Manual d'usuari de la File Encoder Application v1.5

# Índex

[0. Índex 1](#_Toc62345121)

[1. Introducció 2](#_Toc62345122)

[2. Inici ràpid 5](#_Toc62345123)

[2.1. Requeriments 5](#_Toc62345124)

[2.2. Inici ràpid 5](#_Toc62345125)

[3. Interfície d’usuari 5](#_Toc62345126)

[3.1. Pantalla principal 6](#_Toc62345127)

[3.2. Menú Arxiu 9](#_Toc62345128)

[3.3. Menú Eines 10](#_Toc62345129)

[3.4. Menú Vista 10](#_Toc62345130)

[3.5. Menú d’Ajuda 10](#_Toc62345131)

[3.6. Llista de configuracions de encriptació 11](#_Toc62345132)

[3.6.1. Conceptes bàsics 11](#_Toc62345133)

[3.6.2. El formulari 11](#_Toc62345134)

[3.7. Configuració d'encriptació 13](#_Toc62345135)

[3.7.1. Paràmetres de la configuració de encriptació 14](#_Toc62345136)

[3.8. Configuració de la aplicació 19](#_Toc62345137)

[3.8.1. Paràmetres de la configuració d’encriptació de l’aplicació 19](#_Toc62345138)

[3.8.2. Paràmetres de la configuració d’idiomes de l’aplicació 20](#_Toc62345139)

[3.8.3. Paràmetres de la configuració de vista de l’aplicació 22](#_Toc62345140)

[3.9. Esborrament d’arxius 22](#_Toc62345141)

[3.10. Sobre l’aplicació 24](#_Toc62345142)

[3.11. Llicència 24](#_Toc62345143)

[4. Encriptació per la interfície d'ordres 25](#_Toc62345144)

[4.1. Scripts per a Windows 26](#_Toc62345145)

[4.2. Scripts per a Linux y per Mac 26](#_Toc62345146)

[4.3. Paràmetres d'encriptació com a arguments 27](#_Toc62345147)

[5. Mètode d'encriptació 29](#_Toc62345148)

[5.1. Capçalera de l'arxiu encriptat 29](#_Toc62345149)

[5.2. Algoritme d'encriptació 30](#_Toc62345150)

[5.3. Generador pseudoaleatori utilitzat 31](#_Toc62345151)

[5.4. Utilització de fils d’execució (paral.lelisme) 34](#_Toc62345152)

[6. Tipus d’encriptació 36](#_Toc62345153)

[6.1. FileEncoderType-1 36](#_Toc62345154)

[6.2. FileEncoderType-2 37](#_Toc62345155)

[6.3. FileEncoderType-3 37](#_Toc62345156)

[6.4. FileEncoderType-4 38](#_Toc62345157)

[6.5. FileEncoderType-5 39](#_Toc62345158)

[6.6. FileEncoderType-6 39](#_Toc62345159)

[6.7. FileEncoderType-7 40](#_Toc62345160)

[6.8. FileEncoderType-8 41](#_Toc62345161)

# Introducció

La File Encoder Application es una aplicació que permet encriptar arxius.

Básicamente permet:

* Encriptar arxiu.
* Desencriptar arxiu (encriptat prèviament amb aquesta mateixa aplicació).
* Obrir un arxiu encriptat (desencriptant-lo prèviament)

L'aplicació permet operar amb arxius encriptats (amb extensió .jfe) i desencriptats amb la seva interfície gràfica.

Així mateix el motor de l'aplicació pot ser invocat a través de la interfície d'ordres obtenint d'aquesta manera la mateixa funcionalitat quant a encriptació/desencriptació que l'aplicació gràfica.

L'aplicació està escrita en Java i per aquest motiu es portable a diferents plataformes i hauria de ser compatible. És a dir, hauria de ser possible encriptar un arxiu en una plataforma i desencriptar-lo en una altra diferent.

L'aplicació ha sigut provada únicament amb processadors Intel, en Windows 8, Linux i OS-X però també hauria de ser compatible amb qualsevol plataforma que tingui instal.lada la màquina virtual de Java (JRE).

Existeixen diferents paràmetres de configuració de l'encriptació que modificats convenientment poden permetre:

* incrementar la velocitat dels processos d'encriptació/desencriptació.
* incrementar la robustesa dels processos d'encriptació/desencriptació.
* minimitzar l'utilització de la memòria.

Desgraciadament no poden optimitzar-se tots el punts a l'hora. Així doncs, si es requereix d'incrementar la robustesa de l'encriptació a través dels valors dels paràmetres de l'encriptació, això va en contra d'incrementar la velocitat o en contra de minimitzar l'utilització de la memòria.

Si no tens ganes d'aprendre el paràmetres, pots deixar la configuració bàsica que inclou diferents configuracions dels paràmetres basades en el tamany de l'arxiu per permetre que els arxius més grans siguin encriptats amb una configuració més ràpida que els petits.

Independentment dels paràmetres utilitzats per encriptar, una bona contrasenya ajuda a la robustesa de l'encriptació.

Per això s'aconsella d'utilitzar una contrasenya molt llarga (pot ser una frase), per a que un intent de trencar l'encriptació per força bruta sigui més complicat.

Per exemple, una bona contrasenya deuria contenir lletres maiúscules, lletres minúscules números i no estar composta únicament per paraules de diccionari. Si a això afegim que la contrasenya pot tenir una longitud llarga, per exemple entre 30 i 40 caràcters, el sistema d'encriptació es fa més fort.

**Novetats en la versió 1.2**Aquesta nova versió de l’aplicació ha sorgit degut a un error trobat en el fileEncoderType 2, que ha aparegut en fer proves d’encriptació amb arxius grans.

S’ha creat el fileEncodertype 4 per a substituir el fileEncoderType 2, que corregeix l’error trobat i a més augmenta el rang del números fins a 256.

A més s’han creat dos fileEncoderTypes adaptats a arxius grans i molt grans.

Els fileEncoderTypes 5 i 6 son molt més robustos que els seus predecessors per a arxius grans.

El fileEncoderType 6 inclou una simplificació que el fa una mica menys robust que el 5 per a arxius grans, però que, a canvi, augmenta la seva velocitat d’encriptació en un factor de vàries unitats.

Aquest nou tipus (6) no es aconsellable per a encriptar arxius petits o mitjans (menors de 10 MB).

S’han realitzat proves d’encriptació amb arxius grans (més grans de 50 GB) amb èxit.

**Novetats a la versió 1.3**

En aquesta nova versió de l’aplicació, s’han creat dos nous tipus d’encriptació que permeten utilitzar mútiples fils d’execució (paral.lelisme), ideal para a ser utilitzat amb arxius grans.

* fileEncoderType 7.

Aquest tipus d’encriptació té dues maneres de funcionar:

* + Arxiu d’entrada i arxiu de sortida al mateix disc:
		- Hi ha un fil separat per a l’accés a disc (el mateix fil per a llegir i per a escriure).
		- Hi ha un o més fils per a l’encriptació.
	+ Arxiu d’entrada i arxiu de sortida a discos separats:
		- Hi ha un fil separat per a la lectura de l’arxiu de entrada.
		- Hi ha un altre fil separat per a l’escritura de l’arxiu de sortida.
		- Hi ha un o més fils per a l’encriptació.

Depenent de la capacitat de procés de la màquina i de la velocitat dels discos d’entrada i de sortida la millora en la velocitat d’encriptació variarà entre equips.

A les proves que s’han fet (amb el número de fils òptim i essent l’únic consumidor de tots els recursos de la màqnuia), s’ha arribat a dividir el temps total d’encriptación en un factor 2 per a arxius molt grans.

Si a més, fem que els arxius d’entrada i de sortida estiguin a diferents discos, la millora en la velocitat es fa més evident, arribant a factors de millora superiors a 3.

Per a més detalls pots anar als apartats que expliquen el nou tipus d’encriptació.

Tots els FileEncoderType a partir del: ***6.7-FileEncoderType-7***

* + Comparativa de temps d’encriptació/desencriptació d’arxius grans amb el nou tipus d’encriptació (pot variar en diferents sistemes):

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Mida | FileEncoderType | -numOfThreads | Discos diferents | Duració de la encriptació (s) | Duració de la desencriptació (s) |
| 27,2 GB | 6 | (1) | no | 1631 | 1512 |
| 27,2 GB | 7 (nou) | 3 | no | 704 | 886 |
| 27,2 GB | 7 (nou) | 6 | sí | 455 | 669 |

* fileEncoderType 8.

Aquest tipus d’encriptació és equivalent al 7, però permetent dividir l’arxiu encriptat en volums d’una mida concreta.

Per a més informació revisar el punt: ***6.8-FileEncoderType-8***

**Novetats a la versió 1.4**

S’ha corregit un efecte negatiu que es produïa a màquines amb alt dpi (alta densitat en píxels per centímetre) a partir de Java-9.

A partir de Java-9 java introdueix un tractament automàtic tenint en compte la densitat de píxels per centímetre de la pantalla del dispositiu.

Aquest tractament automàtic interferia de manera negativa amb la funcionalitat d’ampliació incorporada a les meves aplicacions.

Per evitar aquest efecte no desitjat, s’ha desactivat la nova funcionalitat de Java-9.

**Novetats a la versió 1.5**

Es fa ús de la versió de plataforma v1.4, que afegeix la consulta de nova versió durant l’inici de l’aplicació.

# Inici ràpid

## Requeriments

Per a iniciar l’aplicació és necessari tenir l’entorn de Java instal.lat (Java Runtime Environment), a la versió 8 o superior.

D’aquesta manera es podrà obrir l’arxiu .jar que hi ha a la carpeta ./binary/

## Inici ràpid

Abans de començar, indicar que l'aplicació utilitza el micròfon per recollir octets aleatoris. És per això que seria necessari tenir un micròfon connectat per a que l'aplicació funcioni de manera òptima.

En aquesta versió s’ha millorat aquesta part i ara si el micròfon està desconnectat, es generen números aleatoris fent servir els generadors de llavors que té el propi Java.

Per començar a utilitzar l'aplicació, segueix el següents passos:

1. Obre la File Encoder Application, fent doble click en: l'arxiu .jar de l'aplicació que es troba a: .../\_binary/jfe.v1.3.jar
2. Canviar l'idioma de l'aplicació (Menú: Eines->Idioma->CAT)
3. Obre una nova finestra d'arxiu (Menú: Arxiu->Nou).
4. Arxiu. Introdueix l'arxiu que vols encriptar (qualsevol nom) o desencriptar (arxiu amb extensió .jfe). Pots polsar el botó "..." per obrir el diàleg de selecció d'arxiu.

Tingues en compte que per encriptar o desencriptar un arxiu, no ha d'existir l'arxiu encriptar o desencriptar. Si existeix aquest arxiu, l'operació fallarà, ja que l'aplicació no sobreescriurà l'arxiu.

1. Contrasenya. Introdueix la contrasenya que tindrà l'arxiu encriptat o que té l'arxiu a desencriptar.
2. Repetir contrasenya. Torna a introduir la contrasenya. Ambdós contrasenyes han de coincidir per poder encriptar/desencriptar.

Després d'aquests passos, ja pots utilitzar els botons d'encriptar, desencriptar o obrir arxiu encriptat.

# Interfície d’usuari

En aquest capítol es veurà como encriptar, desencriptar i obrir arxius encriptats i esborrar arxius existents i també es veuran les opcions més comuns a l'hora d'executar aquestes accions.

## Pantalla principal

En obrir l'aplicació gràfica, apareix una pantalla com la següent:



En ella és pot veure que hi ha un menú principal i un àrea gran on seran les finestres MDI de l'aplicació.

Al menú Arxiu apareix una opció (Nou).

Seleccionant aquesta opció apareixerà una nova finestra d'arxiu.

Es pot obrir tantes finestres d'arxiu com sigui necessari.

L'aspecte de la finestra d'arxiu es aquest:



En aquesta finestra hi ha uns quants paràmetres que s'han d'omplir abans d'accedir a la funcionalitat.

* "Arxiu desencriptat". En aquest quadre de text s'ha de posar el nom de l'arxiu desencriptat.
* "Arxiu encriptat". En aquest quadre de text s'ha de posar el nom de l'arxiu encriptat (amb extensió .jfe).

Per omplir-los es pot fer de dues formes:

* + Clickant el botó de la seva dreta "...". Quan el polsi sobre aquest botó, s'obrirà un diàleg que permetrà navegar pels arxius de l'equip i seleccionar l'arxiu.
	+ Editant-lo amb el teclat (això pot ser útil quan ja tens al quadre de text el nom d'un arxiu i vols editar el nom de l’arxiu).
* "Contrasenya" i "Repetir contrasenya". En aquests dos quadres de text, has d'escriure la contrasenya que s'ha d'aplicar en encriptar o en desencriptar un arxiu.

Els dos quadres de text han de contenir la mateixa contrasenya. Això és així per a que, en cas d'haver escrit malament la contrasenya (sobre tot en encriptat), puguis adonar-te'n. D'una altra manera l'arxiu s'encriptaria amb una contrasenya desconeguda i després no es podria desencriptar l'arxiu.

Òbviament la contrasenya utilitzada per encriptar i la utilitzada per desencriptar ha de ser la mateixa per a que es realitzi el procés de desencriptació correctament.

* El checkbox de “Entrada y sortida són a discos diferents”, indica si es farà servir el paràmetre d’encriptació “-encDecOnDifferentDrives” que diu que l’arxiu d’entrada i el de sortida es troben a discos diferents, i això fa que pels fileEncoderType 7 y 8, es facin servir fils separats per a l’entrada i per a la sortida de disc.
* El checkbox “auto”, indica si el valor del checkbox anterior es calcula automàticament (l’aplicació considera que els arxius es troben a discos diferents si estan a particions diferents, criteri que no sempre és vàlid).

Un cop omplerts els paràmetres anteriors, ja es pot utilitzar la funcionalitat.

Amb la nova finestra d'arxiu es pot accedir a les funcionalitats prement els següents botons:

* "Encriptar". Encripta l'arxiu.
* "Desencriptar". Desencripta l'arxiu.
* "Obrir arxiu encriptat". Desencripta i obre l'arxiu amb l'aplicació predeterminada al sistema per aquest tipus d'arxius.
* Modificar la "Configuració d'encriptació". Serveix per modificar els paràmetres d'encriptació. Veure punt: ***3.7-Configuració d'encriptació***
* "Esborrar arxiu". Al costat dels components de text que contenen els noms d’arxiu encriptats i desencriptats, hi ha uns botons amb una creo que permeten esborrar l’arxiu associat. Veure punt: *3.9-Esborrament d’arxius*
* "Netejar història". Esborra la història del quadre de text Història.
* "Cancel.lar". Cancel.la l'encriptació, desencriptació o esborrat d’arxiu.

Hi ha un quadre de text (Història), en el que s'escriu l'estat i el resultat de les accions que anem fent sobre els arxius.

També existeix una barra de progrés que indica el progrés de l'acció en curs i quan finalitza l'encriptació/desencriptació d'un arxiu, existeix una etiqueta a la dreta de la barra de progrés que indica el temps transcorregut en segons des de l'inici de l'acció.

## Menú Arxiu

El menú Arxiu té aquest aspecte:



En aquest menú apareixen dues opcions:

* **Nou**. En prémer sobre aquest element del menú crearem una nova finestra d'arxiu, que hem vist al punt anterior.
* **Sortir**. Permet sortir de l'aplicació.

## Menú Eines

El menú eines té el següent aspecte:



Aquest menú té tres opcions:

* **Idioma**. En obrir aquest submenú apareixen els idiomes disponibles. Serveix per a poder canviar l'idioma de l'aplicació.

Per defecte hi ha disponibles els següents idiomes:

* "EN". Anglès
* "ES". Castellà
* "CAT". Català
* **Configuracions d'encriptació**. Quan es prem aquest element del menú, apareix un formulari en el que es permet modificar les configuracions d'encriptació utilitzades segons les mides d'arxiu a encriptar. Veure punt: ***3.6-Llista de configuracions de encriptació***
* **Configuració de l'aplicació**. Quan es prem aquest element del menú, apareix un formulari en el que es permet modificar els paràmetres de configuració generals de l'aplicació. Veure punt: ***3.8-Configuració de la aplicació***

## Menú Vista

El menú Vista té aquest aspecte:

 

Aquest menú només té una opció:

* **Zoom**. Permet escollir la mida de les finestres de l’aplicació, indicant un percentatge d’ampliació, on l’aspecte normal es el (100%).

## Menú d’Ajuda

El menú d’Ajuda té el següent aspecte:



Aquest menú només té dues opcions:

* **Ajuda**. Obre aquest arxiu d’ajuda.
* **Buscar nova versió**. Aquesta opció fa una consulta al servidor per a veure si hi ha disponible una nova versió de l’aplicació.
* **Què és nou**. Aquesta versió mostra el document que explica el que és nou a aquesta versió.
* Llicència. Mostra la llicència que es va acceptar el primer cop que es va fer servir l’aplicació. Veure apartat: ***3.11-Llicència***
* Sobre l'aplicació. Quan es prem aquest element de menú, apareix un formulari amb les dades de l'aplicació, els agraïments i les dades de contacte. Veure apartat:

***3.10-Sobre l’aplicació***

## Llista de configuracions de encriptació

Aquest formulari permet crear, modificar i esborrar configuracions d'encriptació o revertir la llista de configuracions d'encriptació per defecte.

### Conceptes bàsics

Com s'ha comentat a la introducció, existeixen alguns paràmetres per a l'encriptació que incideixen sobre la velocitat, l'ús de la memòria i la robustesa de l'encriptació. Veure punt: ***3.7.1-Paràmetres de la configuració de encriptació***

Donat que els paràmetres d'encriptació incideixen sobre tot en la velocitat de l'encriptació/desencriptació, sembla lògic pensar que en funció del tamany de l'arxiu hauria d'utilitzar-se una configuració d'encriptació o una altra.

Per facilitar les coses a l'usuari final, la File Encoder Application permet de tenir configuracions d'encriptació predefinides per les diferents possibilitats de tamany d'arxiu, existint l'opció d'escollir automàticament una configuració d'encriptació en funció del tamany de l'arxiu a encriptar.

Aquest formulari permet mantenir aquestes configuracions d'encriptació definides para a cada interval del mida d'arxiu.

### El formulari

El formulari té el següent aspecte:



En aquest formulari existeix una taula resum de les configuracions d'encriptació ordenades per mida d'arxiu en ordre creixent. En aquesta taula només es pot seleccionar una fila a l'hora.

Cada fila es correspon a mb una configuración d'encriptació, associada a un interval de mides d'arxiu.

La configuració d'encriptació aplicaria a l'interval de tamanys d'arxiu desde el camp SIZE\_FROM de la pròpia configuració d'encriptació (en octets), fins el camp SIZE\_FROM de la següent configuració d'encriptació (la següent fila), o bé ilimitat si no existeix cap fila posterior.

També existeixen una sèrie de botons que aporten la funcionalitat del formulari:

* Botó revertir. Elimina tots els canvis que s'hagin pogut fer sobre les configuracions d'encriptació per interval de mides d'arxiu, deixant la llista de configuracions d'encriptació original (la que venia inicialment en l'aplicació).
* Botó acceptar (aplicar). Permet sortir del formulari guardant els canvis realitzats en les configuracions d'encriptació.
* Botó cancel.lar. Permet sortir del formulari sense guardar ni aplicar els canvis realitzats en les configuracions d'encriptació per interval de mides d'arxiu.

A més, quan es prem el botó dret del ratolí dintre de la taula de configuracions, apareix aquest menú emergent que permet realitzar operacions sobre els elements d’aquesta taula:



* Modificar configuració seleccionada. Obre el formulari que permet de modificar els paràmetres d'encriptació de la configuració d'encriptació seleccionada de la taula. Veure punt: ***3.7-Configuració d'encriptació***
* Modificar nova configuració. Obre el formulari que permet de crear una configuració d'encriptació des de zero, havent d'introduir el paràmetre SIZE\_FROM que permetrà definir l'interval de mides d'arxiu als quals aplica aquesta configuració.
* Esborrar configuració. Esborra la configuració d'encriptació seleccionada de la taula.

## Configuració d'encriptació

Aquest formulari permet de modificar els paràmetres d'encriptació per a una configuració d'encriptació determinada, ja sigui per aplicar-la directament sobre un arxiu a encriptar (des de una finestra d'arxiu) o bé per a modificar els paràmetres de configuració d'encriptació d'un interval de mides d'arxiu determinat.

El formulari té el següent aspecte:



 A aquest formulari pot arribar-se bé des de la finestra d'arxiu, vista al punt: ***3.1-Pantalla principal***  bé des de el formulari de Llista de configuracions d'encriptació al punt: ***3.6.2-El formulari***.

Existeix un botó per a carregar els paràmetres per defecte en funció de la mida de l'arxiu. Aquest botó només estarà habilitat en cas de que l'accés al formulari hagi sigut a través de la finestra d'arxiu. En cas d'haver accedit a aquest formulari a través del formulari de Llista de configuracions d'encriptació, aquest botó estarà deshabilitat.

Aquest botó només ofereix funcionalitat en cas de que estigui habilitat i a més ha d'existir l'arxiu configurat a la finestra d'arxiu. En un altre cas en prémer-lo l'aplicació no farà res.

### Paràmetres de la configuració de encriptació

Es poden configurar el següents paràmetres:

* Mida d'arxiu (des de). Aquest valor no és un paràmetre de configuració pròpiament dit i només està habilitat en cas de que l'accés al formulari hagi sigut a través del formulari de Llista de configuracions d'encriptació.

Això és així perquè en aquest cas es pretén de crear o editar una configuració d'encriptació que aplicarà a un interval de mides d'arxiu. La mida d'arxiu (des de) indicarà l'inici de l'interval de mides d'arxiu en octets. El final de l'interval al que aplicarà la configuració d'aquest formulari, dependrà del paràmetre de mida d'arxiu (des de) de la següent configuració d'encriptació a la Llista de configuracions d'encriptació.

En cas de que s'hagi accedit a aquest formulari des de la finestra d'arxiu, la configuració d'encriptació que s'està editant, en cas de ser acceptada, podrà ser aplicada directament als paràmetres de la propera encriptació, depenent de la configuració de prioritats de configuració d'encriptació explicada al punt: ***3.8-Configuració de la aplicació***

* FileEncoderType. Aquest paràmetre indica què classe de FileEncoder serà utilitzat per encriptar. És un valor numèric que, per la v1.0, pot prendre els valors 1 o 2.
* 1 (NO RECOMANAT). Classe de FileEncoder que utilitza un generador pseudoaleatori caòtic basat en la classe BigDecimal de Java per fer els càlculs.

Com per fer les operacions d'encdirptació s'utilitza aquesta classe a baix nivell, és possible que algun canvi intern d'implementació en aquesta classe en alguna actualització de Java, pogués trencar la compatibilitat cap enrere.

És per això que es va decidir de programar una classe numèrica pròpia menys dependent de Java.

* 2 (OBSOLET). Aquest fileEncoderType conté un error que fa que no sigui aconsellable el seu ús.

Indica que s'utilitzi la classe FileEncoder que utilitza un generador pseudoaleatori caòtic basat en una classe numèrica pròpia per fer els càlculs.

Aquesta classe treballa amb números de precisió variable i no és genèrica. Està molt enfocada a l'interval numèric en que treballa el generador pseudoaleatori caòtic.

Conté la informació del número en un array de long dels que per raons d'optimització només s'utilitzen els 31 bits inferiors de cada element de l'array.

Quan es parli de "blocs" en els següents paràmetres d'encriptació aplicables a aquest FileEncoderType, ens referirem a un element de l'array de long, és a dir, un long (31 bits).

L’encriptador d’aquest tipus, utilitza una combinació d’encriptació XOR combinada amb una reordenació d’octets de cada un del blocs en que es divideix l’arxiu a encriptar.

* 3 (OBSOLET). FileEncoderType idèntic a l’anterior, però amb la particularitat de que la mida dels números augmenta el seu rang. Amb aquest fileEncoderType espot treballar amb mides de número fins a 256.

De la mateixa manera que el fileEncoderType 2, té un error que fa que no sigui aconsellable el seu ús.

* 4. Aquest fileEncoderType és idèntic a l’anterior, amb la diferència de que l’error ha sigut corregit.
* 5. Aquest fileEncoderType és idèntic a l’anterior, però, a més de l’encriptació XOR combinada amb la reordenació d’octets (com tots els anterior), afegeix la particularitat de que els blocs en que es divideix l’arxiu a encriptar, són reordenades. Això el fa molt més fort davant d’intents de trencar l’encriptació per força bruta.

Aquest tipus d’encriptació és particularment fort per a arxius mitjanament grans.

* 6. (NO RECOMANAT) Aquest fileEncoderType és idèntic a l’anterior, però per a accelerar la velocitat d’encriptació/desencriptació, s’ha eliminat la reordenació d’octets en cada un dels blocs. És molt més ràpid que el fileEncoderType 5, i, per a arxius molt grans, hauria de ser bastant difícil de trencar (molt més que el fileEncoderType 4).

No és aconsellable utilitzar-lo amb arxius petits o de mida mitjana (menors de 10 MB).

S’aconsella utilitzar el fileEncoderType 7 en lloc d’aquest, ja que pot ser notablement més ràpid.

* 7. Aquest fileEncoderType és molt paregut a l’anterior, però afegint la possibilitat de fer servir múltiples fils d’execució.

Està especialment aconsellat per a arxius molt grans (més de 100 MB), on es pot apreciar clarament com baixa el temps d’execució en fer servir processament en paral.lel.

* 8. Aquest fileEncoderType és idèntic a l’anterior, però afegint la possibilitat d’escriure l’arxiu encriptat en volums que tenen configurable la seva mida.
* NumBytesFileSlice. Aquest paràmetre de configuració d'encriptació indica el número d'octets de bloc que seran utilitzats per encriptar.

Per arxius grans no és viable carregar tot el contingut de l'arxiu a la memòria i fer els càlculs per a l'encriptació, ja que per a fer aquests càlculs, s'utilitza una memòria entre 100 i 200 cops més gran que la de la mida en octets que s'està encriptant. Per un arxiu de 50 MiB tindríem que la fita superior de la memòria utilitzada serien 10 GiB, quantitat de memòria que no està disponible en moltes de les màquines actuals.

Aquest paràmetre fa que el contingut de l'arxiu es divideixi en blocs i per cadascun d'aquests blocs, primer es llegeixi el contingut del bloc en un array d'octets, s'apliqui l'encriptació i s'escrigui a l'arxiu encriptat el contingut de la bloc encriptada. Per encriptar el següent bloc ja no serà necessari tenir a la memòria les rodanxes anteriors. És per això que no seria necessària tanta memòria com si s'encriptés a l'hora tot l'arxiu complet.

Llavors baixar aquest paràmetre fa que baixi el consum de memòria de l'aplicació.

No obstant no seria bo baixar molt aquest paràmetre, ja que l'encriptació complerta de l'arxiu es pot trencar per força bruta si es trenca l'encriptació de la primera bloc. Per a posar les coses més difícils a qui vulgui trencar aquesta encriptació, aquest paràmetre hauria de configurar-se el més alt possible en funció de la memòria disponible a la màquina on treballem.

Haurem de tenir en compte, però, que si posem aquest paràmetre molt alt, l'arxiu podria no poder ser desencriptat en una màquina amb menys memòria.

Si assignem el valor 0 a aquest paràmetre, això fa que l’arxiu encriptar no es divideixi en blocs (utilitzant un únic bloc que inclou tots els octets de l’arxiu).

* SizeOfNumbersSimpleEncoder. Aquest paràmetre de configuració d'encriptació aplica a la mida dels números aplicat al generador pseudoaleatori caòtic

Veure punt: ***5.2-Algoritme d'encriptació***

El paràmetre SizeOfNumbersSimpleEncoder fa referència a la mida dels números al generador pseudoaleatori utilitzat pel primer pas de l'encriptació (XOR).

Les unitats d'aquest paràmetre són lleugerament diferents pels FileEncoderType 1 i la resta.

* Pel FileEncoderType 1, aquest paràmetre està expressat en octets.
* Pel FileEncoderType 2, 3, 4, 5, 6, 7 i 8 aquest paràmetre està expressat en blocs de 31 bits.

En aquest cas seria igual al número d'elements long que hi ha a l'array que té les dades del número (en cada element long de l'array s'emmagatzemen 31 bits).

* SizeOfNumbersReordererEncoder. Aquest paràmetre d'encriptació aplica al tamany numèric aplicat al generador pseudoaleatori caòtic del segon pas de l'encriptació (reordenació).

Les unitats d'aquest paràmetre és lleugerament diferent pels FileEncoderType 1 i la resta.

* Pel FileEncoderType 1, aquest paràmetre està expressat en octets.
* Pel FileEncoderType 2, 3, 4 i 5 aquest paràmetre està expressat en blocs de 31 bits.

En aquest cas seria igual al número d'elements long que hi ha a l'array que té les dades del número (en cada element long de l'array s'emmagatzemen 31 bits).

* Els fileEncoderType 6, 7 i 8 no utilitzen aquest paràmetre.
* NumBitsPerIterationSimpleEncoder. Aquest paràmetre de configuració d'encriptació aplica al número de bits que torna el generador pseudoaleatori en cada iteració. Aquest paràmetre aplica al generador pseudoaleatori utilitzat al primer pas (XOR).

Aquest paràmetre influeix dràsticament en el temps de computació de l'encriptació.

Per a arxius petits a encriptar, és aconsellable utilitzar un valor d'aquest paràmetre molt petit, per a que la robustesa de l'encriptació sigui més gran.

Per a arxius grans o molt grans, serà millor utilitzar valors grans per a aquest paràmetre, ja que en cas contrari el temps per encriptar/desencriptar seria molt gran i es faria molt pesat haver d'esperar cada cop que es necessiti encriptar/desencriptar l'arxiu.

El valors acceptats pel FileEncoderType 1 i la resta son lleugerament diferents:

* Pel FileEncoderType 1, aquest paràmetre pot acceptar els valors 1, 2 o 4. El valor 4 és el que produeix encriptacions més ràpides, no obtant no s'aconsella utilitzar amb valors de SizeOfNumbersSimpleEncoder menors a 16 octets, ja que en aquest cas, s'obtindrien números entre 0 i 15 en cada iteració que no serien equiprobables. A partir de mides de número de 16 octets sí que podria utilitzar-se el valor 4, però millor a partir de mides de número de 32 octets.
* Pel FileEncoderType 2, 3, 4, 5, 6, 7 i 8 aquest paràmetre pot acceptar els valors 1, 2, 4 o múltiples de 8 fins a 64 (64 és el valor màxim). No tots el valors estan permesos.

Pel valor 4 es aconsellable no utilitzar mides de número (configurats a SizeOfNumbersSimpleEncoder) més petits de 5 blocs. Millor encara a partir de 8 blocs.

Per a valors més grans que 4 (múltiples de 8 fins a 64), el valor configurat ha de complir aquesta condició:

NumBitsPerIterationSimpleEncoder <= 3 x SizeOfNumbersSimpleEncoder

* NumBitsPerIterationReordererEncoder. Aquest paràmetre de configuració d'encriptació aplica al número de bits que torna el generador pseudoaleatori en cada iteració. Aquest paràmetre aplica al generador pseudoaleatori utilitzat al segon pas (reordenació).

Aquest paràmetre influeix dràsticament en el temps de computació de l'encriptació.

Per a arxius petits a encirptar, és aconsellable utilitzar un valor d'aquest paràmetre molt petit, per a que la robustesa de l'encriptació sigui més gran.

Per a arxius grans o molt grans, serà millor utilitzar valors grans per a aquest paràmetre, ja que en cas contrari el temps per encriptar/desencriptar seria molt gran i es faria molt pesat haver d'esperar cada cop que es necessiti encriptar/desencriptar l'arxiu.

El valors acceptats pel FileEncoderType 1 i la resta son lleugerament diferents:

* Pel FileEncoderType 1, aquest paràmetre pot acceptar els valors 1, 2 o 4. El valor 4 és el que produeix encriptacions més ràpides, no obstant no s'aconsella utilitzar amb valors de SizeOfNumbersReordererEncoder menors a 16 octets, ja que en aquest cas, s'obtindrien números entre 0 i 15 en cada iteració que no serien equiprobables. A partir de mides de número de 16 octets sí que podria utilitzar-se el valor 4, però millor a partir de mides de número de 32 octets.
* Pel FileEncoderType 2, 3, 4 i 5 aquest paràmetre pot acceptar els valors 1, 2, 4 o múltiples de 8 fins a 64 (64 és el valor màxim). No tots el valors estan permesos.

Pel valor 4 es aconsellable no utilitzar mides de número (configurats a SizeOfNumbersReordererEncoder) més petits de 5 blocs. Millor encara a partir de 8 blocs.

Per a valors més grans que 4 (múltiples de 8 fins a 64), el valor configurat ha de complir aquesta condició:

NumBitsPerIterationReordererEncoder <= 3 x SizeOfNumbersReordererEncoder

* Els fileEncoderType 6, 7 i 8 no utilitzen aquest paràmetre.

* NumOfThreads. Indica el número de fils d’encriptació que s’intentaran fer servir en el cas de que l’arxiu encriptat i el desencriptat estiguin al mateix disc (pels FileEncoderType 7 i 8).

Es pot configurar amb el valor “optimum”, que indica que prèviament a l’encriptació s’estimarà automàticament el valor óptim.

Aquesta característica és experimental i el millor seria indicar directament el valor numèric òptim pel teu sistema.

El número total de fils a fer servir en aquest cas, seria el valor d’aquest paràmetre més un fil addicional que es farà servir per a la lectura i escritura al disc.

* NumOfThreadsForDifferentDrives. Indica el número de fils d’encriptació que s’intentaran fer servir en cas de que l’arxiu encriptat i el desencriptat es trobin a discos diferents (pels fileEncoderType 7 i 8).

Es pot configurar amb el valor “optimum”, que indica que prèviament a l’encriptació s’estimarà automàticament el valor óptim.

Aquesta característica és experimental i el millor seria indicar directament el valor numèric òptim pel teu sistema.

El número total de fils a utilitzar en aquest cas, és el valor d’aquest paràmetre més dos (un fil addicional que es farà servir per a la lectura de l’arxiu d’entrada i un altre fil per a l’escriptura de l’arxiu de sortida).

* MaxTotalNumOfThreads. Indica el límit màxim dels fils total a fer servir en una encriptación (pels FileEncoderTypes 7 i 8). Si el número total de fils és més gran que el valor d’aquest paràmetre, llavors es limitarà el número de fils d’encriptació al valor adequat per a que no es superi aquest valor.

Es pot fer servir el valor “max”, que indicarà que com a número màxim de fils, es pren el número màxim de fils de processament que soporta el processador sobre el que s’executa l’aplicació (relacionat amb el número de cores que té el processador).

* SizeInBytesForVolumes. Indica el número d’octetsIndica el número máximo de bytes que podrà tenir cada volum de l’arxiu encriptat (pel fileEncoderType 8).

## Configuració de la aplicació

Aquest formulari permet de modificar els paràmetres de configuració generals de l'aplicació.

El formulari té algunes pestanyes que veurem a continuació:

### Paràmetres de la configuració d’encriptació de l’aplicació

La pestanya té aquest aspecte:



Els paràmetres que poden configurar-se son el s següents:

* **Esborrar l'arxiu encriptat després d'encriptar**. Aquest check box permet configurar si, després d'haver encriptat un arxiu, vols esborrar automàticament l'arxiu sense encriptar.

L'esborrat que es fa no es un esborrat normal, sinó que s'esborra escrivint zeros a cada un dels octets de l'arxiu, i després d'això, es fa un esborrat normal.

D'aquesta manera, es impossible recuperar l'arxiu sense encriptar, a menys que desencriptis l'arxiu encriptat de la manera habitual, utilitzant la contrasenya.

* **Canviar el nom de l'arxiu encriptat a .old després d'encriptar**. Aquest check box permet configurar si després d'una encriptació vols guardar l’últim l'arxiu encriptat que ha sigut desencriptat com a .old. D'aquesta manera t'assegures de tenir emmagatzemada una versión encriptada de l'arxiu, per si de cas passa alguna cosa inesperada.
* **Preguntar abans de sobreescriure l'arxiu encriptat .old**. En cas de que l'opció anterior estigui activa, aquesta opció permet configurar si vols ser preguntat per confirmar la sobreescritura d'un arxiu encriptat .old amb el nou arxiu encriptat pendent de ser emmagatzemat com a .old.
* **Prioritat de configuració d'encriptació**. En aquesta taula es pot configurar l'ordre de prioritat de la configuració d'encriptació.

per defecte les opcions tenen aquesta prioritat:

* (1) - Manual. Es refereix a quan apliques una configuració d'encriptació manualment.

És lògic posar-la com a primera opció, ja que si no es posés como a primera opció, seria possible que es fes una modificació a una configuració d'encriptació i que s'acceptés, però que aquesta configuració no fos aplicada quan es fa l'encriptació.

* (2) - Basat en la mida de l'arxiu. Aquesta opció es refereix a que la configuració de l'encriptació s'obté de la llista de configuracions d'encriptació que estan configurades depenent de la mida de l'arxiu. Veure punt: 3.6-Llista de configuracions de encriptació
* (3) - Basats en els paràmetres de l'arxiu encriptat després de desencriptar. Es refereix a recollir la configuració d'encriptació basada en la configuració d'encriptació existent a l'arxiu encriptat que acaba de ser desencriptat.

La manera de configurar aquest ordre de prioritats, és seleccionar a la taula la fila on és l'opció a la que vols canviar-li la prioritat i prémer els botons "A dalt" i "A baix" per incrementar o decrementar la prioritat.

* **Preguntar sempre abans de canviar fileEncoderTypes obsolets**.

En aquesta versió de l’aplicació, s’han trobat uns fileEncoderTypes que són obsolets, degut a un error trobat en ells.

Aquest check box permet configurar si quan es trobi un d’aquests fileEncoderTypes a l’hora d’encriptar un arxiu, es preguntarà a l’usuari què fer.

En cas de que el check box estigui desmarcat, s’habilitarà el següent check box.

* **Canviar sempre fileEncoderTypes obsolets**.

En cas de que el check box anterior estigui marcat, aquest check box no podrà configurar-se, ja que es preguntarà sempre a l’usuario què fer mitjançant una finestra.

En cas de que el check box anterior estigui desmarcat, aquest check box permetrà configurar el comportament quan es trobin el fileEncoderTypes obsolets.

Si es marca aquest check box, es deixarà el fileEncoderType configurat, ignorant que sigui obsolet (això pot ser útil si es desitja desencriptar amb una versió anterior de l’aplicació, que només tenia els fileEncoderTypes 1 i 2).

### Paràmetres de la configuració d’idiomes de l’aplicació

La pestanya té aquest aspecte:



Els paràmetres que poden configurar-se són els següents:

* **Idioma**. És l'idioma dels texts que escriu l'aplicació.

Els idiomes que es poden escollir son:

* EN. Anglès
* ES. Castellà
* L'idioma addicional que per defecte es CAT (català)
* **Locale de l’idioma**. És el Locale de Java que farà servir l’aplicació per a aquest idioma.

L’ús que fa l’aplicació del Locale, es per a donar format a les cadenes numèriques.

* **Idioma web**. Indica l’idioma que es farà servir a les consultes de nova versió al servidor.
* **Idioma addicional**. És un nou idioma addicional que apareix a l'hora de poder canviar d'idioma.

Pel nou idioma tindràs que seleccionar el Locale de Java que es farà servir.

Si vols posar un idioma del que no existeixen els texts en l'aplicació, pots afegir el teu idioma traduint els arxius que hi ha dins del directori que es crea quan prems el botó Acceptar.

Els arxius que s'han de traduir, es copien al directori indicat a: "Directori d'idioma addicional".

El format d'aquests arxius de texts es el de properties de Java.

Pels que no conegueu aquest format, us diré que un arxiu properties, té un títol, i després d'aquest, un número variable d'etiquetes amb el seu valor, semblant al que segueix:

# TITOL

# xxxxxxxxxx

ETIQUETA1=text 1

ETIQUETA2=text 2

...

Les etiquetes no s'han de modificar i els texts s'han de modificar tenint en compte la traducció a l'idioma escollit.

A més, també hi ha alguns arxius en format RTF que tindràs que traduir amb un editor de RTF (com per exemple el Word de Office).

Si crees la traducció per a un idioma addicional diferent als disponibles a l'aplicació, si vols pots enviar-me'l (frojasg1@hotmail.com) i l'inclouré a les següents versions de l'aplicació.

### Paràmetres de la configuració de vista de l’aplicació

La pestanya té aquest aspecte:



* Mida de les finestres de l'aplicació. Aquest paràmetre de configuració permet de canviar la mida de les finestres de l'aplicació, donant la possibilitat d’escollir la mida gran, normal o petita.

## Esborrament d’arxius

L’aplicació no permet encriptar/desencriptar si l’arxiu de sortida ja existeix, és a dir, no permet sobreescriure un arxiu.

Per això s’han afegit opcions per a l’esborrament d’arxius de manera còmoda i flexible.

Per a obrir el diàleg d’esborrament d’arxius, només has de prémer el botó amb una creu associat a l’arxiu que desitges esborrar:



Si l’arxiu que has escollit per a ser esborrar no existeix, llavors apareixerà una indicació al component de text (història) de la part inferior.

Si l’arxiu existia, llavors apareixerà el diàleg que permet escollir el mètode d’esborrament que desitges utilitzar:



En aquest punt es permeten tres opcions:

* Esborrar de manera segura: Es un esborrament que no permet que l’arxiu que s’esborra pugui ser recuperat amb cap eina de recuperació d’arxius.

Es fa servir el mètode d’escriure amb zeros tots els octets de l’arxiu, per després, finalment, fer un esborrament normal.

Aquest tipus d’esborrament, en èsser més costós, permet mostrar el progrés a la barra de progrés i també pot ser cancel.lat per l’usuari mitjançant el botó de cancel.lar que hi ha al costat de la barra de progrés.

* Borrar normal: Es fa un esborrament normal de l’arxiu.
* Cancel.lar: Permet cancel.lar la operación, per si t’havies equivocat de botó.

Un cop has escollit el tipus d’esborrament, l’aplicació comprova si existeis l’arxiu parella (és a dir, si es tracta d’esborrar l’arxiu encriptat, es comprova que l’arxiu desencriptat existeixi, i a l’inrevés).

Això es fa per evitar un possible esborrament accidentat d’un arxiu que no podria ser recuperat mitjançant l’encriptació o desencriptació del seu arxiu parella.

En aquest cas es mostra un avís com aquest:



Que bàsicament demana la confirmació de que es desitja esborrar l’arxiu.

Un cop que l’aplicació s’ha assegurat de que realment vols esborrar l’arxiu, llavors s’executen les accions sobre tots el arxius associats (és a dir, si es tracta d’un arxiu encriptat del fileEncodertype-8, que permet múltiples volums, llavors s’esborrarien tots el volums a l’hora).

## Sobre l’aplicació

La opció Sobre l’aplicació, mostra una finestra amb un resum de les novetats en aquesta versió. També s’inclouen els agraïments.

Té un aspecte com aquest:



## Llicència

La opció Llicència, dins el menú Sobre l’aplicació, mostra la llicència que es va acceptar el primer cop que es va executar l’aplicació.

Té un aspecte com aquest:



# Encriptació per la interfície d'ordres

A més de poder encriptar i desencriptar des de la interfície gràfica de l'aplicació, també és possible invocar a les funcions desencriptar i desencriptar per la interfície d'ordres.

Es pot passar la password d’encriptació mitjançant un paràmetre dels scripts. Això no és molt recomanable, ja que per encriptar/desencriptar s'ha de posar la contrasenya en clar i és possible que algú pugui veure-la simplement mirant la història d'ordres o inclús veient els processos que hi ha actius al sistema. També és possible que tinguis que teclejar la contrasenya i que aquesta es vegi a la teva pantalla, és per això que aquesta no és una manera molt segura d’utilitzar els scripts.

És preferible no passar el paràmetre password (que és opcional) als scripts. D’aquesta manera l’aplicació preguntarà per teclat el valor de la password i la seva confirmació.

Existeix un directori (\_scripts) en el que s'han generat una sèrie de scritps per facilitar la tasca. Hi ha dues versions dels scripts, una per a Windows (scripts \*.bat) i l'altra que serveis tant per Linux com per a Mac (scripts \*.sh)

## Scripts per a Windows

La versió per a Windows dels scripts es troba al directori:

...\\_scripts\windows

Els scripts disponibles son aquests:

* command.interface.FileEncoder.bat
* decodeFile.bat
* encodeFile.bat
* example.decodeFile.bat
* example.encodeFile.bat

Per a invocar aquests scripts, s'ha de fer des de el mateix directori en el que es troben ubicats.

El primer script conté la invocació a l'aplicació de Java, recollint els arguments que li són passats i afegint-los als arguments per a l'aplicació de Java.

El segon script conté les orders per a desencriptar un arxiu encriptat. Pren como a paràmetres el nom de l'arxiu encriptat i la contrasenya.

El tercer script conté les orders per encriptar un arxiu. Pren com a paràmetres el nom de l'arxiu i la contrasenya.

El quart script és un exemple de com invocar al script que encripta.

El cinquè script és un exemple de com invocar al script que desencripta.

En tots els scripts, el paràmetre password s’ha fet opcional, de manera que si s’inclou la password en la invocació a l’aplicació, aquesta preguntarà la password per teclat.

## Scripts per a Linux y per Mac

La versió per a Linux i per a Mac dels scripts es troba al directori:

.../\_scripts/Mac.or.Linux

En un principi aquests scripts estan comprimits a l'arxiu: scripts.tar.gz

S'ha de descomprimir aquest arxiu per a poder treballar amb els scripts. Per fer-ho, des de el directori on es trobe l'arxiu script scripts.tar.gz, teclejar la següent order:

tar -xvzf scripts.tar.gz

Un cop descomprimits al directori, tenim els següents scripts:

* command.interface.FileEncoder.sh
* decodeFile.sh
* encodeFile.sh
* example.decodeFile.sh
* example.encodeFile.sh

Per a invocar aquests scripts, s'ha de fer des de el mateix directori en el que es troben ubicats.

El primer script conté la invocació a l'aplicació de Java, recollint els arguments que li són passats i afegint-los als arguments per a l'aplicació de Java.

El segon script conté les orders per a desencriptar un arxiu encriptat. Pren como a paràmetres el nom de l'arxiu encriptat i la contrasenya.

El tercer script conté les orders per encriptar un arxiu. Pren com a paràmetres el nom de l'arxiu i la contrasenya.

El quart script és un exemple de com invocar al script que encripta.

El cinqué script és un exemple de com invocar al script que desencripta.

En tots els scripts, el paràmetre password s’ha fet opcional, de manera que si s’inclou la password en la invocació a l’aplicació, aquesta preguntarà la password per teclat.

## Paràmetres d'encriptació com a arguments

Dels scripts anteriors el principal és aquest:

command.interface.FileEncoder

Des de ell s'invoca a l'aplicació Java i com a paràmetres pren principalment els que ja s'han descrit al punt: 3.7.1-Paràmetres de la configuració de encriptació

Els paràmetres disponibles per a encriptar/desencriptar son aquests:

* -password Seguir per un argument amb la password. És opcional. Si no es facilita la password, l’aplicació la preguntarà per teclat a l’usuari (password i confirmació).
* -encodedFileName Seguit per un argument amb el nom de l'arxiu encriptat.
* -decodedFileName Seguir per un argument amb el nom de l'arxiu desencriptat.
* -encode o -decode Per a seleccionar entre enc riptació i desencriptació.
* -fileEncoderType SEguir per un argument amb l'identificador del fileEncoderType (1, obsolet o 2) a utilitzar a l'encriptació (només té sentit quan s'encripta)
* -sizeOfNumbersSimpleEncoder Seguir pel tamany dels números per al primer pas d'encriptació (XOR) (només té sentit quan s'encripta).
* -sizeOfNumbersReordererEncoder Seguit pel tamany dels números per al segon pas d'encriptació (reordenació) (només té sentit quan s'encripta).
* -numberOfBitsPerIterationSimpleEncoder Seguir pel número de bits tornats pel generador pseudoaleatori en cada iteració per al primer pas (XOR) (només té sentit quan s'encripta).
* -numberOfBitsPerIterationReordererEncoder Seguir pel número d ebits tornats pel generador pseudoaleatori en cada iteració per al segon pas (reordenació) (només té sentit quan s'encripta).
* -numBytesFileSlice Seguit pel número d'octets que formen un bloc. Es recomana utilitzar un valor alt per a aquest paràmetre. La memòria utilitzada per l'aplicació està limitat aproximadament per 100 cops el tamany del bloc(només té sentit quan s'encripta).
* -useFileSizeForEncryptingParams Si aquest paràmetre està present, els paràmetres d'encriptació (descrits als 5 paràmetres anterior) seran calculats basant-se en el tamany de l'arxiu a encriptar i els 5 valors anteriors seran sobreescrits (només té sentit quan s'encripta).
* -encDecOnDifferentDrives Només aplica als tipus d’encriptación FileEncoderType 7 i 8.

Si aquest paràmetre està present (no té valor associat), indicaria que els arxius d’entrada i de sortida es troben a discos diferents i que l’aplicació farà servir fils separats per a la lectura de l’arxiu d’entrada i per a l’escriptura de l’arxiu de sortida (un per a cadascú).

Si aquest paràmetre no està present llavors es farà servir un sol fil separat conjunt per a la lectura de l’arxiu d’entrada i per a l’escriptura de l’arxiu de sortida.

* -numOfThreads Aquest paràmetre només és vàlid per als tipus d’encriptación FileEncoderType 7 i 8, i indica el número de fils d’encriptació que s’intentaran fer servir (en cas de que no aparegui el paràmetre: -encDecOnDifferentDrives).

 (ver apartado: ***5.4-Utilització de fils d’execució (paral.lelisme)*** sobre l’ús de fils).

Valor *optimum*:

Aquest paràmetre pot configurar-se amb el valor “optimum” (en fase experimental) que indicarà a l’aplicació que aquest paràmetre s’estimarà just abans de l’encriptació, mitjançant la fórmula indicada a l’apartat ***5.4-Utilització de fils d’execució (paral.lelisme)***).

* -numOfThreadsForDifferentDrives. Aquest paràmetre només és vàlid per als tipus d’encriptación FileEncoderType 7 i 8, i indica el número de fils d’encriptació a fer servir en cas de que els arxius d’entrada i de sortida es trobin a discos diferents. (quan el paràmetre: -encDecOnDifferentDrives no està present).

Este parámetro toma valores mayores que el parámetro homólogo (el anterior), cuando los archivos de entrada y salida se encuentran en el mismo disco.

( Veure apartat ***5.4-Utilització de fils d’execució (paral.lelisme)*** per a més detall).

Valor *optimum*:

Aquest paràmetre pot configurar-se amb el valor “optimum” (en fase experimental) que indicarà a l’aplicació que aquest paràmetre s’estimarà just abans de l’encriptació, mitjançant la fórmula indicada a l’apartat ***5.4-Utilització de fils d’execució (paral.lelisme)***).

* -maxTotalNumOfThreads. Aquest paràmetre serveix per a limitar el número màxim de fils a fer servir pels tipus d’encriptación FileEncoderType 7 i 8.

El número total de fils a fer servir, és el número de fils d’encriptación (en cas de limitació, seria el que es decrementaria fins a complir amb el límit d’aquest paràmetre), més el número de fils d’entrada/sortida (1 o 2).

 ( Veure apartat ***5.4-Utilització de fils d’execució (paral.lelisme)*** per a un detall més gran).

Aquest paràmetre es pot configurar amb el valor “max”, que indica el número màxim de fils que permet fer servir el processador on s’executa l’aplicació.

* -sizeInBytesForVolumes. Aquest paràmetre indica la mida màxima (en octets) en què es dividirà l’arxiu encriptat amb el FileEncoderType-8.

# Mètode d'encriptació

Els algoritmes d'encriptació i desencriptació utilitzats són molt similars i idèntics en temps de computació (encriptació simètrica)

En els següents punts es veurà un resum del mètode d'encriptació utilitzat a l'aplicació.

## Capçalera de l'arxiu encriptat

Es calcula una hash de la contrasenya d'encriptació (SHA-256) que torna una clau de 256 bits que anomenarem clau-1.

El tamany de la clau-1 sempre és el mateix.

Si utilitzem el generador pseudoaleatori amb diferents paràmetres de configuració és possible que una clau de 256 bits no sigui òptima.

Es calcula el tamany òptim de la clau a ser utilitzada per inicialitzar els generadors pseudoaleatoris per a l'encriptació i l'anomenem tamany-2.

S'utilitza el micròfon con a font d'octets aleatoris i s'agafen d'ell tamany-2 octets que seran utilitzats per a formar la clau-2 que serà utilitzada per encriptar.

Si el micròfon no està disponible, s’obtindran els octets aleatoris amb la funció generateSeed de la classe SecureRandom.

Aquest mètode d’obtenció d’octets aleatoris és possible que sigui més lent que la obtenció d’octets a través del micròfon. Per això és aconsellable tenir el micròfon connectat.

La clau-2 s'utilitza per a encriptar l'arxiu.

La clau-1 s'utilitza per a encriptar la clau-2.

La clau-2 encriptada, els paràmetres de configuració de l'encriptació (sense encriptar) i una hash (MD5) (encriptada) de l'arxiu original s'escriuran a la capçalera de l'arxiu encriptat. (Això vol dir que a més de l’encriptació/desencriptació, s’ha de llegir l’arxiu desencriptat per a calcular la hash MD5).

Aquesta informació serà utilitzada per a desencriptar l'arxiu. La hash MD5 s'utilitzarà per a comprovar que el procés de desencriptació ha funcionat correctament.

En cas dels fileEncoderType 5, 6, 7 i 8, serà necessari guardar també la longitud de l’arxiu desencriptat, per tal de poder-lo recuperar correctament amb la desencriptació.

En el cas dels FileEncoderType 7 i 8, també es guarda a la capçalera el número de fils d’encriptació a fer servir.

En el cas del FileEncoderType 8, també es guarda la mida màxima dels volums en els que es divideix l’arxiu encriptat.

Degut a la particularitat del FileEncoderType 5, 6, 7 i 8, prèviament a l’acció de desencriptar, s’ha de crear l’arxiu complet amb zeros.

Això fa que per a aquests tipus d’encriptació, la desencriptació es faci una mica més lenta que l’encriptació.

## Algoritme d'encriptació

Aquesta aplicació realitza l'encriptació d'arxius en rodanxes, això és, dividint l'arxiu en parts més petites. Per encriptar cada una d'aquestes rodanxes es segueixen dos passos:

* Encriptació del blocestil XOR. En aquesta part de l'encriptació, generant bits pseudoaleatoris i fent un XOR amb les dades originals, s'obté un bloc encriptada i els octets d'aquest bloc són bastant aleatoris.

Si deixèssim aquí l'encriptació, seria relativament ràpid intentar trencar aquesta encriptació si es coneixen alguns octets de l'inici de l'arxiu sense encriptar, como és possible que es coneguin en el cas d'arxius que es puguin obrir amb alguna aplicació (per exemple Word o Excel), ja que generalment aquests arxius tindran algun tipus de capçalera que fa que l'encriptació d'aquest tipus sigui més vulnerable.

Degut a això l'aplicació genera un segon pas a l'encriptació:

* Reordenació pseudoaleatòria dels octets del bloc. En aquesta part de l'encriptació, es generen posicions pseudoaleatòries, on es van movent un a un els octets del bloc, reordenant el conjunt dels octets.

Per a obtenir els octets inicials de l'arxiu desencriptat, és necessari desencriptar un bloc complerta, això fa que es faci més difícil trencar l'encriptació, ja que és molt més costós en termes de temps de computació desencriptar un bloc complerta (que té mida configurable i que per defecte està a 256.000 octets), que desencriptar els 100 o 1000 primers octets i comparar-los amb una capçalera vàlida de word o excel, per exemple.

Els fileEncoderType 6, 7 i 8, eliminen aquest pas. Per això són molt més ràpids que els altres fileEncoderTypes.

* Reordenació pseudoaleatòria dels blocs. Aquesta part de l’encriptació només està present als fileEncoderType 5, 6, 7 i 8.

Aquest pas permet que l’encriptació d’arxius molt grans sigui molt difícil de trencar, ja que en ser aleatori l’ordre dels blocs, per a desencriptar el primer bloc (que conté la capçalera de l’arxiu desencriptat que pot tenir un format conegut, i permetre determinar si una password generada per força bruta és bona o no), s’haurà de desencriptar en mitja, la meitat dels blocs de l’arxiu.

Si l’arxiu és molt gran, un atac per força bruta es fa inviable, degut al cost computacional (es tardaria molt a trobar la password bona, inclús amb superordinadors).

Aquesta característica fa que els fileEncoderTypes 5, 6, 7 i 8 siguin els més difícils de trencar per a arxius grans.

En els passos anteriors, per a realitzar la seva part de l'encriptació s’utilitza un generador pseudoaleatori caòtic, que en la implementació actual estan caracteritzats bàsicament per un tamay dels números a utilitzar al generador i pel número de bits pseudoaleatoris a tornar en cada iteració. Depenent d'aquestos dos paràmetres el generador pseudoaleatori calcula el número d'octets òptim de la clau amb la que s'ha d'inicialitzar el generador pseudoaleatori.

Com més gran sigui el tamany dels números, més gran serà el tamany òptim de la clau i més gran serà el temps de computació per iteració.

Així doncs, un tamany més gran dels números fa que el temps d'encriptació/desencriptació sigui més gran. L'efecte sobre el temps de computació d'aquest paràmetre és més gran com més petit sigui el número de bits per iteració que torna el generador pseudoaleatori.

La configuració ideal seria una que produís una encriptació robusta i que fos ràpida. Per a aconseguir aquest objectiu, podríem utilitzar tamanys de número grans (més robust) amb un número alt de bits tornats per iteració (més ràpid) i combinat amb tamanys de bloc el més grans possible (molt més robust, però com més gran es aquest valor, més memoria s'utilitza).

Per arxius petits s'hauria d'utilitzar un número molt petit de bits tornats per iteració (per exemple: 1) i un tamany de números gran. El tamany del bloc hauria de ser com a mínim igual al tamany de l'arxiu a encriptar.

Com a exemples de configuracions d’encriptació òptimes:

* Per a arxius molt petits:
* fileEncoderType: 4
* Mida de números: 256
* Bits per iteració: 1
* Mida de bloc: 0
* Per a arxius grans (més grans de 100 MB):
* fileEncodertype: 7
* Mida de números: 10
* Bits per iteració: 64
* Mida de bloc: (com a molt la mida de l’arxiu / 10, amb un màxim de 16 MB).
* Número de fils: 3 (per a arxius d’entrada i de sortida al mateix disc).
* Número de fils: 5 ( per a arxius d’entrada i de sortida a discos separats).

## Generador pseudoaleatori utilitzat

El generador pseudoaleatori utilitzat en aquesta aplicació, és un generador pseudoaleatori basat en sequències caòtiques.

És un generador pseudoaleatori molt senzill i de molt fàcil implementació.

La descripció d'aquest generador pseudoaleatori s'ha extret del llibre:

"Secuencias pseudoaleatorias para telecomunicaciones" Edicions UPC (1996) Ernesto J. Forner Cruselles y José L. Melús Moreno

Un agraïment per a ells per escriure un llibre tan interessant.

Citant del propi llibre:

"

*Este generador, propuesto por M. Romera, I. Jiménez y J. Negrillo [ROM90], está basado*

*también en la generación de secuencias pseudoaleatorias mediante el empleo de funciones caóticas.*

*[ROM90] ROMERA, M.; JIMENEZ, I. NEGRILLO, J. Generación de Secuencias Cifrantes Mediante*

*Funciones Caóticas. I Reunión Española de Criptología. Mallorca, 1990.*

*...*

*La secuencia caótica de este generador (de números reales) está definida por:*

*Xo = 0*

*Xi+1 = Xi2 + K*

 *Si -2 <= K <= 0,25, entonces los números de esta secuencia están acotados: -2 <= Xi <= 2*

*Unas secuencias son cíclicamente convergentes (periodos 1, 2, 3 ...) y otras son caóticas.*

*Cuando K es muy próximo a -2, por ejemplo K = -1,99999XXXXXXXXXXX, las series que se obtienen a partir de la iteración real de Mandelbrot son casi siempre caóticas.*

*...*

*La secuencia real obtenida puede convertirse fácilmente en una secuencia pseudoaleatoria binaria, tomando el signo de cada número de la serie (la distribución es simétrica respecto a cero), o aplicando un criterio de paridad a los dígitos de cada número de la serie.*

"

Basant-nos en aquest generador de seqüències caòtiques, hem creat el nostre generador molt similar a aquest, que a grans trets compleix amb les següents condicions:

-1 <= Xo  <= 1

K = -1,99999999xxxxxxxxxxxxxxxxxxxxxxxx

Per a inicialitzar el generador pseudoaleatori, necessitarem una llavor (un número d'octets), que utilitzarem per a inicialitzar Xo y la part variable de K.

Tant X com K han de ser números de precisió configurable que permeti una precisió molt gran, ja que si utilitzen els tipus bàsics de precisió més gran que existeixen a Java (double), el rang de la llavor seria molt limitat i per força bruta podria trencar-se fàcilment el sistema pseudoaleatori.

Les opcions que tenim són:

* Utilitzar la classe BigDecimal de Java (Utilitzat en el FileEncoderType=1, no recomanat).
* Programar una classe nova que tracti números de precisió variable (Utilitzat en el FileEncoderType=2 i 3 (OBSOLETS) i FileEncoderType=4 (recomanat per a arxius petits), 5 (recomant per a arxius de mida mitjana), 6 (no recomanat)i 7 i 8 (recomanats per a arxius grans).

Els bits pseudoaleatoris que es deriven de la seqüència caòtica són obtinguts d'aquestes maneres:

* Quan el número de bits produïts per iteració és 1, 2 o 4 (per a tots els fileEncoderTypes): Es compten els bits "1" del Xi i es fa el mòdul (2 si el número de bits per iteració era 1, 4 si era 2 o 16 si era 4).

Aquesta és la versió més robusta del generador pseudoaleatori (més costosa en temps de computació i menys depenent del valor concret de Xi)

D'aquesta manera s'obtenen els bits pseudoaleatoris en cada iteració de la seqüència caòtica.

* Si s'utilitza un bit per iteració, no hi ha limitació de la mida del número, ja que els possibles valors produïts (0 o 1) són sempre equiprobables independentment del número de bits utilitzat.
* Si s'utilitzen 2 bits per iteració, es millor utilitzar números de mida superior o igual a 16 bits, ja que per exemple, fent el mòdul 4 de la compta de bits "1" de un número caòtic de 8 bits (resultant 0, 1, 2 o 3), aquests valors no serien equiprobables, però amb mides de número de 16 bits, la diferència de probabilitat ja és negligible.
* Si s'utilitzen 4 bits per iteració, és millor utilitzar números de mida superior o igual a 256 bits.

A la següent taula es poden veure les probabilitats de cada valor possible en funció de la mida del número quan s'han de produir 4 bits pseudoaleatoris per iteració:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Valor | númerosde 16 bits | númerosde 32 bits | númerosde 64 bits | númerosde 128 bits | númerosde 192 bits | númerosde 256 bits |
| 0 | 0,00305176% | 13,99499346% | 9,93997199% | 7,29371224% | 6,55137753% | 6,33706399% |
| 1 | 0,02441406% | 13,17175925% | 9,64196694% | 7,21415681% | 6,52843586% | 6,33043664% |
| 2 | 0,18310547% | 10,97647697% | 8,80338313% | 6,98766512% | 6,46310389% | 6,31156353% |
| 3 | 0,85449219% | 8,08803737% | 7,57614083% | 6,64887061% | 6,36532878% | 6,28331793% |
| 4 | 2,77709961% | 5,25798649% | 6,17124246% | 6,24950378% | 6,24999687% | 6,24999998% |
| 5 | 6,66503906% | 3,00877392% | 4,81247919% | 5,85042763% | 6,13466680% | 6,21668205% |
| 6 | 12,21923828% | 1,52314156% | 3,69661687% | 5,51233488% | 6,03689611% | 6,18843647% |
| 7 | 17,45605469% | 0,73142946% | 2,96941304% | 5,28654495% | 5,97156857% | 6,16956339% |
| 8 | 19,63806152% | 0,48979651% | 2,71754309% | 5,20728020% | 5,94862872% | 6,16293605% |
| 9 | 17,45605469% | 0,73142946% | 2,96941304% | 5,28654495% | 5,97156857% | 6,16956339% |
| 10 | 12,21923828% | 1,52314156% | 3,69661687% | 5,51233488% | 6,03689611% | 6,18843647% |
| 11 | 6,66503906% | 3,00877392% | 4,81247919% | 5,85042763% | 6,13466680% | 6,21668205% |
| 12 | 2,77709961% | 5,25798649% | 6,17124246% | 6,24950378% | 6,24999687% | 6,24999998% |
| 13 | 0,85449219% | 8,08803737% | 7,57614083% | 6,64887061% | 6,36532878% | 6,28331793% |
| 14 | 0,18310547% | 10,97647697% | 8,80338313% | 6,98766512% | 6,46310389% | 6,31156353% |
| 15 | 0,02441406% | 13,17175925% | 9,64196694% | 7,21415681% | 6,52843586% | 6,33043664% |

Com es pot observar a la taula, si la mida dels números és petit no tindrem uns bits retornats el suficientment equiprobables com per a encriptar.

* Quan el número de bits produïts per iteració és un múltiple de 8 entre 8 i 64 (ambdós inclosos) (només FileEncoderType 2, 3, 4, 5, 6, 7 i 8):

En aquest cas es prenen octets complerts que formen part de Xi per a utilitzar-los com si fossin números pseudoaleatoris. Això no és exacte, però per a que vagi més ràpid s'han de treure el bits pseudoaleatoris d'algun lloc. Segurament no és tan robust com comptar el número de bits "1" del número Xi, però crec que pot servir.

Obtenir els bits pseudoaleatoris per aquest mètode és molt ràpid. Només s'han d'agafar els octets pseudoaleatoris directament. A més, permet d'agafar un número gran de bits per iteració.

La condició que s'ha de complir entre el número de bits produïts per iteració i la mida en blocs (blocs de 31 bits, cada bloc s'emmagatzema en un long, que a la seva vegada s'emmagatzema en un array de longs de longitud variable) es aquesta:

NumeroBitsPerIteracio / 8 <= 3 x NumeroBlocsPerNumero

Ja que s'agafen com a molt 3 octets de cada bloc.

## Utilització de fils d’execució (paral.lelisme)

Aquesta característica només està present als FileEncoderType 7 i 8.

Aquests tipus d’encriptació afegeixen suport per a múltiples fils d’execució.

* Ús dels fils:
	+ Quan l’arxiu encriptat i desencriptat es troben al mateix disc:
		- Un fil separat que s’utilitza per a centralitzar l’entrada/sortida des de/cap als arxius. Aquest fil alimenta als fils d’encriptació, llegint rodanxes de l’arxiu d’entrada i escrivint el resultat a l’arxiu de sortida.
		- Un conjunt de fils d’encriptació.
	+ Quan l’arxiu encriptat i el desencriptat es troben a discos separats:
		- Un fil separat que es fa servir per a centralitzar la lectura de l’arxiu d’entrada. Aquest fil alimenta els fils d’encriptació, llegint rodanxes de l’arxiu d’entrada.
		- Un fil separat que es fa servir per a centralitzar l’escriptura de l’arxiu de sortida.

Aquest fil rep rodanxes a escriure, i les va escrivint en paral.lel a la lectura de l’arxiu d’entrada.

* + - Un conjunto de fils d’encriptació.
* Característiques dels fils d’encriptació:

Cada fil d’encriptació fa servir un encriptador/desencriptador propi i cadascun d’aquests fils es caracteritza per un índex que va desde 0 fins al total de fils d’encriptació utilitzats.

Cada fil d’encriptació, rebrà per ordre totes les rodanxes amb una posició de rodanxa congruent amb l’índex del fil mòdul el número total de fils d’encriptació (és a dir, les rodanxes es van repartint en ordre per a cada fil d’execució).

Cada fil d’encriptació fa servir l’encriptador/desencriptador per a encriptar/desencriptar en ordre les rodanxes que li corresponen de l’arxiu d’entrada.

* Valor òptim del número de fils d’encriptació
	+ Cas de un sol fil d’entrada/sortida.

El número mínim de fils d’encriptació que minimitza el temps total de procés es pot calcular teòricament amb aquesta fórmula:

$$optimum=SenserSuperior\left( \frac{T\_{p}}{\left(T\_{i}+T\_{o}\right)}\right)$$

On: $optimum$ és el número òptim de fils d’encriptació a fer servir

 $T\_{p}$ és el temps de processament (encriptació pura) d’una rodanxa.

 $T\_{i}$ és el temps de lectura d’una rodanxa.

 $T\_{o}$ és el temps d’escriptura d’una rodanxa.

* + - Tenim que $T\_{p}$ depèn dels paràmetres d’encriptació (la mida dels números a fer servir pel generador pseudoaleatori i també el número de bits obtinguts per iteració). Com és obvi $T\_{p}$ també depèn de la potència del processador.
		- I tenim que $T\_{i}$ i $T\_{o}$ depenen de la unitat de disc on es troba l’arxiu d’entrada i on s’escriurà l’arxiu de sortida. També dependrà de si el disc està sent utilitzat en aquests moments per una altra aplicació, de si està fragmentat, etc.
	+ Cas de fils d’entrada i sortida separats (en el cas de que els arxius siguin a discos separats)

El número òptim de fils pot ser calculat com:

$$optimum=SenserSuperior\left( \frac{T\_{p}}{max\left(T\_{i}, T\_{o}\right)}\right)$$

Ja que els fils de lectura i d’escriptura de disc estan separats (treballant en paral.lel), i el temps total que es tarda en llegir i escriure una rodanxa, pot calcular-se com el màxim entre el temps de lectura i el temps d’escriptura (que en qualsevol cas serà més petit que la suma d’ells).

Això vol dir que el número òptim de fils en aquest cas serà més gran o igual al del cas d’entrada i sortida conjunta (al mateix disc).

* Limitacions teòriques:

El número de fils d’encriptació no hauria de ser més gran que el número de fils en paral.lel que suporta el processador menys el número de fils dedicats a lectura/escriptura de disc (per a aplicar aquest límit, es pot fer servir el paràmetre: -maxTotalNumOfThreads, que limita automàticament el màxim número total de fils a fer servir).

El número màxim de fils que suporta el processador acostuma a ser un múltiple del número de cores que té el processador.

Per exemple, el processador del meu PC es un i7, (4 cores), però degut al hyper-threading, el número de fils simultanis que gestiona el processador es de 8.

Després del càlcul del número òptim de fils d’encriptació, s’ha de limitar aquest resultat al límit teòric que acaben de veure.

Això és així, perquè podria ser que tinguéssim un sistema amb el disc molt ràpid (temps d’entrada i de sortida petits), i un temps de processament gran (processador molt lent).

En aquest cas tindríem un valor óptim gran, que podria ser superior al número màxim de fils que és recomanable fer servir (relacionat amb les capacitat del nostre processador).

En aquest cas, encara que tinguem un disc molt ràpid, tindríem el coll d’ampolla al processador, i en aquest cas no podríem fer servir el número òptim de fils.

* L’opció més ràpida

Si els arxius estan a discos separats, es pot aconseguir una eficiència i ocupació de processador més grans, traduint-se en una velocitat d’encriptació més gran. (Sempre que tinguem un processador suficientment potent).

Si es busca rapidesa a l’encriptació, idealment s’ha de fer que els arxius d’entrada i de sortida es trobin a discos separats.

* Memòria utilitzada

Un altre punt a tenir en compte és la memòria utilitzada per l’aplicació.

Com més gran sigui el número de fils, més gran serà la quantitat de memòria feta servir per l’aplicació.

És per això que s’ha definit un límit, per a evitar valors molt grans sense sentit que farien servir molta memòria.

# Tipus d’encriptació

L’aplicació FileEncoderApplication encripta en base a un conjunt de tipus d’encriptació que es va ampliant en cada versió.

Això permet mantenir la compatibilitat cap enrere, i es pot augmentar la seva funcionalitat afegint nous tipus d’encriptació.

En aquest capítol detallarem els diferents tipus d’encriptació disponibles en aquesta versió de l’aplicació.

## FileEncoderType-1

FileEncoderType **no recomanat**, que funciona amb un generador pseudoaleatori caòtic que internament utilitza números en format BigDecimal.

La desavantatge d’aquest generador pseudoaleatori es que està intimament lligat a la implementació en Java, sent més complicada la seva traducció a d’altres possibles llenguatges de programació.

A més, fent servir aquest tipus de números, es perdia el control i podria haver passat que la implementació d’aquesta classe canviés entre versions de Java, trencant la compatibilitat de l’aplicació executada sobre diferents versions de JRE.

Ès per això que la utilització d’aquest tipus d’encriptació no està recomanada.

Però encara existeix per a mantenir la compatibilitat cap enrere.

Les característiques d’aquest tipus d’encriptació són aquestes:

* Basat en rodanxes.
* Cada rodanxa es codifica amb una encriptació basada en XOR.
* Cada rodanxa reordena els seus octets internament, per a fer més costosa la seva desencriptació.
* Generador pseudoaleatori caòtic basat en la classe de Java BigDecimal.
* Paràmetres:
	+ NumBytesFileSlice. Mida de la rodanxa en octets
	+ SizeOfNumbersSimpleEncoder. Mida dels números BigDecimal (en octets) del generador pseudoaleatori XOR (rang-> 1-127)
	+ SizeOfNumbersReordererEncoder. Mida dels números BigDecimal (en octets) del generador pseudoaleatori fet servir per a la reordenació. (rang-> 1-127)
	+ NumBitsPerIterationSimpleEncoder. Número de bits que s’obtindran del generador pseudoaleatori en cada iteració del generador pseudoaleatori XOR.
	+ NumBitsPerIterationReordererEncoder. Número de bits que s’obtindran del generador pseudoaleatori en cada iteració del generador pseudoaleatori para la reordenació.

## FileEncoderType-2

FileEncoderType **obsolet**, que funcionava amb un generador pseudoaleatori caòtic que internament feia servir números en format BigLong que va passar a ser BigLong\_deprecated desprès de que aparegués un ERROR, que apareixia sempre en encriptar arxius grans.

Es un tipus d’encriptació que es manté per compatibilitat cap enrere.

Les característiques d’aquest tipus d’encriptació són aquestes:

* Basat en rodanxes.
* Cada rodanxa es codifica amb una encriptació basada en XOR.
* Cada rodanxa reordena els seus octets internament, per a fer més costosa la seva desencriptació.
* Generador pseudoaleatori caòtic basat en la clase pròpia BigLong\_deprecated, que **té un error greu**.
* Paràmetres:
	+ NumBytesFileSlice. Mida de la rodanxa en octets
	+ SizeOfNumbersSimpleEncoder. Mida dels números BigLong\_deprecated (en bloques de 31 bits) del generador pseudoaleatori XOR (rang-> 1-127)
	+ SizeOfNumbersReordererEncoder. Mida dels números BigLong\_deprecated (en bloques de 31 bits) del generador pseudoaleatori fet servir per a la reordenació. (rang-> 1-127)
	+ NumBitsPerIterationSimpleEncoder. Número de bits que s’obtindran del generador pseudoaleatori en cada iteració del generador pseudoaleatori XOR.
	+ NumBitsPerIterationReordererEncoder. Número de bits que s’obtindran del generador pseudoaleatori en cada iteració del generador pseudoaleatori para la reordenació.

## FileEncoderType-3

FileEncoderType **obsolet**, que es idèntic a l’antarior, però amb la mida del números extesa, per a aprofitar també el bit de signe de l’octet de la capçalera que guarda el seu valor.

És un tipus que es manté per compatibilitat cap enrere.

Les característiques d’aquest tipus d’encriptació són aquestes:

* Basat en rodanxes.
* Cada rodanxa es codifica amb una encriptació basada en XOR.
* Cada rodanxa reordena els seus octets internament, per a fer més costosa la seva desencriptació.
* Generador pseudoaleatori caòtic basat en la clase pròpia BigLong\_deprecated, que **té un error greu**.
* Paràmetres:
	+ NumBytesFileSlice. Mida de la rodanxa en octets
	+ SizeOfNumbersSimpleEncoder. Mida dels números BigLong\_deprecated (en bloques de 31 bits) del generador pseudoaleatori XOR (rang-> 1-256)
	+ SizeOfNumbersReordererEncoder. Mida dels números BigLong\_deprecated (en bloques de 31 bits) del generador pseudoaleatori fet servir per a la reordenació. (rang-> 1-256)
	+ NumBitsPerIterationSimpleEncoder. Número de bits que s’obtindran del generador pseudoaleatori en cada iteració del generador pseudoaleatori XOR.
	+ NumBitsPerIterationReordererEncoder. Número de bits que s’obtindran del generador pseudoaleatori en cada iteració del generador pseudoaleatori para la reordenació.

## FileEncoderType-4

FileEncoderType **especialment recomanat per a arxius petits**.

És idèntic a l’anterior, però amb l’error de la classe clase BigLong solucionat.

Les característiques d’aquest tipus d’encriptació són aquestes:

* Basat en rodanxes.
* Cada rodanxa es codifica amb una encriptació basada en XOR.
* Cada rodanxa reordena els seus octets internament, per a fer més costosa la seva desencriptació.
* Generador pseudoaleatori caòtic basat en la clase pròpia BigLong. De moment no s’han trobat errors.
* Paràmetres:
	+ NumBytesFileSlice. Mida de la rodanxa en octets
	+ SizeOfNumbersSimpleEncoder. Mida dels números BigLong\_deprecated (en bloques de 31 bits) del generador pseudoaleatori XOR (rang-> 1-256)
	+ SizeOfNumbersReordererEncoder. Mida dels números BigLong\_deprecated (en bloques de 31 bits) del generador pseudoaleatori fet servir per a la reordenació. (rang-> 1-256)
	+ NumBitsPerIterationSimpleEncoder. Número de bits que s’obtindran del generador pseudoaleatori en cada iteració del generador pseudoaleatori XOR.
	+ NumBitsPerIterationReordererEncoder. Número de bits que s’obtindran del generador pseudoaleatori en cada iteració del generador pseudoaleatori para la reordenació.

## FileEncoderType-5

FileEncoderType **no recomanat**. (ja que es va crear per a se utilitzat amb arxius grans, però amb una mida de rodanxa petit. Això no és recomanable, ja que **el capçat del disc** es torna boig i **podria fer-se malbé**).

Les característiques d’aquest tipus d’encriptació són aquestes:

* Basat en rodanxes.
* Cada rodanxa es codifica amb una encriptació basada en XOR.
* Cada rodanxa reordena els seus octets internament, per a fer més costosa la seva desencriptació.
* Les rodanxes reordenen la seva posició pseudoaleatòriament.
* Generador pseudoaleatori caòtic basat en la clase pròpia BigLong. De moment no s’han trobat errors.
* Paràmetres:
	+ NumBytesFileSlice. Mida de la rodanxa en octets
	+ SizeOfNumbersSimpleEncoder. Mida dels números BigLong\_deprecated (en bloques de 31 bits) del generador pseudoaleatori XOR (rang-> 1-256)
	+ SizeOfNumbersReordererEncoder. Mida dels números BigLong\_deprecated (en bloques de 31 bits) del generador pseudoaleatori fet servir per a la reordenació. (rang-> 1-256)
	+ NumBitsPerIterationSimpleEncoder. Número de bits que s’obtindran del generador pseudoaleatori en cada iteració del generador pseudoaleatori XOR.
	+ NumBitsPerIterationReordererEncoder. Número de bits que s’obtindran del generador pseudoaleatori en cada iteració del generador pseudoaleatori para la reordenació.

## FileEncoderType-6

FileEncoderType (**recomanat per a arxius molt grans**, en ordinador que disposin de **poca memòria RAM** lliure).

És idèntic al del punt anterior, però eliminant la reordenació interna dels octets de cada rodanxa.

Es fa servir per a arxius grans, ja que en suprimir la reordenació interna dels octets de cada rodanxa, s’incrementa la velocitat moltíssim.

A més, per a fer aquest tipus d’encriptació més difícil de trencar, es fa una reordenació pseudoaleatòria de l’ordre de les rodanxes a l’arxiu.

Això fa que (en mitja), s’hagin de desencriptar la meitat de les rodanxes de l’arxiu encriptat, per a obtenir la rodanxa inicial de l’arxiu desencriptat.

A més, això fa que les rodanxes puguin ser més grans (ja no es necessita tanta memòria per a la reordenació dels octets de la rodanxa), evitant el problema del capçal explicat al punt anterior.

Mp obstant, per a aquesta versió de l’aplicació s’han creat tipus d’encriptació més ràpids (que fan servir múltiples fils), especialment dissenyats per a treballar amb arxius grans i que fan que aquest tipus d’encriptació només sigui recomanable quan es disposa de poca memòria RAM lliure al sistema.

Les característiques d’aquest tipus d’encriptació són aquestes:

* Basat en rodanxes.
* Cada rodanxa es codifica amb una encriptació basada en XOR.
* Les rodanxes reordenen la seva posició pseudoaleatòriament.
* Generador pseudoaleatori caòtic basat en la clase pròpia BigLong. De moment no s’han trobat errors.
* Paràmetres:
	+ NumBytesFileSlice. Mida de la rodanxa en octets
	+ SizeOfNumbersSimpleEncoder. Mida dels números BigLong\_deprecated (en bloques de 31 bits) del generador pseudoaleatori XOR (rang-> 1-256)
	+ NumBitsPerIterationSimpleEncoder. Número de bits que s’obtindran del generador pseudoaleatori en cada iteració del generador pseudoaleatori XOR.

## FileEncoderType-7

FileEncoderType (**recomanat per a arxius molt grans**).

Si el teu ordinador té problemes de memòria RAM lliure, hauria de configurar-se el número de fils d’encriptació a 1.

És idèntic al del punt anterior, però fent servir múltiples fils, cosa que bé configurat pot donar-li molta més velocitat a l’encriptació.

Les característiques d’aquest tipus d’encriptació són aquestes:

* Basat en rodanxes.
* Cada rodanxa es codifica amb una encriptació basada en XOR.
* Les rodanxes reordenen la seva posició pseudoaleatòriament.
* Generador pseudoaleatori caòtic basat en la clase pròpia BigLong. De moment no s’han trobat errors.
* Es fan servir diferent fils d’execució en paral.lel:
	+ Quan l’arxiu encriptat i el desencriptat estan al mateix disc:
		- Un fil separat comú per a la lectura i escriptura del disc.
		- Un o més fils per a encriptar.
	+ Quan l’arxiu encriptat i el desencriptat es troben a discos diferents:
		- Un fil separat per a la lectura del disc de l’arxiu d’entrada.
		- Un fil separat per a l’escriptura en disc de l’arxiu de sortida.
		- Un o més fils per a encriptar.
* Paràmetres:
	+ NumBytesFileSlice. Mida de la rodanxa en octets
	+ SizeOfNumbersSimpleEncoder. Mida dels números BigLong\_deprecated (en bloques de 31 bits) del generador pseudoaleatori XOR (rang-> 1-256)
	+ NumBitsPerIterationSimpleEncoder. Número de bits que s’obtindran del generador pseudoaleatori en cada iteració del generador pseudoaleatori XOR.
	+ NumOfThreads. Número de fils d’encriptació pel cas de l’arxiu encriptat i desencriptat al mateix disc.
	+ NumOfThreadsForDifferentDrives. Número de fils d’encriptació pel cas d’arxiu encriptat i arxiu desencriptat a discos diferents.
	+ MaxTotalNumberOfThreads. Límit per al número total de fils a fer servir (contant els fils d’encriptació i els d’entrada i sortida).

## FileEncoderType-8

FileEncoderType (recomant **per a arxius molt grans**). Especialment recomanat **quan el disc** on s’escriurà l’arxiu encriptat **té limitació de mida màxima d’arxiu**.

Si el teu ordinador té problemes de memòria RAM lliure, s’hauria de configurar el número de fils d’encriptació a 1.

És idèntic al del punt anterior, però afegint la possibilitat de definir una mida màxima de volum (es dividirà l’arxiu encriptat en volums, respectant aquesta mida màxima).

Les característiques d’aquest tipus d’encriptació són aquestes:

* Basat en rodanxes.
* Cada rodanxa es codifica amb una encriptació basada en XOR.
* Les rodanxes reordenen la seva posició pseudoaleatòriament.
* Generador pseudoaleatori caòtic basat en la clase pròpia BigLong. De moment no s’han trobat errors.
* Es fan servir diferent fils d’execució en paral.lel:
	+ Quan l’arxiu encriptat i el desencriptat estan al mateix disc:
		- Un fil separat comú per a la lectura i escriptura del disc.
		- Un o més fils per a encriptar.
	+ Quan l’arxiu encriptat i el desencriptat es troben a discos diferents:
		- Un fil separat per a la lectura del disc de l’arxiu d’entrada.
		- Un fil separat per a l’escriptura en disc de l’arxiu de sortida.
		- Un o més fils per a encriptar.
* Con la possibilitat de dividir l’arxiu encriptat en volums.
* Paràmetres:
	+ NumBytesFileSlice. Mida de la rodanxa en octets
	+ SizeOfNumbersSimpleEncoder. Mida dels números BigLong\_deprecated (en bloques de 31 bits) del generador pseudoaleatori XOR (rang-> 1-256)
	+ NumBitsPerIterationSimpleEncoder. Número de bits que s’obtindran del generador pseudoaleatori en cada iteració del generador pseudoaleatori XOR.
	+ NumOfThreads. Número de fils d’encriptació pel cas de l’arxiu encriptat i desencriptat al mateix disc.
	+ NumOfThreadsForDifferentDrives. Número de fils d’encriptació pel cas d’arxiu encriptat i arxiu desencriptat a discos diferents.
	+ MaxTotalNumberOfThreads. Límit per al número total de fils a fer servir (contant els fils d’encriptació i els d’entrada i sortida).
	+ SizeInBytesForVolumes. Mida màxima en octets per a cadascun dels volums en els que es dividirà l’arxiu encriptat a l’hora d’encriptar.