Creació d'una APP d'encriptació i desencriptació d'imatges

Memòria del projecte Final de Màster (MISTIC)
realitzat per
Marc Forn Rodríguez
i dirigit per
Jordi Herrera Joancomartí

Terrassa, Gener de 2014

El sotasignat, ***Jordi Herrera Joancomartí***,
professora del MISTIC,

CERTIFICA:

Que el treball al que correspon la present memòria
ha estat realitzat sota la seva direcció
per en ***Marc Forn Rodríguez***
I per a que consti firma la present.
Terrassa, ***Gener*** de ***2014***

Signat: ***Jordi Herrera Joancomartí***

Index

1. Introducció

Actualment la majoria de dispositius mòbils tenen càmeres de fotos que s'utilitzen durant el dia a dia de milers d'usuaris, totes aquestes imatges queden emmagatzemades dins el telefon. En el cas de que el nostre telefon sigui robat o algun usuari maliciós accedís al terminal podria consultar tota la informació que tenim a dins el telefon. Es per això que cada dia és mes importat no només protegir l'accés als terminals amb una password o un patró (molts cops fàcilment esbrianble) sinó que es gairebé una obligació encriptar les dades que es troben en l'interior del terminal, perquè en el cas que algun usuari maliciós tingués accés al terminal no pugui accedir a la informació que es troba dins del terminal.

Per dur a terme el projecte utilitzarem els llenguatges de programació següents: Android i Java.

1.1 Objectius generals

L'objectiu principal que volem aconseguir amb el desenvolupament d'aquest projecte és la de crear una aplicació mòbil per a dispositius Android capaç de prendre imatges, encriptar-les dins el terminal i posteriorment desencriptar-les i mostrar les imatges originals. En el cas de que la password de desencriptació sigui incorrecte es mostrarà una imatge que res tindrà a veure amb l'original.

1.2 Estat Actual

En l'actualitat existeix diverses aplicacions que realitzen funcionalitats semblants a les que es volen implementar en aquest projecte, algunes d'elles són:

TSP (Top Secret Picture):
https://play.google.com/store/apps/details?id=feipeng.ultimatesecret1
Aquesta APP permet encriptar/desencriptar les imatges que tens el dispositiu Android. Té un

explorador de fitxers intern per a poder visualitzar totes les imatges encriptades.

Aquesta versió es troba actualment sense suport ja que s'ha desenvolupat una nova aplicació de pagament.

SecPhoto:
https://play.google.com/store/apps/details?id=kr.co.bitek.securephoto
El funcionament és semblant a l'aplicació anterior, amb la diferència que permet crear una contrasenya per a cada imatge, enlloc d'una genèrica per a totes les imatges que es vulguin encriptar.

1.3 Motivacions

Una de les principals motivacions a l'hora de triar aquest projecte era que volia millorar els coneixements actuals sobre desenvolupament d'aplicacions mòbils, fusionant els coneixements adquirits els darrers mesos en Android amb el temari aprés durant el MISTIC. JA que voldria centrar el meu futur professional en el desenvolupament d'aplicacions per a dispositius mòbils i la seguretat en aquest àmbit no es tant forta com hauria de ser-ho.

1.4 Estructura de la memòria

La memòria es divideix en 8 capítols:

El primer capítol és aquesta introducció, s'explica el títol del projecte, els objectius que s'han de complir i quin és l'estat actual del projecte que volem desenvolupar. En l'apartat motivacions es parla de quines coses ens han fet arribar a l'elaboració d'aquest projecte

En el segon capítol es tracten els objectius concrets del projecte, les seves funcionalitats, l'anàlisi de costos, el pressupost del projecte i els riscos que poden sorgir durant l'elaboració d'aquest, així com les seves solucions.

En el tercer capítol es detalla l'anàlisi de requeriments, que engloba els requisits funcionals del nostre projecte, juntament amb els requisits no funcionals.

En el capítol quatre s'explica el disseny a fons; com està estructurada les diverses funcionalitats de l'APP (algoritmes i directori d'imatges).

En el capítol cinc s'explica com funciona la Interfície de l'aplicació, com l'usuari interactua amb ella i com aquesta interactua amb l'aplicació en si.

En el sisè capítol es tracta tots els temes referents al desenvolupament de l'aplicació, es parlarà dels factors que han afavorit al desenvolupament d'aquest i també es citaran les dificultats que hem trobat a l'hora de dur-lo a terme. També tractarem quines millores podríem dur a terme en el nostre projecte per fer-lo més eficient o reduir costos.

En el setè capítol extreure'm les conclusions del projecte, quines coses hem après, quines podríem haver millorat, quins problemes ens hem trobat i com hem pogut solucionar-los.

En el capítol vuit, mencionarem totes les fonts que hem emprat per a dur a terme aquest projecte i aquesta memòria, juntament amb les definicions dels tecnicismes emprats en l'elaboració del projecte complet.

2. Estudi de Viabilitat

En aquest capítol es tractarà amb detall la viabilitat d'aquest projecte. Analitzarem que es vol realitzar i amb quines eines ho farem. També tindrem en compte quins han de ser els requisits que el nostre projecte ha de complir i estudiarem amb quins recursos comptem per dur-lo a terme i per últim analitzarem els costos de personal i eines que en faran falta.

2.1 Objectius del projecte

Els objectius del projecte són els següents:

1- Crear una aplicació que permeti prendre imatges i emmagatzemar la seva informació real de forma secreta.

2- La imatge presa ha de seguir sent una imatge, encara que no es conegui la clau secreta (es mostrarà soroll).

3- Fàcil comprensió i ús de la interfície de l'APP per part de l'usuari final.

Objectius	Objectiu 1	Objectiu 2	Objectiu 3
Crítics	✸		
Prioritaris		✸	✸
Secundaris			

2.2 Parts Interessades

Les parts interessades en el projecte són les que es llisten a continuació:

* Usuari amb un dispositiu Android que vulgui mantenir les seves imatges emmagatzemades de forma segura.

* Empreses o entitats que vulguin mantenir i/o enviar les seves imatges de forma segura a terminals mòbils sota al sistema operatiu Android.

2.3 Producte i documentació

El projecte obtingut és una Aplicació mòbil per a dispositius Android on qualsevol usuari que disposi d'un terminal amb Android hi podrà accedir. Juntament amb l'aplicació mòbil també es lliurà la memòria d'aquest projecte. On es tracten tots els temes importants que s'han tingut en compte a l'hora de la creació del projecte.

2.4 Planificació del projecte

El projecte es desenvoluparà des del Setembre de 2013 al Gener 2014, amb una dedicació de 18 hores setmanals. Amb un total d'hores dedicades al projecte de 300 hores.

Data començament: 1 Setembre 2013
Data finalització: 3 Gener 2013
Eines de planificació: Microsoft Project

2.4.1 Recursos del projecte

En la següent taula podem observar els costos, en quan a recursos, del projecte. Tenim tres recursos diferents, el cap del projecte, que s'encarregarà que el projecte es dugui a terme correctament, l'analista que analitzarà totes les tasques que s'hauran de fer i per ultim un programador/Provador que s'encarregara d'implementar el codi perquè l'aplicació sigui una realitat. En el nostre cas, els tres recursos serà la mateixa persona, ja que al ser un projecte de fi de màster només tenim un recurs humà.

Recursos humans	**Valoració**
Cap del projecte	*100 €/h*
Analista	*50 €/h*
Programador / Provador	*35 €/h*

* Recursos materials: S'utilitzaran els recursos materials disponibles en la zona de treball de l'alumne. Tot el desenvolupament es farà utilitzant programari de domini

públic.

* Costos indirectes: amortització dels recursos de desenvolupament. S'utilitzarà l'ordinador propi de l'alumne per abaratir costos del projecte. Els únics costos indirectes que trobarem seran: la connexió a Internet i la corrent que consumeixi l'ordinador.

2.4.2 Planificació temporal

En la següent gràfica es mostren les tasques del projecte juntament amb les dates previstes d'inici i acabament.

Taques	Sub-Tasques	Inici	Finalització
Inici del projecte		01/09/13	01/09/13
Planificació			
	Estudi de Viabilitat	01/09/13	15/09/13
	Valoració E.V.	15/09/13	16/09/13
Analisis de la APP			
	Analisis de requisits	16/09/13	17/09/13
	Analisis de dades	17/09/13	18/09/13
	Analisis de seguretat	18/09/13	25/09/13
	Analisis de legalitat	25/09/13	26/09/13
	Documentació	26/09/13	29/09/13
Disseny de la APP			
	Disseny de la interificie	29/09/13	02/10/13
	Disseny de la lògica interna	02/10/13	08/10/13
	Disseny de les proves	08/10/13	12/10/13
	Documentació del disseny	12/10/13	14/10/13
	Revisió del disseny	14/10/13	16/10/13
Desenvolupament APP			
	Preparació entorn desenvolupament	16/10/13	16/10/13
	Configuració Eclipse + Android SDK	16/10/13	16/10/13
	Creació interficie	16/10/13	20/10/13
	Creació lògica	20/10/13	28/10/13
Testing			
	Proves unitaries	28/10/13	01/11/13
	Proves d'integració	01/11/13	13/11/13
	Proves de riscos	12/11/13	13/11/13
	Proves d'stress	13/11/13	15/11/13
	Documentació de desenvolupament	15/11/13	02/12/13
	Prova Global	02/12/13	08/12/13
Implantació			
	Instal·lació	08/12/13	08/12/13
	Proves reals	08/12/13	10/12/13
Memoria TFM		10/12/13	03/01/14
Tancament TFM		03/01/14	03/01/14
Defensta del TFM		03/01/14	10/01/14

2.5 Pressupost

En aquest apartat tractarem els costos econòmics del projecte, tant pel que fa als recursos humans com als recursos tècnics.

2.5.1 Estimació cost de personal

En la següent taula podem veure desglossat els costos de cada un del personal que durà a terme l'aplicació.

	Task Name	Fixed Cost	Fixed Cost Accrual	Total Cost	Baseline	Variance	Actual	Remaining
1	Inici Projecte: Matriculació	0,00 €	Prorated	200,00 €	0,00 €	200,00 €	0,00 €	200,00 €
2	**Planificacio**	**0,00 €**	**Prorated**	**3.600,00 €**	**0,00 €**	**3.600,00 €**	**0,00 €**	**3.600,00 €**
5	**Analisis de l'aplicació w**	**0,00 €**	**Prorated**	**1.238,46 €**	**0,00 €**	**1.238,46 €**	**0,00 €**	**1.238,46 €**
12	**Disseny de l'aplicació**	**0,00 €**	**Prorated**	**1.100,50 €**	**0,00 €**	**1.100,50 €**	**0,00 €**	**1.100,50 €**
19	**Desenvolupament Aplic**	**0,00 €**	**Prorated**	**13.860,00 €**	**0,00 €**	**13.860,00 €**	**0,00 €**	**13.860,00 €**
26	**Testing**	**0,00 €**	**Prorated**	**1.610,50 €**	**0,00 €**	**1.610,50 €**	**0,00 €**	**1.610,50 €**
33	**Implantació**	**0,00 €**	**Prorated**	**1.387,50 €**	**0,00 €**	**1.387,50 €**	**0,00 €**	**1.387,50 €**
37	Memoria Final Projecte	0,00 €	Prorated	5.000,00 €	0,00 €	5.000,00 €	0,00 €	5.000,00 €
38	Tancament Projecte	0,00 €	Prorated	100,00 €	0,00 €	100,00 €	0,00 €	100,00 €
39	Defensa del projecte	0,00 €	Prorated	500,00 €	0,00 €	500,00 €	0,00 €	500,00 €

2.5.2 Estimació cost recursos

En la següent taula podem observar quins són els costos dels recursos, així com el període d'amortització i el període d'utilització.

	Cost amortització	Cost unitari	Període amortització	Període utilització
Pc Programador	100.00 €	1,200.00 €	500h	250h
MS Project	30.00 €	360.00 €	4h	1h
Programari lliure	0.00 €	0.00 €	Des de l'inici	250

2.5.3 Resum i anàlisis cost benefici

A continuació es mostra la suma tota dels costos:

Cost desenvolupament software: 20000€
Cost amortització material: 500€

Cost total(aprox.): 20.500€

2.6 Avaluació de riscos

En aquest apartat tractarem tots els problemes que poden sorgir durant l'elaboració del projecte, quin grau de perill té cadascun i que podem fer per evitar-los.

2.6.1 Llista de riscos

R1. Planificació temporal optimista: estudi de viabilitat. No s'acaba en la data prevista, augmenten els recursos.

R2. Manca alguna tasca necessària: estudi de viabilitat. No es compleixen els objectius del projecte.

R3. Pressupost poc ajustat: estudi de viabilitat. Menys qualitat, pèrdues econòmiques.

R4. Canvi de requisits: estudi de viabilitat, anàlisi. Endarreriment en els desenvolupament i resultat.

R5. Equip del projecte massa reduït: estudi de viabilitat. Endarreriment en la finalització del projecte, no es compleixen els objectius del projecte.

R6. Eines de desenvolupament inadequades: implementació. Endarreriment en la

finalització del projecte, menys qualitat, ...

R7. Manquen requisits o són inadequats, endarreriments, insatisfacció usuaris.

R8. No es fa correctament la fase de test: desenvolupament, implantació. Manca de qualitat, deficiències en l'operativa, insatisfacció usuaris, pèrdua econòmica.

R9. Incompliment d'alguna norma, reglament o legislació: en qualsevol fase. No es compleixen els objectius, repercussions legals.

R10. Manca d'implantació de mesures de seguretat: estudi de viabilitat, anàlisi, desenvolupament. Pèrdua d'informació, incompliment legal, pèrdues econòmiques.

R11. Abandonament del projecte abans de la finalització: en qualsevol fase. Pèrdues econòmiques, frustració.

2.6.2 Catalogació de riscos

En la següent taula podem veure quina es la probabilitat de que cada esdeveniment es produeixi i quin seria l'impacte en el projecte de cada una d'elles.

	Probabilitat	**Impacte**
R1	Alta	Crític
R2	Alta	Crític
R3	Alta	Crític
R4	Alta	Marginal
R5	Alta	Crític
R6	Baixa	Crític
R7	Baixa	Crític
R8	Alta	Crític
R9	Mitjana	Crític
R10	Alta	Crític

R11	Mitjana	Catastròfic

2.6.3 Pla de contingència

En la següent taula es tracten les possibles solucions a cada risc.

	Solució que cal adoptar
R1	Ajornar alguna funcionalitat, afrontar possibles pèrdues, fer una assegurança.
R2	Revisar l'estudi de viabilitat, modificar la planificació.
R3	Re-negociar amb el client, afrontar possibles pèrdues, fer una assegurança.
R4	Re-negociar amb el client, ajornar funcionalitat, modificar planificació i pressupost.
R5	Demanar un ajornament, negociar amb el client, afrontar pèrdues.
R6	Millorar la formació de l'equip, preveure eines alternatives, millorar la qualitat.
R7	Fixar un calendari de reunions, millorar el contacte amb el client.
R8	Dissenyar els test amb antelació, realitzar tests automàtics, negociar contracte de manteniment, donar garanties, afrontar pèrdues econòmiques.
R9	Revisar les normes i legislació, consultar un expert, afrontar possibles repercussions penals.
R10	Revisar la seguretat en cada fase, aplicar polítiques de seguretat actives.
R11	No té solució.

2.7 Conclusió de l'Estudi de Viabilitat

La conclusió que podem extreure un cop fet l'estudi de viabilitat i valorant totes les opcions, és que el projecte es viable i per tant es tirarà endavant.

3. Anàlisis de requeriments

En aquest capítol tractarem tots els requisits que la nostra aplicació ha de complir, ja siguin funcionals o no funcionals.

En les següents figures es mostren els esquemes de funcionament de l'aplicació.

3.1 Requisits funcionals

A continuació es llisten totes les funcionalitats que ha de tenir la nostra aplicació.

a) Capturar imatges amb la càmera:
L'aplicació ha de ser capaç d'invocar a la càmera del sistema, prendre una foto i que aquesta sigui accessible des de la nostre APP

b) Encriptació de l'imatge presa:
S'ha de sol·licitar una password per la imatge presa, que posteriorment s'utilitzarà per encriptar la imatge.

c) Desencriptació d'imatges:
S'ha de sol·licitar una password per la imatge que es vulgui visualitzar, que posteriorment s'utilitzarà per desencriptar la imatge. En el cas de que la password sigui la correcte es mostrarà la imatge original, en cas contrari es mostrarà la imatge amb “soroll”.

d) La imatge encriptada haurà de seguir sent una imatge:
L'aplicació ha de permetre visualitzar la imatge encriptada i mostrar-la com si aquesta fos una imatge (per efectuar aquesta acció s'afegirà una capçalera bitmap en el proces d'encriptació, per davant de tot el fitxer encriptat).

e) Visualitzar la imatge encriptada a través d'un visor d'imatges:
L'APP ha de permetre visualitzar totes les imatges encriptades, a traves del visor

d'imatges propi d'Android, emmagatzemades en el terminal. Per aquest cas s'haurà de poder visualitzar la imatge amb “soroll”.

3.2 Requisits no funcionals

A continuació es llisten els requisits que ha de complir l'aplicació i que no tracten cap funcionalitat d'aquesta.

a) Compliment de la LOPD:
L'aplicació ha de respectar tota la informació que es guardi en ella i que no es vulneri cap llei de protecció de dades pel que fa als usuaris de l'aplicació

b) Tolerància a errades i accions incorrectes:
L'aplicació ha de suportar possibles accions incorrectes per part de l'usuari, ja que aquest al no tenir nocions de programació podria cometre fàcilment algun error. Aquest ha d'estar contemplat per la nostra aplicació i minimitzat al màxim.

c) La seguretat de les imatges:
L'aplicació haurà d'emmagatzemar les imatges encriptades correctament per que un usuari maliciós no tingui accés a a aquestes i a la informació que es guarda en elles

3.3 Restriccions del sistema

a) El projecte ha d'estar finalitzat abans del 03 Gener 2014:
El projecte ha d'estar acabat abans del 3 de Gener del 2014, per a poder finalitzar els estudis en aquesta data.

b) L'aplicació s'ha de desenvolupar utilitzant programari lliure:
Totes les eines que s'utilitzaran per la creació d'aquest projecte han de ser de programari lliure, ja sigui el sistema operatiu sobre el que codificarem l'aplicació (Debian) o els terminals sobre els que correrà l'APP (Android). S'utilitzarà

programari lliure per abaratir costos de construcció i per seguir la filosofia del software lliure.

3.4 Catalogació i priorització dels requisits

En la següent taula es pot observar la prioritat de cada requisit funcional.

Requisits funcionals	RF a	RF b	RF c	RF d	RF e
Essencial	✸	✸	✸		
Condicional				✸	
Opcional					✸

En la següent taula es pot observar la prioritat de cada requisit no funcional.

No Funcionals	RNF a	RNF b	RNF c
Essencial	✸		✸
Condicional		✸	
Opcional			

4. Disseny de la APP

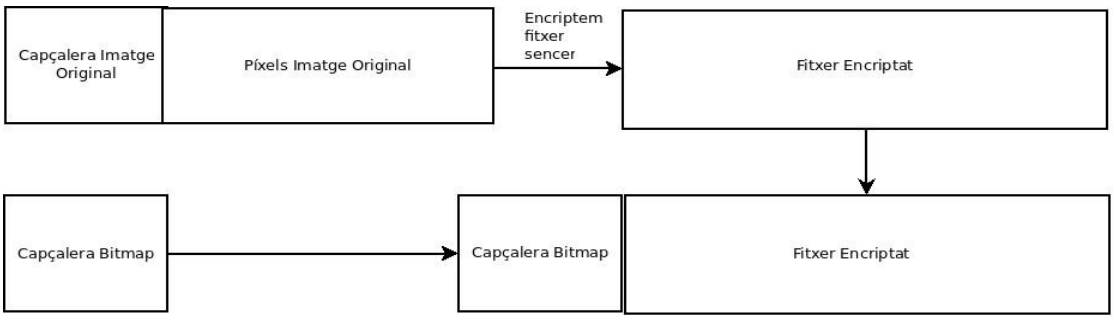
En aquest capítol s'expliquen els aspectes tècnics del projecte. Veurem les diferents funcionalitats que haurà d'implementar la APP juntament amb els algoritmes de seguretat utilitzats en el tractament de les imatges.
Parlarem també del funcionament de l'aplicació i comentarem els diferents casos d'us.

4.1 Esquema de l'Aplicació

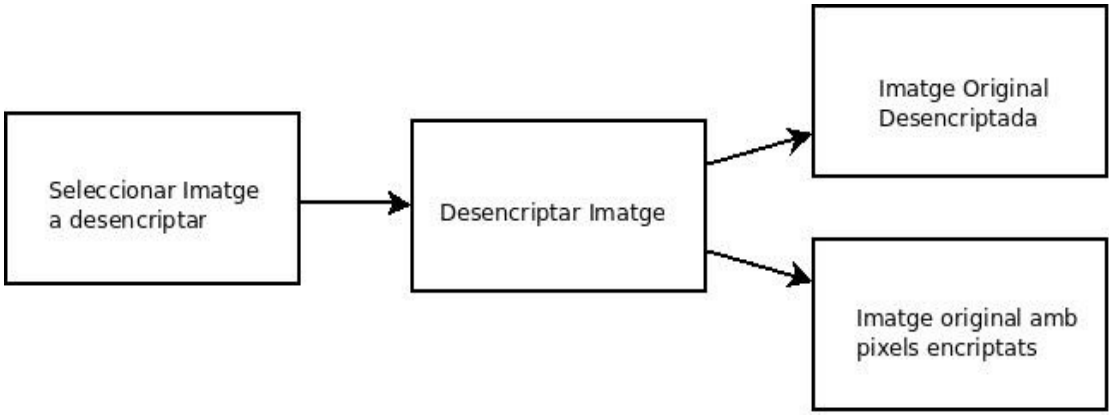
En les següents figures es mostren els esquemes de funcionament de l'aplicació.

En la primera imatge podem veure quins són els passos que s'hauran de seguir per prendre una imatge i posteriorment encriptar-la. En el pas d'encriptació d'imatges s'ha d'encriptar tot el fitxer (imatge més capçaleres) i posteriorment s'ha d'afegir una capçalera bitmap al fitxer resultat de l'encriptació. De manera que el fitxer que tindrem ara seguirà sent una imatge però la informació d'aquesta estarà encriptada i únicament es mostrarà soroll.

En el següent esquema podem observar quins són els passos que haurà de seguir l'APP per encriptar una imatge i que aquesta segueixi sent una imatge. Afegint-hi una capçalera bitmap a tot el fitxer encriptat per a que el fitxer final segueixi sent una imatge i aquest es pugui obrir amb qualsevol visualitzador d'imatges (mostrant-se una imatge que no té res a veure amb l'imatge original).



En el següent diagrama podem observar quins són els passos a seguir per a desencriptar una imatge prèviament encriptada amb Secure Photo. En el cas de que la clau de desencriptació sigui incorrecte s'haurà de mostrar una imatge amb soroll, que correspondrà a la informació de la imatge original encriptada més una capçalera de bitmap.



4.2 Seguretat de l'Aplicació

Per realitzar l'encriptació de les imatges s'ha utilitzat el mètode de criptografia simètrica, que consisteix en utilitzar una mateixa clau per a xifrar i desxifrar missatges. Les dues parts que es comuniquen han de conèixer amb anterioritat quina és la clau utilitzada per encriptar la imatge. Aquest sistema de xifrat posa tota la seguretat en la clau i no en l'algoritme, de manera que si algun atacant coneix l'algoritme utilitzat no podrà desxifrar la imatge si no coneix la clau d'encriptació.

Degut a que tota la seguretat es troba en la clau és molt important que aquesta sigui molt difícil d'esbrinar. Els algoritmes de xifrat moderns com AES (Advanced Encryption Standard) utilitzen claus de 128 bits, el que significa que existeixen 2 elevat a 128 possibles claus.

4.2.1. Algoritme de generació de la clau de xifrat

L'algoritme utilitzat per obtenir la clau de xifrat és el següent:

```
public static byte[] getRaw(String password_) throws Exception {

        byte[] keyStart = password_.getBytes();
        KeyGenerator kgen = KeyGenerator.getInstance("AES");
        SecureRandom sr = SecureRandom.getInstance("SHA1PRNG", "Crypto");
        sr.setSeed(keyStart);
        kgen.init(128, sr);
        SecretKey skey = kgen.generateKey();
        byte[] key = skey.getEncoded();

        return key;
}
```

a) En aquest algoritme primer de tot es passa la clau introduïda per pantalla en format String, a un array de bytes.

b) A continuació es crea un objecte KeyGenerator amb una instancia AES.

c) Posteriorment es crea un objecte de tipus SecureRandom, indicant l'algoritme (SHA1PRNG) i el proveïdor utilitzat (CRYPTO).

d) Establim la llavor (setSeed()) del generador de claus. Una contrasenya diferent

proporcionarà una llavor diferent i per tant una clau de xifrat diferent.

e) Un cop establida la llavor inicialitzem l'objecte KeyGenerator amb la longitud de la clau indicada (128 bits) i l'objecte SecureRandom que conté la llavor amb la clau d'encriptació introduïda.

f) Després generem un objecte de tipus SecretKey amb les característiques de l'objecte KeyGenerator inicialitzat en el punt anterior. Després convertim aquest objecte a una array de bytes i obtenim una clau d'encriptació/desencriptació.

4.2.2. Algoritme d'encriptació

L'algoritme utilitzat per encriptar les imatges és el següent.

```
public static byte[] encrypt(byte[] raw, byte[] clear) throws Exception {

        SecretKeySpec skeySpec = new SecretKeySpec(raw, "AES");
        Cipher cipher = Cipher.getInstance("AES");
        cipher.init(Cipher.ENCRYPT_MODE, skeySpec);
        byte[] encrypted = cipher.doFinal(clear);
        return encrypted;
}
```

En aquest algoritme li passem la clau d'encriptació, prèviament generada (veure punt anterior) i un array de bytes amb la informació a encriptar, en aquest cas l'array de bytes correspon a una imatge.

a) Es crea un objecte SecretKeySpec indicant quina és la clau d'encriptació i quin algoritme de xifrat s'utilitzarà.

b) Es crea un objecte Cipher indicant en la seva instanciació que l'algoritme de xifrat utilitzat es l'AES.

c) S'inicialitza l'objecte Cipher indicant que es troba en mode d'encriptació e indicant també l'objecte a encriptar.

d) Es finalitza l'encriptació i es retorna una array de bytes amb la informació encriptada.

4.2.3. Algoritme de desencriptació

L'algoritme utilitzat per desencriptar les imatges és el següent.

```
public static byte[] decrypt(byte[] raw, byte[] encrypted) throws Exception
{
	SecretKeySpec skeySpec = new SecretKeySpec(raw, "AES");
	Cipher cipher = Cipher.getInstance("AES");
	cipher.init(Cipher.DECRYPT_MODE, skeySpec);
	byte[] decrypted = cipher.doFinal(encrypted);
	return decrypted;
}
```

En aquest algoritme li passem la clau de desencriptació i un array de bytes amb la informació a desencriptar.

a) Es crea un objecte SecretKeySpec indicant quina és la clau de desencriptació i quin algoritme de xifrat s'utilitzarà.
b) Es crea un objecte Cipher indicant en la seva instanciació que l'algoritme de xifrat utilitzat es l'AES.
c) S'inicialitza l'objecte Cipher indicant que es troba en mode de desencriptació e indicant també l'objecte a desencriptar.
d) Es finalitza la desencriptació i es retorna una array de bytes amb la informació desencriptada. En el cas de que la clau de desencriptació introduïda sigui incorrecte l'algoritme retorna una Exception (Bad Padding Exception) que es tractada per l'aplicació per mostrar la imatge amb soroll enlloc de la imatge original que es mostraria en cas de que la desencriptació finalitzi correctament.

5. Interfície de l'aplicació

La interfície és la capa que se situa entre l'usuari final i l'aplicació. És la que permet interactuar a l'usuari amb la lògica de l'aplicació d'una manera senzilla. A continuació, es mostren alguns exemples de la interfície, com l'usuari interactua amb ella i finalment com ella interactua amb l'aplicació en sí.

5. Pantalles de l'aplicació

5.1 Estructura general de la Interfície

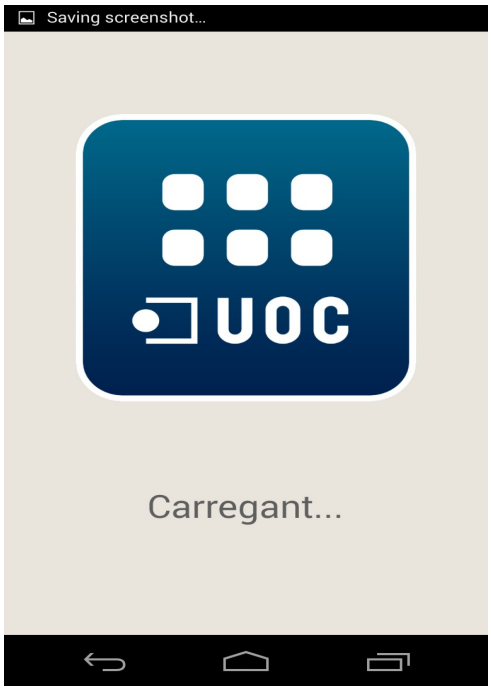
La nostra aplicació té una aparença senzilla, no està carregada de botons i tota la informació essencial es pot trobar amb un cop d'ull en el menú desplegable (Navigation Drawer)

Hem utilitzat Layouts atractiu a la vista, per això hem creat l'aplicació sobre un fons blanc i un menú de navegació amb una textura vermella. Tots els colors e icones escollides han estat analitzades amb detall i respecten la política de privacitat de les imatges (totes elles sota la llicencia Creative Commons per a us no comercial).

En la barra superior, a la part esquerra hem col·locat el logo de la APP, i al costat el nom de l'Activity sobre la que ens trobem.

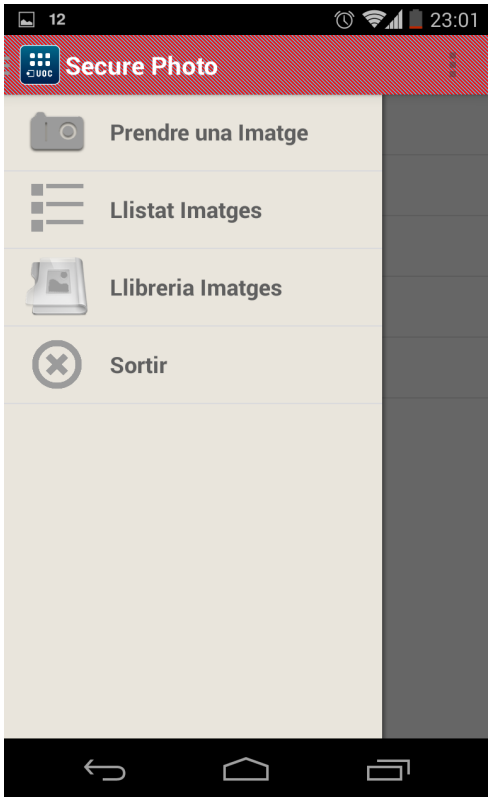
En la part central del Layout hem col·locat totes les Activities i Fragments dels que disposa la APP.

5.2 Pagina de Carrega



Aquesta és la primera pàgina (o Activity) que es mostra en obrir l'aplicació. En aquesta Activity es carrega tota la informació i es verifiquen totes les funcionalitats per a verificar que el terminal pot executar Secure Photo sense cap problema. El temps de visualització d'aquesta Activity depèn de la capacitat de processat del terminal

5.3 Menú Inicial



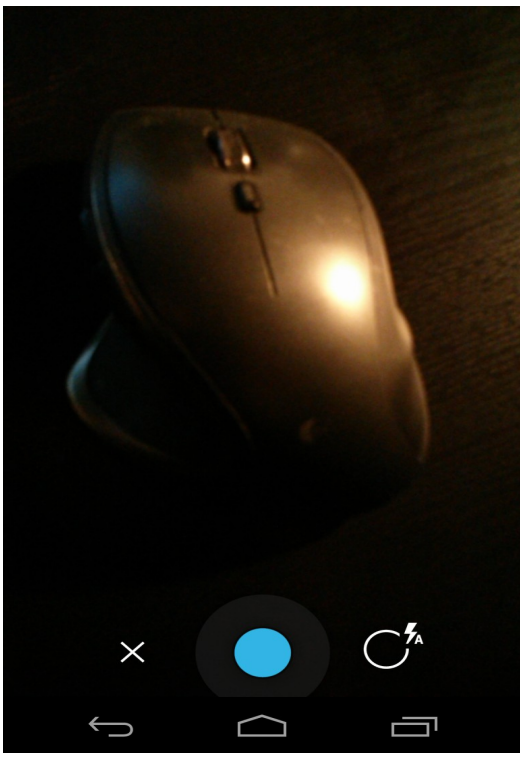
Aquesta Activity es carrega un cop les comprovacions de la pàgina de carrega finalitzen correctament. En el menú inicial podem observar les 3 funcionalitats bàsiques de la APP.

La primera d'elles (Prendre una imatge) es prendre una imatge.

La segona (Llistat Imatges) ens permet llistar totes les imatges que hem encriptat amb Secure Photo.

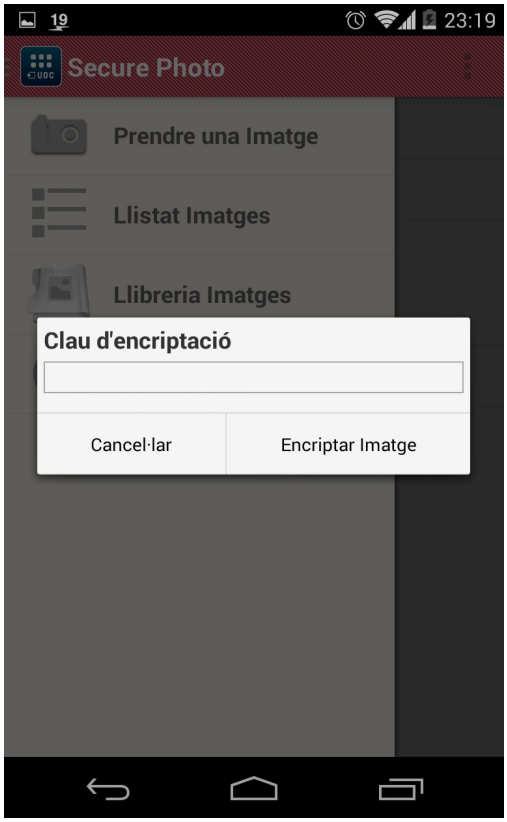
I la tercera funcionalitat (Llibreria Imatges) ens permet obrir el visor d'imatges d'Android amb les imatges encriptades anteriorment amb Secure Photo. Si clickem en aquesta funcionalitat únicament veurem les imatges amb soroll.

5.4 Prendre una imatge (1)



Aquesta funcionalitat permet invocar la càmera del sistema per a prendre una imatge. Un cop hem capturat la imatge que volem apareix un menú per introduir la clau d'encriptació.

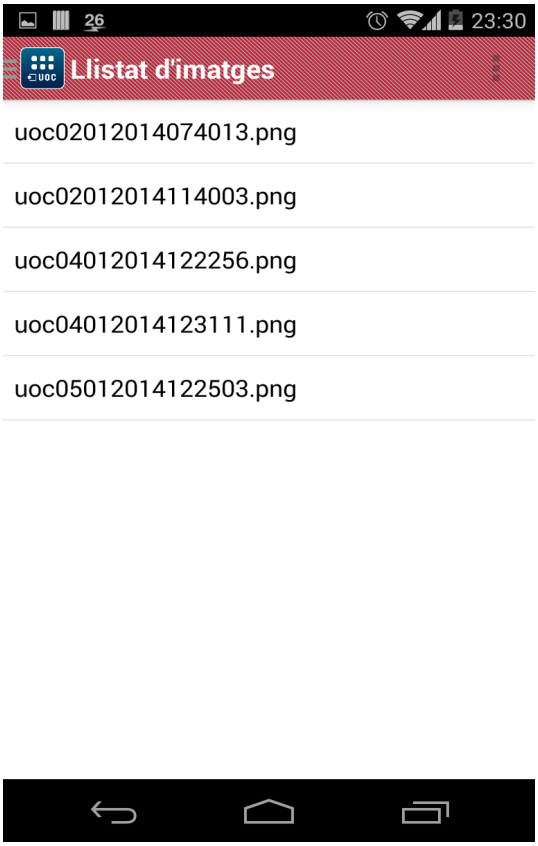
5.5 Prendre una imatge (2)



En aquesta pantalla s'ens sol·licita una clau d'encriptació per l'imatge presa. Si introduïm una clau de menys de 4 caràcters o major a 8 caràcters l'APP ens mostra un missatge indicant que la longitud de la clau ha d'estar compresa entre 4-8 caràcters.

Un cop inserim correctament una clau d'encriptació i encriptem la imatge ens apareix l'Activity amb el llistat d'imatges encriptades amb Secure Photo.

5.6 Llistat d'imatges (1)



En aquesta pantalla podem observar quantes i quines són les imatges encriptades amb Secure Photo. Podem observar com els noms de les imatges encriptades corresponen al prefix “uoc” més un timestamp per evitar imatges duplicades.

Si clickem sobre alguna de les imatges s'ens demanarà la clau de desencriptació d'aquesta (veure Llistat d'imatges 2).

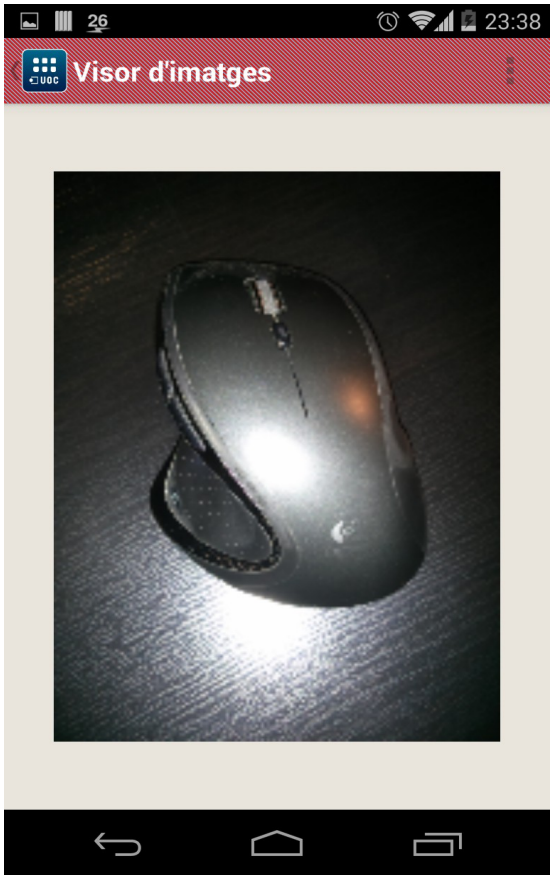
5.7 Llistat d'imatges (2)

En aquesta pantalla s'ens sol·licita la clau de desencriptació de la imatge. Si introduïm una clau de menys de 4 caràcters o major a 8 caràcters l'APP ens mostra un missatge indicant que la longitud de la clau ha d'estar compresa entre 4-8 caràcters.

Un cop inserim correctament una clau de desencriptació la APP desencriptarà la imatge. Si el procés de desencriptació ha finalitzat correctament es mostrarà la imatge original (Visor d'Imatges 1), en cas contrari es mostrarà la imatge amb els

píxels encriptats (Visor d'Imatges 2).

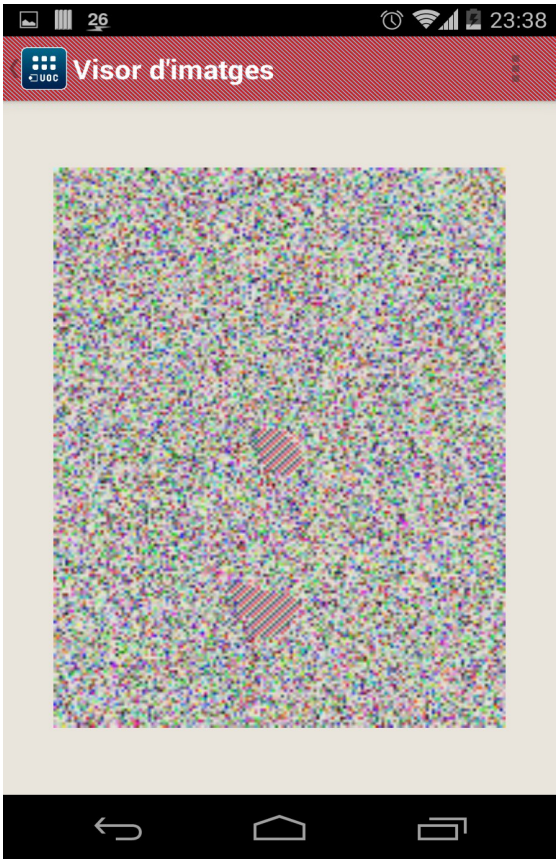
5.8 Visor d'imatges (1)



En aquesta pantalla hem implementat un visor d'imatges per la imatge escollida en el llistat d'imatges. En cas de que la imatge sigui correctament desencriptada, degut a que s'ha introduït correctament la clau de desencriptació, es mostrarà la imatge original.

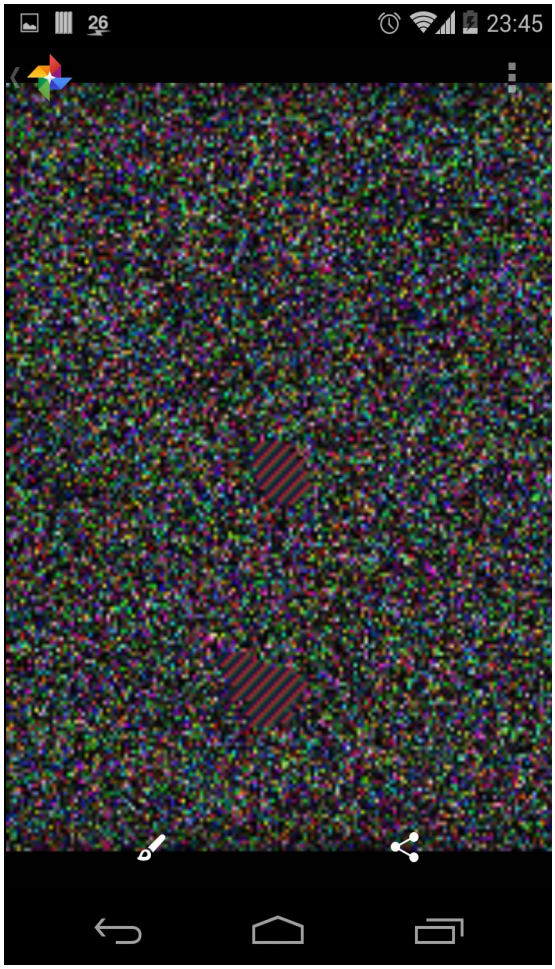
En cas contrari es mostrarà la imatge original amb els píxels encriptats, amb soroll (veure Visor d'Imatges 2).

5.9 Visor d'imatges (2)



En el cas de que la clau de desencriptació sigui incorrecte es mostrarà la imatge original amb els píxels encriptats, preservant d'aquesta manera la imatge real oculta en l'imatge mostrada.

5.10 Llibreria d'imatges (2)



En aquesta pantalla s'invoca directament el visor d'imatges intern d'Android. Podem observar com les imatges mostrades es troben totes amb soroll, degut a que aquestes es troben encriptades. Si ens fixem en l'imatge mostrada actualment podrem verificar que és la mateixa que la del nostre visor d'imatges (degut a que la imatge és la mateixa).

6. Execució del projecte

En aquest capítol s'explica com ha sigut l'execució del projecte, els problemes sorgits, com els hem resolt, les coses que hem apres i finalment s'enumeren les possibles millores que es podrien fer més endavant.

6.1 Problemes sorgits

Durant l'elaboració de qualsevol projecte, l'aparició de problemes és un tema impossible d'esquivar. En aquest apartat explicarem tots el problemes que hem trobat a l'hora de la creació de la nostra APP. Ja siguin problemes de codificació com problemes d'execució.

6.1.1. Problema logístic

Amb el primer problema que ens vam trobar va ser on executar la APP, ja que el sistema operatiu Android es troba en més de 2.000 terminals diferents, i el comportament de les APP's no és el mateix en tots. Per això es va optar per executar la APP en un Nexus 4 (dispositiu que dona menys problemes als desenvolupadors Android). Posteriorment s'han hagut de fer algunes adaptacions per a que funcionés en la resta de terminals (p.e: Samsung Galaxy S3).

6.1.2. Problema Recursos

El següent problema que hem vaig trobar va ser l'aprenentatge dels diversos llenguatges de programació involucrats en el projecte. Els meus coneixements

de tots els llenguatges utilitzats en la creació d'aquesta aplicació eren bàsics, era tot el que havia après en els meus estudis universitaris i les meves estones lliures, ja que en la feina actual no treballo amb les tecnologies aquí involucrades.
Per poder aprofundir més en el temari i conèixer més els llenguatges vaig tenir que accedir a diversos recursos web, com serien manuals i exemples d'APP's. Aquests recursos van ser contrastats diverses vegades, perquè tots sabem que el contingut d'Internet és públic i no sempre es cent per cent fiable.

Un altre dels temes als que vaig tenir que fer front, va ser l'idioma, vaig trobar varis exemples en castellà, però aquests o bé eren massa antiquats o contenien greus problemes de seguretat. Pel que vaig optar a consultar pagines en Angles, on la informació al respecte era major i era molt més fàcil de contrastar.

6.1.3. Problema Edició

Durant la fase de creació ens hem trobat amb diversos problemes, hem hagut de comprovar moltes línies de codi per trobar errors que a simple vista no es veien i feien que l'aplicació no funciones de la manera que ho havia de fer.

Un altre problema que m'he trobat a l'hora de la creació de l'aplicació ha sigut no definir bé les funcionalitats. A mida que el projecte anava avançant m'he trobat amb el principal problema d'aconseguir que la imatge xifrada seguís sent una imatge. La idea inicial era encriptar tot el fitxer de la imatge i posteriorment afegir-hi una capçalera d'imatge per davant per a que el nou fitxer seguís sent una imatge, amb la informació encriptada.

El principal problema es que no he trobat forma d'afegir únicament una capçalera d'imatge al fitxer encriptat, ja que quan ho feia e intentava llegir la imatge em donava que estava corrupte. Després de moltes hores es va optar per una altre opció:

1) Prendre la imatge amb la càmera

2) Encriptar únicament els píxels de la imatge per a conservar la capçalera (taronja + vermell)

3) Després encriptar la imatge sencera (capçalera + píxels) (verd)

4) Afegir en el mateix buffer la imatge del punt 2, la imatge del punt 3 i afegir la longitud de la imatge del punt 2

5) Gravar la informació del buffer en la memòria interna del terminal.

D'aquesta forma tenim dues imatges dins d'una (Original amb capçaleres bitmap i píxels encriptats + fitxer sencer encriptat).

Per tal de redefinir bé les funcionalitats de la APP el tutor ha estat de gran ajuda.

6.1.4. Problema Test

Un cop finalitzada la fase de creació, on tot el codi ha estat picat, venia la fase de depuració. Aquesta es la part que més problemes m'ha donat, ja que al ser una sola persona m'ha fet estar hores provant totes les possibles execucions de l'aplicació emulant diversos terminals (tablets, mòbils...).

6.2 Que hem apres

Durant l'elaboració d'aquest projecte hem apres varies coses que a continuació explicarem amb detall.

El projecte va ser començat a l'estiu del 2013, el fet d'intentar donar un canvi de rumb al meu futur professional cap al mon dels terminals mòbils i el fet d'estudiar el MISTIC, va ser la combinació ideal per escollir aquest projecte. Que millor que ajuntar els meus estudis actuals amb la meva feina futura.

On he notat una millora considerable, ha sigut en el domini de l'entorn/llenguatge Java/Android, on he pogut veure el potencial real d'aquest llenguatge i he pogut crear una APP per a encriptar i desencriptar imatges, del resultat de la qual n'estic molt satisfet.

Amb aquest projecte s'han millorat els coneixements i s'ha entès amb un cas pràctic com funciona la criptografia. Durant els transcurs de la APP hem hagut de consultar apunts de tot el MISITIC i hem pogut crear un cas pràctic amb tota la teoria apresa durant el Màster, el que ha servit per assentar les bases del coneixements.

6.3 Possibles futures implementacions

Pel fet de que el projecte sigui entregat no vol dir que l'aplicació s'hagi de quedar tal i com està. Amb el pas del temps es poden implementar noves funcionalitats.

Algunes funcionalitats que s'han pensat i que es podrien implementar són:

6.3.1. Enviar les imatges a altres dispositius

Es podria implementar una funcionalitat que permeti als usuaris poder enviar les imatges encriptades a altres usuaris, i si aquests coneixen la clau puguin accedir a la informació correcte, en cas contrari veurien la imatge encriptada.

6.3.2. Backup en servidor de les imatges encriptades

Un cop una imatge es presa que aquesta es guardi en un servidor extern, per si en algun moment no tenim accés al terminal, podem seguir tenint les imatges emmagatzemades en una altre localització.

4.1.1. Canviar la password d'encriptació

Un cop tenim les imatges emmagatzemades en una carpeta dins el nostre terminal, hauríem de poder canviar la password d'encriptació d'una imatge per una altre de nova.

7. Conclusions

Aquest projecte a part de ser un projecte final de màster també ha sigut un projecte de realització personal, ja que ha unit dues parts de la meva vida; la meva carrera professional i les meves activitats personals. Potser, gracies a això l'elaboració d'aquest projecte se m'ha fet menys feixuga.

S'hi han dedicat moltes hores, moltes més de les esperades, però el resultat ha estat gratificant. S'han pogut assolir tots els objectius marcats i fins i tot s'han pogut implementar funcionalitats que en un principi no estaven pensades.

Una cosa que he apres en l'elaboració d'aquest projecte es que no ha de perquè acabar aquí, amb el temps es poden implementar noves funcionalitats i gracies a conèixer el codi al 100% aixo es pot fer d'una manera molt més rapida i còmode.

Els companys de treball que han vist la APP han quedat sorpresos de les funcionalitats que aquesta implementa i han mostrat interès en utilitzar-la per a protegir les seves imatges personals.

A nivell personal, la satisfacció es màxima. S'ha pogut desenvolupar el projecte en els terminis establerts. Tenia algun dubte de que això no es pogués dur a terme per culpa de tenir dues feines i no disposar de tot el temps del que es voldria.

Una cosa clara sobre el projecte es que aquest no finalitza amb la seva entrega. Tinc pensades futures implementacions que vull dur a terme tant aviat com tingui temps. A mida que una nova implementació es afegida sorgeixen més ganes de seguir millorant.

Finalment, agrair tota la feina al meu tutor per donar-me suport i guiar-me durant la creació del projecte. Ja que sense aquesta ajuda en certs moments et sents perdut i no saps quin camí agafar.

8. Fonts d'informació

En aquest capítol es detallen les fonts consultades per dur a terme tant el projecte com la memòria d'aquest. Per a cada font, es mostra el lloc on ha estat localitzada i quan s'ha consultat.

En l'ultim apartat trobem un petit diccionari on es mostra el significat de cadascuna de les paraules tècniques utilitzades durant la creació del projecte o de la memòria.

8.1 Bibliografia bàsica

Manual Android:
Descripció: Guies Oficials de les API's d'Android.
URL:http://developer.android.com/guide/index.html
Data consulta: durant el transcurs del projecte.

Descripció: Pagina web amb diversos exemples de funcionalitats d'Android.
URL: http://www.sgoliver.net/
Data consulta: durant el transcurs del projecte.

AES:
Descripció: Informació sobre l'algoritme de xifrat
URL: http://en.wikipedia.org/wiki/Aes
URL:http://www.cubrid.org/blog/dev-platform/understanding-encryption-security-through-java-cryptography-architecture/
Data consulta: 15-25 setembre 2013

Exemples d'algoritmes AES:

Descripció: Fòrum informàtic amb exemples d'algoritmes d'encriptació.

URL: http://stackoverflow.com/questions/10782187

URL: http://stackoverflow.com

Data consulta: 20 Novembre 2013

Descripció: Article amb exemples d'algoritmes d'encriptació.

URL: http://www.macs.hw.ac.uk/~ml355/lore/pkencryption.htm

Data consulta: 22 Novembre 2013

Tractament Imatges (Bitmap):

Descripció: Referencies sobre l'objecte BITMAP d'Android

URL:http://developer.android.com/reference/android/graphics/Bitmap.html

Data consulta: 24 Novembre 2013

Class BufferedOutputStream (Java):

Descripció: Referencies sobre la classe d'escriptura d'informació en memòria.

URL:http://docs.oracle.com/javase/7/docs/api/java/io/BufferedOutputStream.html

Data consulta: Desembre 2013

Web de Projectes de la UOC:

Descripció: Campus Virtual de la UOC amb guies sobre com realitzar el TFM.

URL:http://cv.uoc.es/cdocent/HKZB5UG6XS130_6R5O43.pdf

URL:http://cv.uoc.es/cdocent/8QROP4G6IXT6ND3J1_XE.pdf

Data consulta: 20 Desembre 2013

8.2 Definicions, acrònims i abreviacions

Criptografia:

L'estudi de formes de convertir informació des de la seva forma original cap a un codi incomprensible, de forma que sigui incomprensible pels que no coneguin aquesta tècnica.

AES:

L' Advanced Encryption Standard (AES), també conegut com Rijndael (pronunciat "Rain Doll" en anglès), és un esquema de xifrat per blocs adoptat com un estàndard de xifrat pel govern dels Estats Units.

Android:

És un conjunt de programari per a telèfons mòbils que inclou un sistema operatiu, programari intermediari i aplicacions

LOPD:

Llei orgànica de protecció de dades.

Usuari:

Persones físiques amb accés al sistema.

Internet:

Xarxa de xarxes informàtiques, descentralitzada, ampliable indefinidament i d'abast mundial.