

# JAES

## Cross-platform AES File Encryption tool

Versione Software 0.9.2

Versione Manuale 0.1

JAES è un tool cross platform per la cifratura/decifratura simmetrica di file tramite password con algoritmo AES a 256 bit.

Il software consiste in una GUI java che si interfaccia verso le librerie crittografiche “BouncyCastle”(c)<sup>1</sup>, delle quali sfrutta l'implementazione dell'algoritmo ”*PBEWithMD5And256BitAES-CBC-OpenSSL*” (in future versioni potrebbero essere resi disponibili anche altri algoritmi).

Scopo del progetto è fornire un tool per la protezione “da occhi indiscreti/non autorizzati” di documenti digitali, a proprio uso o per interscambio con altre parti, come ce ne sono già molti ma che a differenza di altri sia:

- estremamente semplice da usare anche per utenti inesperti
- utilizzabile indipendente dal tipo di sistema operativo
- facilmente installabile e distribuibile
- che offra un *adeguato livello di sicurezza limitatamente agli scopi prefissati*
- non proprietario
- di origine “trusted”.

JAES viene distribuito gratuitamente e senza alcuna garanzia né assunzione di responsabilità di alcun tipo: l'utilizzo del software da parte dell'utente finale implica pertanto l'accettazione da parte del medesimo della licenza di utilizzo riportata sia all'interno dell'applicativo che nel paragrafo 5 del presente manuale.

---

<sup>1</sup> [www.bouncycastle.org](http://www.bouncycastle.org)

# Manuale Utente

## Indice generale

1 .Prerequisiti di sistema.....	3
2 .Installazione e Avvio.....	3
2.1 .Windows.....	3
2.2 .Macintosh.....	3
2.3 .Unix (Solaris, Linux).....	4
3 .Cifratura/Decifratura di File.....	4
4 .Informazioni.....	6
5 .Licenza.....	7

## 1 . Prerequisiti di sistema

Prerequisito essenziale per il funzionamento del tool è l'installazione della **Sun JRE v. 1.4** o successive.

## 2 . Installazione e Avvio

### 2.1 . Windows

Per installare il tool JAES su sistema operativo Windows è necessario seguire i seguenti passi:

1. Decomprimere il file *jaes-win-0.9.2.zip* in una qualsiasi cartella del sistema in cui si vuole utilizzare JAES.
2. Aprire la cartella *jaes* creata, in cui si trovano i file:
  - *jaes.exe*
  - *jaes.jar*
  - *bcprov-jdk14-137.jar*.
3. Eseguire (doppio click) il file *jaes.exe*

#### Troubleshooting:

nel caso in cui non parta o dia errore il file *jaes.exe*, procedere come segue:

1. Aprire il prompt di comandi di Windows.
2. Posizionarsi nella cartella *jaes* (es. **cd c:\programmi\jaes**)
3. eseguire il comando **<java\_home>/bin/java -jar jaes.jar**

Il tool si apre ed è pronto per l'utilizzo.

### 2.2 . Mac OSX

Per installare il tool JAES su su sistema operativo Mac OSX è necessario seguire i seguenti passi:

1. Decomprimere il file *jaes-mac-0.9.2.zip* in una qualsiasi cartella del sistema in cui si vuole utilizzare JAES.
2. Eseguire (doppio click) il file *jaes*

Il tool si apre ed è già pronto per essere utilizzato.

## 2.3 . Unix (Solaris, Linux, ...)

Per installare il tool JAES su unix (solaris, linux, ..) è necessario seguire i seguenti passi:

1. Decomprimere il file *jaes-unix-0.9.2.tar.gz* in una qualsiasi cartella del sistema in cui si vuole utilizzare Jaes.
2. Eseguire il file *jaes.run*

Il tool si apre ed è già pronto per essere utilizzato.

## 3 . Cifratura/Decifratura di File

Appena avviato il tool appare sullo schermo la seguente finestra che contiene due schede:

- Main
- Info



Illustrazione 1: Jaes - Scheda Main

Descrizione immagine:

1. **Destination Folder:** campo non editabile. E' la cartella in cui viene salvato il file

criptato o decriptato, viene automaticamente valorizzato con il percorso del file di origine.

2. **Passphrase:** campo editabile da 2 a 16 caratteri di ogni tipologia (alfanumerici e caratteri speciali). In questo campo deve essere inserita la parola chiave da utilizzare per criptare/decriptare il file. Nel caso in cui si voglia criptare un file allora tale parola chiave dovrà essere ripetuta nel campo sottostante *Repeat Passphrase*. Nel caso in cui si voglia decriptare un file è sufficiente digitare solo nel campo *Passphrase* la parola chiave con cui il file è stato criptato.

3. **Shared Secret:** combobox che consentono di inserire una combinazione numerica e sequenziale necessaria alla decifratura del file. Se non si vuole usufruire di questa utility è sufficiente lasciare le combobox valorizzate a *01* come di default.

Lo Shared Secret è generalmente un valore concordato a priori tra le due parti che vogliono scambiarsi file cifrati, mentre la Passphrase viene concordata di volta in volta.

N.B.: Solo la stessa combinazione di Passphrase e Shared Secret usata in cifratura consentirà successivamente la corretta decifratura del file.

4. **File to Encrypt or Decrypt:** cliccando sul pulsante *Browse...* è possibile cercare nel proprio sistema e selezionare il file che si desidera criptare/decriptare. Dopo aver scelto il file il campo sovrastante viene valorizzato con il percorso scelto (path del file).

I file cifrati verranno creati con estensione “.jaes”.

N.B. In questo momento viene valorizzato anche il campo Destination Folder (vedere punto 1).

5. **Encrypt/Decrypt:** nel caso in cui si voglia criptare il file cliccare sul pulsante *Encrypt*, cliccare invece sul pulsante *Decrypt* nel caso contrario.

N.B.: è possibile decifrare solo file con estensione “.jaes”

**ATTENZIONE:** il processo di decifratura avverrà anche in caso si immetta una coppia Passphrase/Shared-secret errata, ma in tal caso il file di output non sarà utilizzabile. Tale comportamento è voluto ed assicura una sicurezza maggiore dell'applicativo.

6. **Progress:** barra di avanzamento automatico che informa in tempo reale sulla percentuale di avanzamento dell'operazione effettuata.

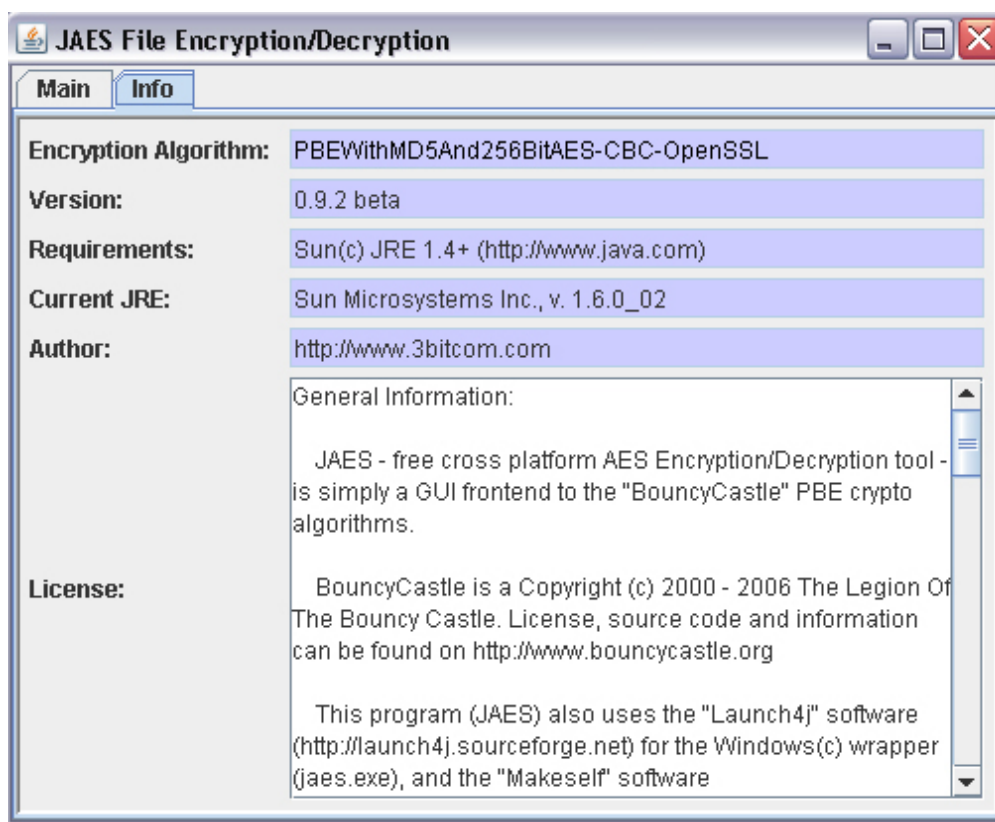


Illustrazione 2: Jaes - Scheda Info

Descrizione immagine:

la scheda Info fornisce le informazioni principali relative a:

- Algoritmo utilizzato per criptare i file
- Versione del tool
- Versione JRE necessaria come prerequisito
- Versione JRE correntemente utilizzata
- Autore del tool
- Licenza completa del tool.

## 4. Informazioni

Il tool JAES è reperibile sul sito [www.3bitcom.com](http://www.3bitcom.com) – area download, oppure facendone espressamente richiesta tramite e-mail all'indirizzo [info@3bitcom.com](mailto:info@3bitcom.com).

## 5 . Licenza

General Information:

JAES - free cross platform AES Encryption/Decryption tool - is simply a GUI frontend to the "BouncyCastle" PBE crypto algorithms.

BouncyCastle is a Copyright (c) 2000 - 2006 The Legion Of The Bouncy Castle. License, source code and information can be found on <http://www.bouncycastle.org>

This program (JAES) also uses the "Launch4j" software (<http://launch4j.sourceforge.net>) for the Windows(c) wrapper (jaes.exe), and the "Makeself" software (<http://freshmeat.net/projects/makeself>) for the Unix wrapper (jaes.run).

This program (JAES) is free software and you can freely redistribute it but without any modification if not previously authorized by the author.

This program (JAES) is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

SECURITY AND INTEGRITY OF YOUR DATA IS NOT GUARANTEED!

Disclaimer of Warranty:

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

THERE IS ALSO NO WARRANTY THAT COMPATIBILITY BETWEEN DIFFERENT VERSION OF THE PROGRAM WILL BE MAINTAINED: THIS MEANS THAT IF YOU ENCRYPT A FILE WITH JAES VERSION x.y YOU COULD NOT BE ABLE TO DECRYPT IT USING JAES VERSION k.z

KEEP ALWAYS A BACKUP OF YOUR UNENCRYPTED DATA IN A SECURE PLACE!

Limitation of Liability:

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.