aleatorietat fa que la la clau derivada sigui més resistent contra atacs de diccionari.

Blowfish: És un sistema de xifratge per blocs de clau simètrica, dissenyat el 1993 per Bruce Schneier i s'inclou en un gran nombre de paquets de xifratge i productes d'encriptació.

Criptografia: És un terme d'origen grec que prové dels mots krypto ('amagar') i grapho ('escriure'). Podem dir que la criptografia és la ciència i l'estudi de l'escriptura secreta.

Criptosistema: Sistema que ofereix mitjans segurs de comunicació amb els que l'emissor oculta o xifra el missatge abans de transmetre-ho perquè només un receptor autoritzat pugui desxifrar-ho.

NIST: Institut Nacional de Normes i Tecnologies ('National Institute of Standards and Technology') és una agència de l'Administració de Tecnologia del Departament de Comerç dels Estats Units i que ter per missió, promoure la innovació i la competència industrial als Estats Units, mitjançant avenços en metrologia, normes i tecnologia de forma que millorin l'estabilitat econòmica i la qualitat de vida.

Phishing: Tipus d'abús informàtic que es comet per mitjà de l'ús d'un tipus d'enginyeria social caracteritzat per intentar adquirir informació confidencial de forma fraudulenta (com poden esser una contrasenya o informació detallada sobre targetes de crèdit o altra informació bancaria). L'abusador es fa passar per una empresa o persona de confiança en una aparent comunicació oficial electrònica, generalment un correu electrònic, o algun sistema de missatgeria instantània.

Principi de Kerckhoffs: Estableix que la seguretat d'un criptosistema ha de recaure en la seguretat de la clau, suposant-se coneguts la resta de paràmetres.

Twofish: És un sistema de xifratge per blocs de clau simètrica amb una longitud de bloc de 128 bits i mida de la clau fins a 256 bits. Va esser un dels cinc finalistes de la competició DES. És el successor de Blowfish.

URL: De l'anglès de 'Uniform resource locator', és una seqüencia de caràcters, d'acord a un format modèlic i estàndard, que s'utilitza per a nomenar recursos d'Internet per a la seva localització o identificació, com per exemple documents textuals, imatges, vídeos, etc.

Usabilitat: Facilitat amb què la gent pot usar una eina o un giny, per aconseguir un objectiu concret. Permet més eficiència (amb menys temps es pot acabar una tasca contreta), facilitat d'aprenentatge i més satisfacció de l'usuari.

Xifratge: procediment gràcies al qual s'escriu un missatge emprant un codi secret o xifra de forma que la comprensió del missatge sigui impossible o, si més no, difícil a tota persona que no tingui la clau secreta per desxifrar-lo.

XOR: Una porta lògica digital que implementa la disjunció exclusiva, és a dir, una sortida serà alta (1) si una, i només una de les entrades es alta (1). Si les dues entrades son altes o les dues són baixes, el resultat és baix (0).

8 Bibliografia.

[1] Advanced Encryption Standard (AES). FIPS PUBS, 2001. Disponile a: <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

[2] Advanced Eccryption Standard. Viquipèida, 2013. Disponible a: <http://ca.wikipedia.org/wiki/Advanced_Encryption_Standard>

[3] Class Cipher. Oracle.com, 2013. Disponible a: <http://docs.oracle.com/javase/7/docs/api/javax/crypto/Cipher.html>

[4] Modes d'operació dels sistemes de xifratge per blocs. Viquipèdia, 2014. Disponible a: <http://ca.wikipedia.org/wiki/Modes_d'operaci%C3%B3_dels_sistemes_de_xifratge_per_blocs>

[5] Password-Based Cryptography Specification. IETF, 2000. Disponible a: <http://tools.ietf.org/html/rfc2898>

[6] PBKDF2. Viquipèdia, 2014. Disponible a: <http://en.wikipedia.org/wiki/PBKDF2>

[7] Rainbow table. Wiquipèdia, 2014. Disponible a: <http://en.wikipedia.org/wiki/Rainbow_table>

[8] Using the Core API in Java. Dropbox.com. Disponible a: <https://www.dropbox.com/developers/core/start/java>

[9] FERRER, JOSEP DOMINGO; HERRERA, JORDI; RIFÀ, HELENA. Criptografia. Universitat Oberta de Catalunya, 2006. ISBN: 84-9788-388-8

[10] Java Crypto Library. Cryptojs, 2013. Disponible a: <http://cryptojs.altervista.org/secretkey/doc/doc_aes_java.html>

[11] Comprobando la fortaleza de las contraseñas. El club del programador, 2012, Disponible a: <http://www.elclubdelprogramador.com/2012/02/19/php-comprobando-la-fortaleza-de-las-contrasenas-mejorado/>

[12] Password Strength Control. Code Project, 2010. Disponible a: <http://www.codeproject.com/Articles/59186/Password-Strength-Control>