Manual d'usuari de la File Encoder Application v1.0

# Índex

[0. Índex 1](#_Toc415691702)

[1. Introducció 1](#_Toc415691703)

[2. Inici ràpid 2](#_Toc415691704)

[3. Funcionament de l'aplicació 3](#_Toc415691705)

[3.1. Pantalla principal 3](#_Toc415691706)

[3.2. Menú Arxiu 6](#_Toc415691707)

[3.3. Menú Eines 6](#_Toc415691708)

[3.4. Menú Sobre l'aplicació 7](#_Toc415691709)

[3.5. Llista de configuracions de encriptació 7](#_Toc415691710)

[3.5.1. Conceptes bàsics 7](#_Toc415691711)

[3.5.2. El formulari 8](#_Toc415691712)

[3.6. Configuració d'encriptació 9](#_Toc415691713)

[3.6.1. Paràmetres de la configuració de encriptació 9](#_Toc415691714)

[3.7. Configuració de la aplicació 12](#_Toc415691715)

[4. Encriptació per la interfície d'ordres 14](#_Toc415691716)

[4.1. Scripts per Windows 15](#_Toc415691717)

[4.2. Scripts per Linux y per Mac 15](#_Toc415691718)

[4.3. Paràmetres d'encriptació com a arguments 16](#_Toc415691719)

[5. Mètode d'encriptació 17](#_Toc415691720)

[5.1. Capçalera de l'arxiu encriptat 17](#_Toc415691721)

[5.2. Algoritme d'encriptació 17](#_Toc415691722)

[5.3. Generador pseudoaleatori utilizat 18](#_Toc415691723)

# Introducció

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

Básicamente permet:

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

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'únic desavantatge d'utilitzar l'linterfície d'ordres és que s'ha d'escriure la contrasenya en clar i pot ser vista per algun curiós.

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 sigur probada únicament amb processadors Intel, en Windows 8, Linux i OS-X pero també hauria de ser compatible amb qualsevol plataforma que tingui instal.lada la màquina virtual de Java (JRE).

Existeixen diferents paràmetres de configuración 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 robustasa 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, pot deixar-se 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'utilzar 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 caracters, el sistema d'encriptació es fa més fort.

# Inici ràpid

Abans de començar, indicar que l'aplicació utilitza el micròfon per recollir octets aleatoris. És per això que sería necesari tenir un micròfon connectat per a que l'aplicació funcioni de manera òptima. D'altra manera l'encriptació seria molt més dèbil.

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/FileEncoderApplication.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, exceptuant l'extensió .jfe) o desencriptar (arxiu amb extensió .jfe). Pots pulsar el botó "..." per obrir el diàlog 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.

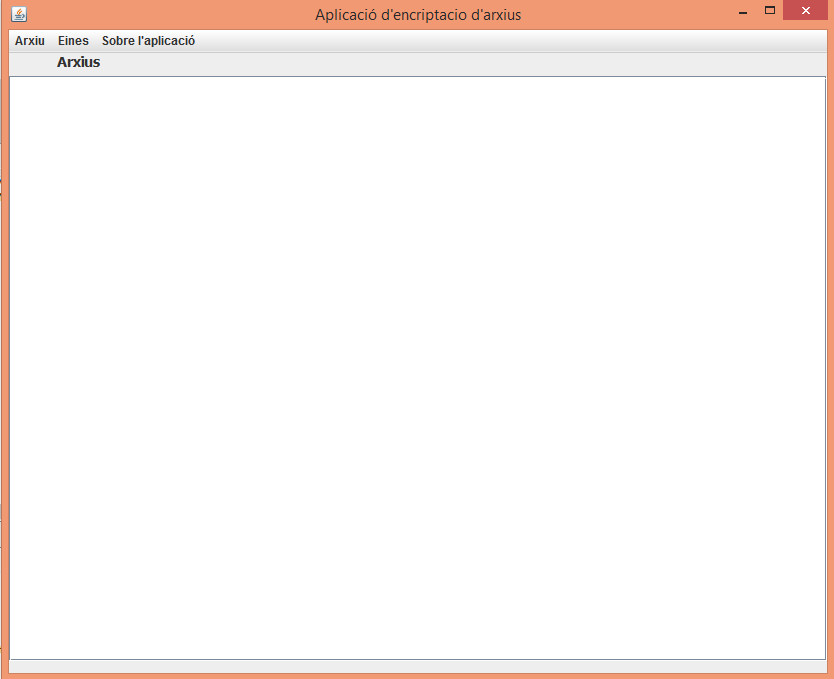
Després d'aquests passos, ja pots utilitzar els botons d'encriptar, desencriptar o obrir arxiu encriptat.

# Funcionament de l'aplicació

En aquest capítul es veurà como encriptar, desencriptar i obrir arxius encriptats 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.

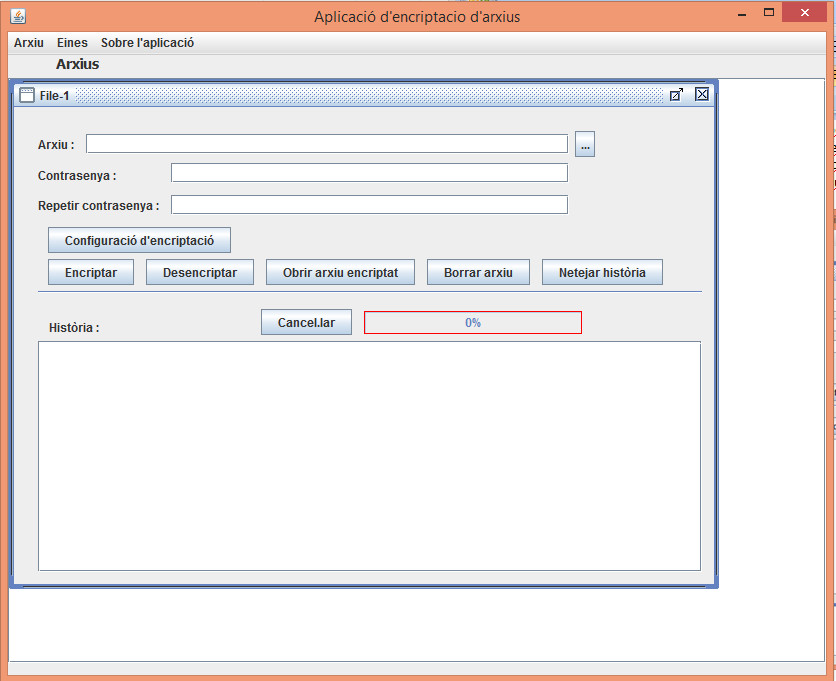
A l'àrea on seran les finestres dels arxius, existeix un menú emergent que apareix en prémer el botó dret sobre ella.

En aquest menú apareix una sola 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". En aquest quadre de text s'ha de possar el nom de l'arxiu sobre el que s'aplicaran les accions.

L'arxiu pot ser o be un arxiu sense encriptar (amb qualsevol extensió), o bé un arxiu encriptat (amb extensió .jfe).

Per omplir-lo 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 passar de treballar amb l'arxiu sense encriptat a treballar amb l'arxiu encriptat, afegint l'extensió .jfe o esborrant-la)
* "Contrasenya" i "Repetir contrasenya". En aquestos 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 después no es podria desencriptar l'arxiu.

Obviament 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.

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 predefinida al sistema per aquest tipus d'arxius.
* Modificar la "Configuració d'encriptació". Serveix per modificar els paràmetres d'encriptació. Veure punt: 3.6-Configuració d'encriptació
* "Borrar arxiu". Esborra l'arxiu.
* "Netejar història". Esborra la història del cuadre de text Història.
* "Cancel.lar". Cancel.la l'encriptació o desencriptació.

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 existeis 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 desde l'inici de l'acció.

## Menú Arxiu

El menú Arxiu té aquest aspecte:

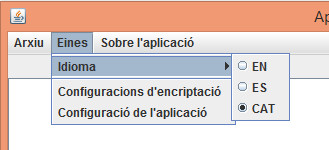


En aquest menú apareixen dues opcións:

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

## Menú Eines

El menú eines té el següent aspecte:



Aquest menú té tres opcions:

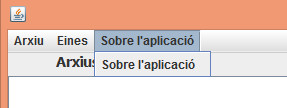
* Idioma. En obrir aquest submenú apareixen els idiomes disponibles. Serveix per a poder canviar l'idioma de l'aplicació.

Per defecte hi ha disponibles els següents idiomes:

* "EN". Anglès
* "ES". Castellanà
* "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 els tamanys d'arxiu a encriptar. Veure punt: 3.5-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: 3.7-Configuració de la aplicació

## Menú Sobre l'aplicació

El menú Sobre l'aplicació té el següent aspecte:



Aquest menú només té una opció:

* 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.

## 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 comantat 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: 3.6.1-Paràmetres de la configuració de encriptació

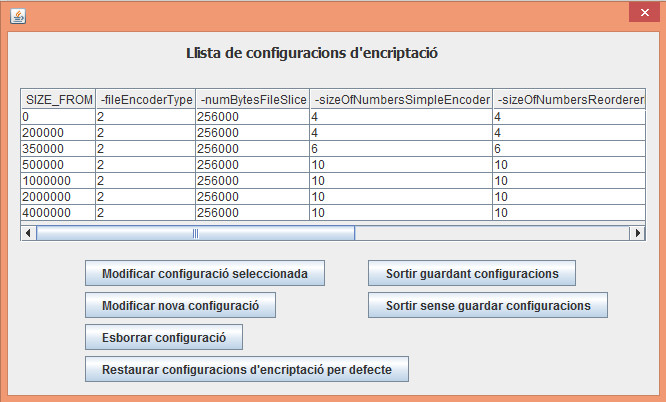
Donat que els paràmetres d'encriptació incideixen sobre tot en la velocitat de l'encriptació/desencriptació, sembla lògic pensar que en funció del tamany de l'arxiu hauria d'utilitzar-se una configuració d'encriptació o una altra.

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 tamany d'arxiu.

### El formulari

El formulari té el següent aspecte:



En aquest formulari existeix una taula resum de les configuracions d'encriptació ordenades per tamany 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 tamanys 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.

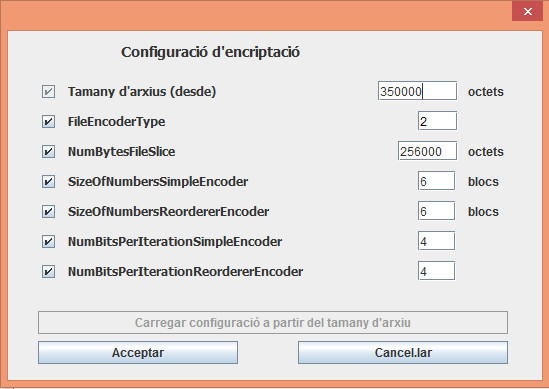
També existeixen una sèrie de botons que aporten la funcionalitat del formulari:

* 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: 3.6-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 tamanys d'arxiu als quals aplica aquesta configuració.
* Esborrar configuració. Esborra la configuració d'encriptació seleccionada de la taula.
* Restaurar configuracions d'encriptació per defecte. Elimina tots els canvis que s'hagin pogut fer sobre les configuracions d'encriptació per interval de tamany d'arxiu, deixant la llista de configuracions d'encriptació original (la que venia inicialment en l'aplicació).
* Sortir guardant configuracions. Permet sortir del formulari guardant els canvis realitzats en les configuracions d'encriptació.
* Sortir sense guardar configuracions. Permet sortir del formulari sense guardar ni aplicar els canvis realitzats en les configuracions d'encriptació per interval de tamany d'arxiu.

## 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 tamanys d'arxiu determinat.

El formulari té el següent aspecte:



A aquest formulari pot arrivar-se bé desde la finestra d'arxiu, vista al punt: 3.1-Pantalla principal bé des de el formulari de Llista de configuracions d'encriptació al punt: 3.5.2-El formulari.

Existeix un botó per a carregar els paràmetres per defecte en funció del tamany de l'arxiu. Aquest botó només estará 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 estará 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 següenst paràmetres:

* Tamany d'arxiu (des de). Aquest valor no és un paràmetre de configuració propiament 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 perque en aquest cas es pretén de crear o editar una configuració d'encriptació que aplicarà a un interval de tamanys d'arxiu. El tamany d'arxiu (des de) indicarà l'inici de l'interval de tamany d'arxiu en octets. El final de l'interval al que aplicarà la configuració d'aquest formulari, dependrà del paràmetre de tamany 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: 3.7-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 (obsolet). 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 (aconsellat). Aquest és el valor aconsellat per aquesta versió de l'aplicació.

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).

* NumBytesFileSlice. Aquest paràmetre de configuració d'encriptació indica el número d'octets de rodanxa 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, d'utilitza una memòria entre 40 i 100 cops més gran que la del tamany en octets que s'està encriptant. Per un arxiu de 100 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 rodanxes i per cada una d'aquestes rodanxes, primer es llegeixi el contingut de la rondanxa en un array d'octets, d'apliqui l'encriptació i s'escrigui a l'arxiu encriptat el contingut de la rodanxa encriptada. Per encriptar la següent roadnxa 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 rodanxa. 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.

* SizeOfNumbersSimpleEncoder. Aquest paràmetre de configuración d'encriptació aplica al tamany numèric aplicat al generador pseudoaleatori caòtic

Veure punt: 5.2-Algoritme d'encriptació

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

Les unitats d'aquest paràmetre són llleugeramet diferents pels FileEncoderType 1 i 2.

* Pel FileEncoderType 1, aquest paràmetre està expressat en octets.
* Pel FileEncoderType 2, 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 el 2.

* Pel FileEncoderType 1, aquest paràmetre està expressat en octets.
* Pel FileEncoderType 2, 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).

* 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 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 el 2 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 tamanys de número de 16 octets sí que podria utilitzarse el valor 4, pero millor a partir de tamanys de número de 32 octets.
* Pel FileEncoderType 2, 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 tamanys 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 el 2 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 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 tamanys de número de 16 octets sí que podria utilitzarse el valor 4, pero millor a partir de tamanys de número de 32 octets.
* Pel FileEncoderType 2, 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 tamanys de número (configurats a SizeOfNumbersReordererEncoder) més petits de 5 blocs. Millor encara a partir de 8 blocs.

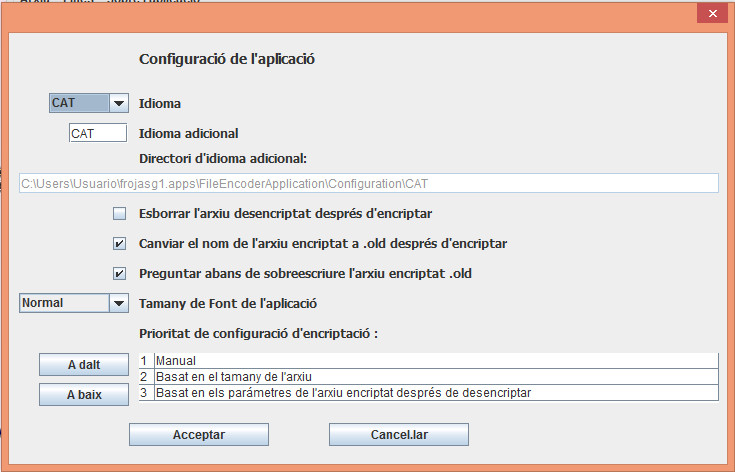
Per a valors més grans que 4 (múltiples de 8 fins a 64), el valor configurat ha de complir aquesta condició:

NumBitsPerIterationReordererEncoder <= 3 x SizeOfNumbersReordererEncoder

## Configuració de la aplicació

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

El formulari té el següent aspecte:



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

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

Els idiomes que es poden escollir son:

* EN. Anglès
* ES. Castellà
* L'idioma adicional que per defecte es CAT (català)
* Idioma adicional. És l'idioma adicional que apareix a l'hora de poder canviar d'idioma.

Si vols posar un idioma del que no existeixen els texts en l'aplicació, pots canviar l'idioma adicional al teu idioa i traduir 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 adicional".

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.

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

* 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, sino que s'esborra escribint 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 lúltim 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.
* Tamany de font de l'aplicació. Aquest paràmetre de configuració permet de canviar el tamany de font utilitzat a l'aplicació:

Hi ha dues opcions:

* Normal. En aquest cas les fonts que apareixen a la pantalla son les originals.
* Gran. En aquest cas les fonts que apareixen a la pantalla son 1,4 vegades més grans que les originals.
* 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 uqe es fes una modificació a una configuración d'encriptació i que s'acceptés, pero que aquesta configuració no fos aplicada quan es fa l'encriptació.

* (2) - Basat en el tamany 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 del tamany de l'arxiu. Veure punt: 3.5-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 order 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.

# Encriptació per la interfície d'ordres

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

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 uqe tinguis que teclejar la contrasenya i que aqueste es vegi a la teva pantalla, és per això que no és un sistema molt segur. No obstant es pot fer.

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

## 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.

## Paràmetres d'encriptació com a arguments

Dels scripts anteriors el principal és aquest:

command.interface.FileEncoder

Desde ell s'invoca a l'aplicació Java i com a paràmetres pren principalment els que ja s'han descrit al punt: 3.6.1-Paràmetres de la configuració de encriptació

Els paràmetres disponibles per a encriptar/desencriptar son aquests:

* -password Seguir per un argument amb la contrasenya.
* -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 una rodanxa. Es recomana utilitzar un valor alt per a aquest paràmetre. La memòria utilitzada per l'aplicació està limitat aproximadament per 100 cops el tamany de la rodanxa (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).

# 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.

**És per això que és important tenir el micròfon connectat,** per a poder obtenir octets per a formar la clau el més aleatoris possible.

Si el micròfon no està connectat, aquests octets aleatoris son obtinguts utilitzant la classe SecureRandom de Java, utilitzant com a mínim un octet gairebé aleatori com a llavor.

Això no és molt, es per això que és molt important tenir connectat el micrófon per a poder obtenir octets realment aleatoris.

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.

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

## Algoritme d'encriptació

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

* Encriptació de la rodanxa estil XOR. En aquesta parte de l'encriptació, generant bits pseudoaleatoris i fent un XOR amb les dades originals, s'obté una rodanxa encriptada i els octets d'aquesta rodanxa són bastant aleatoris.

Si deixessim aquí l'encriptació, sería 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 aplicacio (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 de la rodanxa. En aquesta part de l'encriptació, es generen posicions pseudoaleatòries, on es van movent un a un els octets de la rodanxa, reordenant el conjunt dels octets.

Per a obtenir els octets inicials de l'arxiu desencriptat, és necessari desencriptar una rodanxa complerta, això fa que es faci més difícil trencar l'encriptació, ja que és molt més costós en termes de temps de computació desencriptar una rodanxa complerta (que té tamany 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.

Cada un dels passos anteriors, per a realitzar la seva part de l'encriptació utilitzen 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 rodanxa 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 de la rodanxa hauria de ser com a mínim igual al tamany de l'arxiu a encriptar.

## Generador pseudoaleatori utilizat

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 trencarse fàcilment el sistema pseudoaleatori.

Les opcions que tenim són:

* Utilitzar la classe BigDecimal de Java (Utilitzat en el FileEncoderType=1, obsolet).
* Programar una classe nova que tracti números de precisió variable (Utilitzat en el FileEncoderType=2).

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 (FileEncoderType 1 i 2): 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 del tamany 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 tamany 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, pero amb tamanys de número de 16 bits, la diferència de probabilitat ja és negligible.
* Si s'utilitzen 4 bits per iteració, és millor utilitzar números de tamany superior o igual a 256 bits.

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Valor | números de 16 bits | números de 32 bits | números de 64 bits | números de 128 bits | números de 192 bits | números de 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 el tamany 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):

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, pero 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 el tamny 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.