

## **MULTIOBFUSCATOR v2.00 CRITTOGRAFIA & OFFUSCAMENTO**

Sicurezza avanzata di file & testo, semplice, sicura e gratuita  
*EmbeddedSW, 2013*

Inviate i vostri suggerimenti, commenti, segnalazioni, richieste  
a [embedded@embeddedsw.net](mailto:embedded@embeddedsw.net)

## **MULTIOBFUSCATOR HOMEPAGE**

### [NOTE LEGALI](#)

-  [CARATTERISTICHE: PERCHÈ QUESTO PROGRAMMA CRITTOGRAFICO È DIFFERENTE DAGLI ALTRI?](#)
-  [CARATTERISTICHE: ARCHITETTURA DEL PROGRAMMA](#)
-  [CARATTERISTICHE: MULTI CRITTOGRAFIA E OFFUSCAMENTO DATI](#)
-  [COSA È LA CRITTOGRAFIA NEGABILE?](#)

### [OPZIONI: LIVELLO DI RUMORE](#)

#### [SETUP DELLE PASSWORD SEMPLICE](#)

#### [SETUP DELLE PASSWORD MEDIO](#)

#### [SETUP DELLE PASSWORD AVANZATO – CIFRATURA](#)

#### [SETUP DELLE PASSWORD AVANZATO – DECIFRAZIONE](#)

 <b>SEMPLICE</b>	  
 <b>MEDIO</b>	  
 <b>ESPERTO</b>	  
 <b>ESPERTO</b>	  

[CIFRATURA FILE – SETUP DI BASE \(1 PASSWORD\)](#)

[DECIFRAZIONE FILE – SETUP DI BASE \(1 PASSWORD\)](#)

[CIFRATURA FILE – SETUP MEDIO \(4 PASSWORD\)](#)

[DECIFRAZIONE FILE – SETUP MEDIO \(4 PASSWORD\)](#)

[CIFRATURA FILE – SETUP AVANZATO \(4 PASSWORD+ESCA\)](#)

[DECIFRAZIONE FILE – SETUP AVANZATO \(4 PASSWORD+ESCA\)](#)

[RUMORE RANDOM COME ESCA \(FILE\)](#)

 <b>SEMPLICE</b>	  
 <b>MEDIO</b>	  
 <b>ESPERTO</b>	  
 <b>ESPERTO</b>	  

[CIFRATURA TESTO – SETUP DI BASE \(1 PASSWORD\)](#)

[DECIFRAZIONE TESTO – SETUP DI BASE \(1 PASSWORD\)](#)

[CIFRATURA TESTO – SETUP MEDIO \(4 PASSWORD\)](#)

[DECIFRAZIONE TESTO – SETUP MEDIO \(4 PASSWORD\)](#)

[CIFRATURA TESTO – SETUP AVANZATO \(4 PASSWORD+ESCA\)](#)

[DECIFRAZIONE TESTO – SETUP AVANZATO \(4 PASSWORD+ESCA\)](#)

[RUMORE RANDOM COME ESCA \(TESTO\)](#)



## NOTE LEGALI

Ricordate: questo programma non è stato scritto per uso illegale. L'uso di questo programma in violazione delle leggi del vostro paese è assolutamente proibito. L'autore declina qualsiasi responsabilità conseguente dall'uso improprio di questo programma.

Né codice né formati coperti da brevetto sono stati inseriti in questo programma.

### QUESTO È UN SOFTWARE FREEWARE

Questo software è rilasciato con licenza [CC BY-ND 3.0](#)

Siete liberi di copiare, distribuire, modificare e fare uso commerciale di questo software alle seguenti condizioni:

- Dovete citare l'autore (e detentore del copyright): [EmbeddedSW](#)
- Dovete fornire un link alla Homepage dell'autore: [EMBEDDEDSW.NET](#)

[INDIETRO](#)



## Caratteristiche: perchè questo programma crittografico è differente dagli altri?

MultiObfuscator è un programma professionale di crittografia, con caratteristiche uniche che non troverete in nessun'altro programma gratuito o commerciale. MultiObfuscator è 100% gratuito e adatto alla memorizzazione e trasmissione di dati altamente sensibili.

Una panoramica delle sue caratteristiche

- [LIVELLI DI SICUREZZA]

I dati sono crittografati (1), sottoposti a scrambling (2) e a whitening (3).

[CARATTERISTICHE: ARCHITETTURA DEL PROGRAMMA](#)

- [LIVELLO 1 - MULTI CRITTOGRAFIA MODERNA]

Un insieme di 16 algoritmi di crittografia a 256bit, moderni e open-source è stato unito per formare un algoritmo di multi crittografia a doppia password (256bit+256bit).

- [LIVELLO 2 - SCRAMBLING BASATO SU CSPRNG]

I dati crittografati sono sempre sottoposti a scrambling per spezzare qualsiasi struttura residua dello stream. Viene inizializzato un nuovo generatore di numeri pseudo-casuali crittograficamente sicuro (CSPRNG) con una terza password (256bit) e i dati vengono mischiati globalmente con indici random.

- [LIVELLO 3 - WHITENING BASATO SU CSPRNG]

I dati sottoposti a scrambling sono sempre mischiati ad una grande quantità di rumore. Viene inizializzato un nuovo CSPRNG con una quarta password (256bit) e i dati vengono frammentati bit-a-bit secondo una permutazione random.

- [SICUREZZA EXTRA - CRITTOGRAFIA NEGABILE]

I dati altamente sensibili possono essere protetti usando dei dati meno sensibili come esca.

[COSA È LA CRITTOGRAFIA NEGABILE?](#)

- [CODICE SORGENTE]

Questo programma può essere considerato come una semplice GUI per Windows della libreria [LIBOBFUSCATE](#), indipendente dal sistema e open-source. Gli utenti e gli sviluppatori sono assolutamente liberi di utilizzare la libreria di base (100% del codice di crittografia e offuscamento), leggerla e modificarla.

*Siete gentilmente pregati di inviarmi i porting/upgrade/personalizzazioni/sw derivati di libObfuscate, per analizzarli e aggiungerli alla homepage del progetto. Un repository ufficiale, centrale e aggiornato eviterà dispersione e irraggiungibilità del codice derivato dal progetto.*

[INDIETRO](#)



## CARATTERISTICHE: ARCHITETTURA DEL PROGRAMMA

MultiObfuscator implementa la multi crittografia (un tipo avanzato di [CRITTOGRAFIA PROBABILISTICA](#)) unendo 16 moderni algoritmi crittografici a blocchi open-source, scelti fra [AES-PROCESS](#), [NESSIE-PROCESS](#) e [CRYPTREC-PROCESS](#). Il Cypher-Block-Chaining (CBC) ha il ruolo di wrapper per questi algoritmi a blocchi, permettendo loro di comportarsi come algoritmi a stream.

Il whitening è il nucleo della [CRITTOGRAFIA NEGABILE](#)

- MultiObfuscator supporta dati e un'esca (un primo livello di crittografia negabile)
- MultiObfuscator non può, per costruzione, ricostruire l'associazione *Dati*  $\leftrightarrow$  *Offset* e, al momento della decifrazione, deve indovinarla lentamente, per tentativi

[COSA È LA CRITTOGRAFIA NEGABILE?](#)

Le ultime versioni di OpenPuff/MultiObfuscator condividono alcune caratteristiche uniche con il progetto [RUBBERHOSE FILESYSTEM](#) (1997-2000). Un'evoluzione indipendente e convergente ha condotto autori diversi a concentrare gli sforzi verso un obiettivo comune: la [NEGABILITÀ PLAUSIBILE](#).

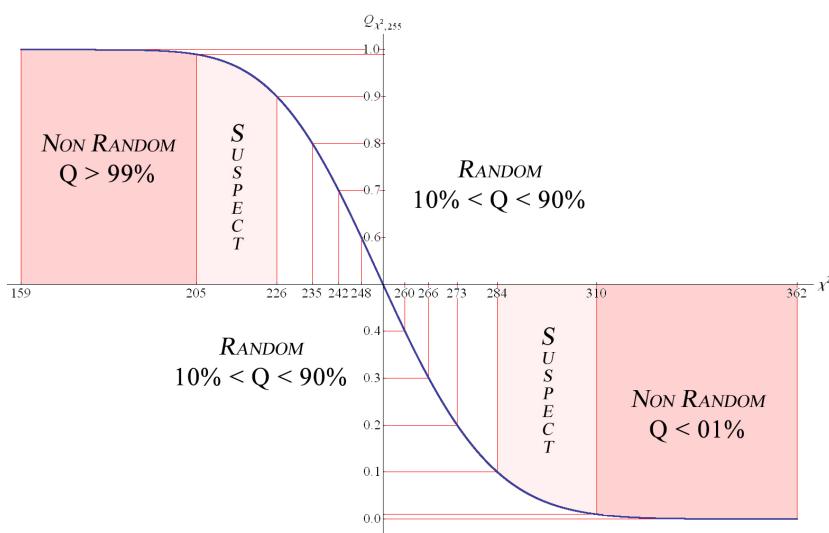
Rubberhose è *stato* (a causa dell'abbandono) un progetto avanzato che ha introdotto nuovi concetti

- aspetti: gli utenti forniscono passwords diverse e ottengono, dallo stesso contenitore, dati diversi
- negabilità plausibile: l'estrema difesa contro la coercizione legale e fisica

Gli anni sono trascorsi e, sfortunatamente, gli attaccanti moderni non sarebbero più ingannati da un offuscamento di solo whitening. Le [BATTERIE DI TEST STATISTICI](#) per i generatori di numeri random ([NIST](#), [DIEHARD](#), [ENT](#)) scoprirebbero facilmente la [DEGRADAZIONE DI RANDOMICITÀ](#) del vostro contenitore e, per relazione diretta, l'ammontare di dati che sono stati nascosti all'interno.

MultiObfuscator implementa un auto-aggiustamento basato sulla [DISTRIBUZIONE- \$\chi^2\$](#) :

- eccede la [DISTRIBUZIONE- \$\chi^2\$](#)  il 50% delle volte ( $Q = 0.5$ ), come un vera sequenza random creata da [EVENTI DI DECADIMENTO RADIAZIONE](#)
- ottiene un punteggio  $\geq 98\%$  nel sistema NIST di misura della randomicità



[INDIETRO](#)



## CARATTERISTICHE: MULTI CRITTOGRAFIA E OFFUSCAMENTO DATI

### **FAQ 1: Perché non è stata implementata una crittografia standard AES-256 or RSA-1024?**

La moderna crittografia open-source

- è stata studiata approfonditamente e analizzata dalla comunità scientifica
- è largamente accettata come lo strumento più sicuro per proteggere i dati
- soddisfa praticamente ogni necessità *standard* di sicurezza

MultiObfuscator non appoggia nessuna [TEORIA DELLA COSPIRAZIONE](#) contro la nostra privacy ([BACKDOOR SEGRETE](#), design crittografici intenzionalmente deboli, ...). Non c'è nessuna ragione per non avere fiducia nella moderna crittografia pubblicamente disponibile (sebbene qualche vecchio cifrario sia già stato [VIOLATO](#)).

Alcuni utilizzatori, comunque, molto probabilmente nascondono dati molto sensibili, con una necessità *insolitamente alta* di sicurezza. I loro segreti hanno bisogno di subire un approfondito processo di [OFFUSCAMENTO](#) dei dati per poter sopravvivere *più a lungo* alle indagini forensi e agli attacchi brute-force potenziati da hardware specializzato.

### **FAQ 2: La multi crittografia è simile alla cifratura multipla?**

La multi crittografia è qualcosa di molto diverso dalla [CIFRATURA MULTIPLA](#) (crittografare più di una volta). Non ci sono opinioni largamente condivise riguardo all'affidabilità della cifratura multipla. Si pensa che sia:

- [MIGLIORE](#) della cifratura singola
- [DEBOLE](#) come il cifrario più debole della coda/processo di crittografia
- [peggiore](#) della cifratura singola

MultiObfuscator appoggia l'ultima tesi (peggiore) e non crittografa mai dati già crittografati.

### **FAQ 3: La multi crittografia è simile alla crittografia random/polimorfica?**

La crittografia random, alias. [CRITTOGRAFIA POLIMORFICA](#), è una ben nota [CRITTOGRAFIA FRAUDOLENTA](#). La multi crittografia è qualcosa di molto diverso e non aspira mai a costruire cifrari migliori, random o generati dinamicamente.

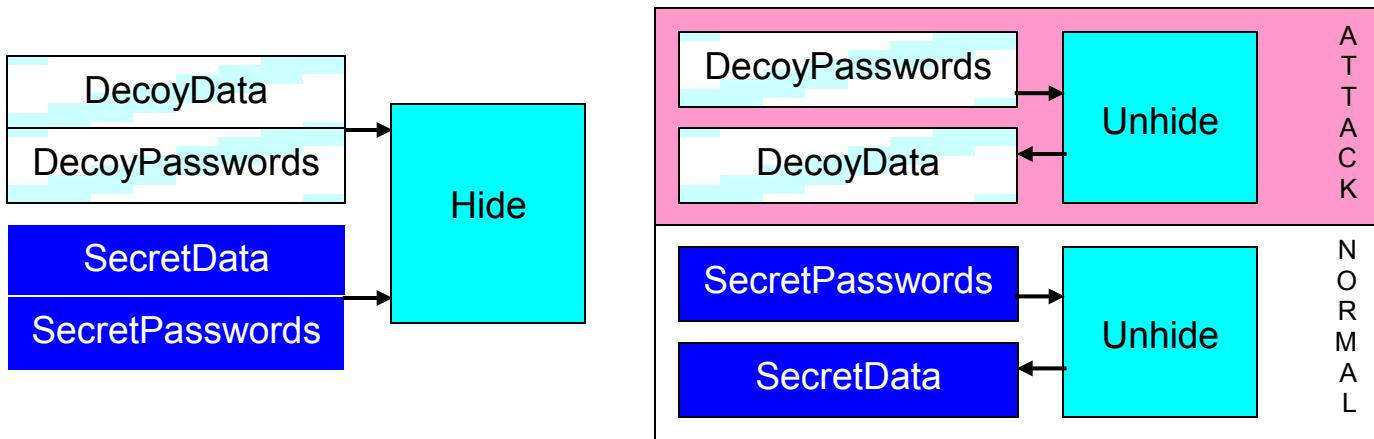
MultiObfuscator si basa unicamente sulla moderna crittografia stabile e open-source.

## [CARATTERISTICHE: ARCHITETTURA DEL PROGRAMMA](#)

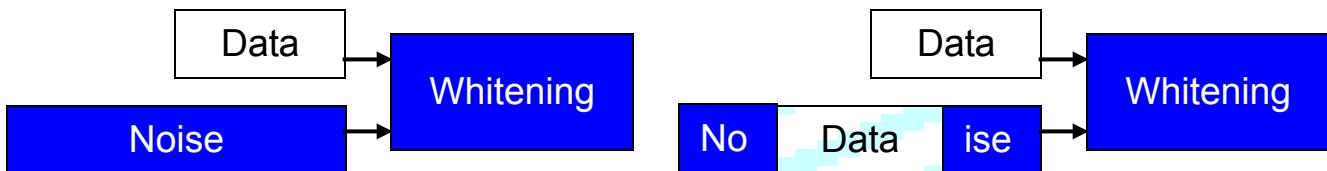
[INDIETRO](#)

## COSA È LA CRITTOGRAFIA NEGABILE?

La **CRITTORGRAFIA NEGABILE**, è una tecnica basata sull'uso di un'esca che permette di negare in maniera convincente di stare nascondendo dati sensibili, anche se gli attaccanti possono dimostrare che si sta nascondendo qualcosa. Basta semplicemente fornire un'esca sacrificabile che **plausibilmente** deve rimanere confidenziale. Verrà rivelata all'attaccante, sostenendo che questa è l'unico contenuto.



Come è possibile? I dati crittografati e sottoposti a scrambling, sono sottoposti a whitening ([CARATTERISTICHE: ARCHITETTURA DEL PROGRAMMA](#)) con una grande quantità di rumore. I dati esca possono sostituire un po' del rumore senza compromettere le proprietà finali di [RESISTENZA ALLA CRITTANALISI](#).

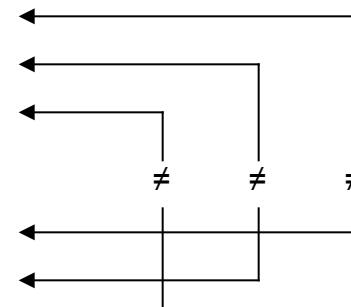


I dati sensibili e i dati esca sono crittografati usando password differenti. Si devono selezionare due diversi insiemi di diverse password.

## Esempio:

Sensible data:      Password (A)      “*FirstDataPssw1*”  
                        Password (B)      “*SecondDataPssw2*”  
                        Password (C)      “*AnotherDataPssw3*”  
 $(A \cap B) 70\%, (A \cap C) 67\%, (B \cap C) 68\%, \text{HAMMING DISTANCE} \geq 25\%$

Decoy data:      Password (A')      "FirstDecoyPssw1"  
                   Password (B')      "SecondDecoyPssw2"  
                   Password (C')      "AnotherDecoyPssw3"  
 $(A' \cap B') 72\%, (A' \cap C') 60\%, (B' \cap C') 70\%, \text{HAMMING DISTANCE} \geq 25\%$



Le password devono essere diverse (a livello di bit) e lunghe almeno 8 caratteri.

Esempio: "DataPssw1" (A) "DataPssw2" (B) "DataPssw3" (C)

(A) 01000100 01100001 01110100 01100001 01010000 01110011 01110011 01110111 00110001  
(B) 01000100 01100001 01110100 01100001 01010000 01110011 01110011 01110111 00110010  
(C) 01000100 01100001 01110100 01100001 01010000 01110011 01110011 01110111 00110011

(A ∩ B) 98%, (A ∩ C) 99%, (B ∩ C) 99%, HAMMING DISTANCE < 25% KO

Esempio: "FirstDataPssw1" (A) "SecondDataPssw2" (B) "AnotherDataPssw3" (C)

(A) 01000110 01101001 01110010 01110011 01110100 01000100 01100001 01110100 01100001 ...  
(B) 01010011 01100101 01100011 01101111 01101110 01100100 01000100 01100001 01110100 ...  
(C) 01000001 01101110 01101111 01110100 01101000 01100101 01110010 01000100 01100001 ...

(A ∩ B) 70%, (A ∩ C) 67%, (B ∩ C) 68%, HAMMING DISTANCE ≥ 25% OK

Verranno richiesti

- due **diversi** insiemi di diverse password
  - un file di dati sensibili
  - un file di dati esca **compatibile** (per dimensione) con i dati sensibili
- $$\sum_{k \in \{1, N-1\}} \text{used\_bytes}(\text{whiteBlock}_k) < \text{Sizeof}(\text{Decoy}) \leq \sum_{k \in \{1, N\}} \text{used\_bytes}(\text{whiteBlock}_k)$$

Esempio:

whiteBlocks	Data bytes	SensitiveData	DecoyData
+Block (1/N)	32	32	Used
...	2016	2016	Used
+Block (N-1/N)	32	32	Used
+Block (N/N)	32	15	1 – 32
	Total = 2112	Total = 2095	2080 < Size ≤ 2112

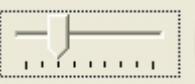
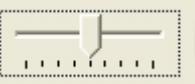
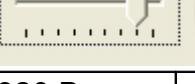
[INDIETRO](#)



## OPZIONI: LIVELLO DI RUMORE

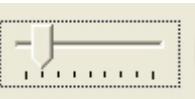
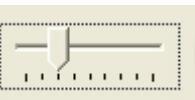
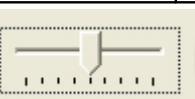
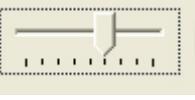
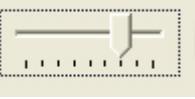
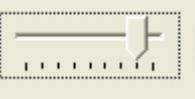
### Modalità file:

- **Formato:** file raw binario
- **Blocco di dimensione costante:** Noise + Data = 960 byte
- **Dimensione dell'output protetto:**  $((\text{size} + 256) / \text{Data}) * 960 \leq 256 \text{ Mb}$

Noise Level	Noise	Data	Min. Plain → Locked Size	Max. Plain → Locked Size
300%	720	<b>240</b>	1 B → 1920 B	64 Mb → 256 Mb
		Whitening 300%: 720 noise / 240 data	  	
400%	768	<b>192</b>	1 B → 1920 B	51 Mb → 256 Mb
		Whitening 400%: 768 noise / 192 data	  	
500%	800	<b>160</b>	1 B → 1920 B	42 Mb → 256 Mb
		Whitening 500%: 800 noise / 160 data	  	
900%	864	<b>96</b>	1 B → 2880 B	25 Mb → 256 Mb
		Whitening 900%: 864 noise / 96 data	  	
1100%	880	<b>80</b>	1 B → 3840 B	21 Mb → 256 Mb
		Whitening 1100%: 880 noise / 80 data	  	
1400%	896	<b>64</b>	1 B → 4800 B	17 Mb → 256 Mb
		Whitening 1400%: 896 noise / 64 data	  	
1900%	912	<b>48</b>	1 B → 5760 B	12 Mb → 256 Mb
		Whitening 1900%: 912 noise / 48 data	  	
2900%	928	<b>32</b>	1 B → 8640 B	8 Mb → 256 Mb
		Whitening 2900%: 928 noise / 32 data	  	
5900%	944	<b>16</b>	1 B → 16320 B	4 Mb → 256 Mb
		Whitening 5900%: 944 noise / 16 data	  	

## Modalità testo:

- **Formato:** testo/email
- **Blocco di dimensione costante:** Noise + Data = 960 byte → codifica a 6 bit → 1280 byte
- **Dimensione dell'output protetto:** ((size + 256) / Data) \* 1280 ≤ 256 Kb

Noise Level	Noise	Data	Min. Plain → Locked Size	Max. Plain → Locked Size
300%	720	<b>240</b>	1 B → 2560 B	46 Kb → 256 Kb
		Whitening 300%: 720 noise / 240 data	  	
400%	768	<b>192</b>	1 B → 2560 B	36 Kb → 256 Kb
		Whitening 400%: 768 noise / 192 data	  	
500%	800	<b>160</b>	1 B → 2560 B	30 Kb → 256 Kb
		Whitening 500%: 800 noise / 160 data	  	
900%	864	<b>96</b>	1 B → 3840 B	18 Kb → 256 Kb
		Whitening 900%: 864 noise / 96 data	  	
1100%	880	<b>80</b>	1 B → 5120 B	15 Kb → 256 Kb
		Whitening 1100%: 880 noise / 80 data	  	
1400%	896	<b>64</b>	1 B → 6400 B	12 Kb → 256 Kb
		Whitening 1400%: 896 noise / 64 data	  	
1900%	912	<b>48</b>	1 B → 7680 B	9 Kb → 256 Kb
		Whitening 1900%: 912 noise / 48 data	  	
2900%	928	<b>32</b>	1 B → 11520 B	6 Kb → 256 Kb
		Whitening 2900%: 928 noise / 32 data	  	
5900%	944	<b>16</b>	1 B → 21760 B	3 Kb → 256 Kb
		Whitening 5900%: 944 noise / 16 data	  	

[INDIETRO](#)



## SETUP DELLE PASSWORD SEMPLICE



### CIFRATURA/DEFICRAZIONE FILE/TESTO – SETUP DI BASE (1 PASSWORD)

<p>Insert main passwords (Min: 8, Max: 32)</p> <p>(A) Cryptography <input type="text" value="xxxxxxxx"/> <input checked="" type="checkbox"/> Enable (B)</p> <p>(B) Cryptography <input type="text"/> <input type="checkbox"/> Enable (C)</p> <p>(C) Scrambling <input type="text"/> <input type="checkbox"/> Enable (D)</p> <p>Passwords Check <span style="background-color: green; color: white; padding: 2px;">A = B = C = D</span></p> <p><math>H(X, Y) = \text{Hamming distance}(\text{Passw } X, \text{Passw } Y) \geq 25\%</math></p> <p>(D) Whitening <input type="text"/> <input type="checkbox"/> Enable (D)</p>	<p>Insert decoy passwords (Min: 8, Max: 32)</p> <p><input type="checkbox"/> Decoy Enable!</p> <p>(A) Cryptography <input type="text"/> <input type="checkbox"/> Enable (B)</p> <p>(B) Cryptography <input type="text"/> <input checked="" type="checkbox"/> Enable (C)</p> <p>(C) Scrambling <input type="text"/> <input checked="" type="checkbox"/> Enable (D)</p> <p>Passwords Check <span style="background-color: green; color: white; padding: 2px;">Disabled</span></p> <p><math>H(X, Y) = \text{Hamming distance}(\text{Passw } X, \text{Passw } Y) \geq 25\%</math></p>
(I)	(II)

(I) (Cryptography A)	La prima password
(Enable B)	Abilita/disabilita la seconda password
(Enable C)	Abilita/disabilita la terza password
(Enable D)	Abilita/disabilita la quarta password
(II) (Decoy Enable!)	Abilita/disabilita l'esca

- A) Disabilitare l'esca
- B.1) Disabilitare le password (Main\_B / Main\_C / Main\_D)
- B.2) Inserire una password (Main\_A) qualsiasi

*Le password (Main\_B / Main\_C / Main\_D) disabilitate diventeranno uguali alla password (Main\_A)!*

#### Vincoli:

- 1) Length (Main\_A)  $\geq 8$

#### Esempio:

A = B = C = D

Main: ok

Main\_A = “any password”

[INDIETRO](#)



## **SETUP DELLE PASSWORD MEDIO**



CIFRATURA/DECIFRAZIONE FILE/TESTO – SETUP MEDIO (4 PASSWORD)

Insert main passwords (Min: 8, Max: 32)	
(A) Cryptography	<input type="text" value="xxxxxxxx"/>
(B) Cryptography	<input type="text" value="xxxxxxxxxx"/>
(C) Scrambling	<input type="text" value="xxxxxx"/>
Passwords Check	
$H(A, B) H(A, C) H(B, C) = \{ 32\%, 38\%, 43\% \}$	
$H(X, Y) = \text{Hamming distance}(\text{Passw } X, \text{Passw } Y) \geq 25\%$	
(D) Whitening	<input type="text" value="xxxxxx"/>
<input checked="" type="checkbox"/> Enable (D)	

Insert decoy passwords (Min: 8, Max: 32)	
<input type="checkbox"/> Decoy Enabled	
(A) Cryptography	<input type="text"/>
(B) Cryptography	<input type="text"/>
(C) Scrambling	<input type="text"/>
Passwords Check	
Disabled	
$H(X, Y) = \text{Hamming distance}(\text{Passw } X, \text{Passw } Y) \geq 25\%$	

(I)	<i>(Cryptography A)</i>	La prima password (chiavi crittografiche)
	<i>(Cryptography B)</i>	La seconda password (CSPRNG crittografico)
	<i>(Scrambling C)</i>	La terza password (CSPRNG scrambling)
	<i>(Whitening D)</i>	La quarta password (CSPRNG whitening)
	<i>(Enable B)</i>	Abilita/disabilita la seconda password
	<i>(Enable C)</i>	Abilita/disabilita la terza password
	<i>(Enable D)</i>	Abilita/disabilita la quarta password
(II)	<i>(Decoy Enable!)</i>	Abilita/disabilita l'esca

- A) Disabilitare l'esca
  - B.1) Abilitare tutte o solo qualcuna delle password opzionali (Main\_B / Main\_C / Main\_D)
  - B.2) Inserire password (Main\_A / Main\_B / Main\_C) differenti
  - B.3) Inserire una password (Main\_D) qualsiasi

*Le password (Main\_B / Main\_C / Main\_D) disabilitate diventeranno uguali alla password (Main\_A)!*

## Vincoli:

- |      |                            |   |
|------|----------------------------|---|
| 1.1) |                            | Length (Main_A) $\geq$ 8  |
| 1.2) | Enabled? (Main_B)          | $\rightarrow$ Length (Main_B) $\geq$ 8                                      |
| 1.3) | Enabled? (Main_C)          | $\rightarrow$ Length (Main_C) $\geq$ 8                                      |
| 1.4) | Enabled? (Main_D)          | $\rightarrow$ Length (Main_D) $\geq$ 8                                      |
| 2.1) | Enabled? (Main_B)          | $\rightarrow$ <a href="#">HAMMING DISTANCE</a> (Main_A / Main_B) $\geq$ 25% |
| 2.2) | Enabled? (Main_C)          | $\rightarrow$ <a href="#">HAMMING DISTANCE</a> (Main_A / Main_C) $\geq$ 25% |
| 2.3) | Enabled? (Main_B / Main_C) | $\rightarrow$ <a href="#">HAMMING DISTANCE</a> (Main_B / Main_C) $\geq$ 25% |

## Esempio:

H(A, B ) H(A, C ) H( B, C ) = { 2%, 38%, 38% }

Main: Main\_A è troppo simile a Main\_B

Main\_A = “**some\_crypt\_a**”

Main\_B = “**some\_crypt\_b**”

Main\_C = “scramble\_c”

Main\_D = “whiten\_d”

H(A, B ) H(A, C ) H( B, C ) = { 32%, 1%, 33% }

Main: Main\_A è troppo simile a Main\_C

Main\_A = “**some\_crypt\_a**”

Main\_B = “another\_crypt\_b”

Main\_C = “**some\_crypt\_c**”

Main\_D = “whiten\_d”

H(A, B ) H(A, C ) H( B, C ) = { 32%, 33%, 0% }

Main: Main\_B è troppo simile a Main\_C

Main\_A = “some\_crypt\_a”

Main\_B = “**another\_crypt\_b**”

Main\_C = “**another\_crypt\_c**”

Main\_D = “whiten\_d”

H(A, B ) H(A, C ) H( B, C ) = { 32%, 38%, 43% }

Main: ok

Main\_A = “some\_crypt\_a”

Main\_B = “another\_crypt\_b”

Main\_C = “scramble\_c”

Main\_D = “whiten\_d”

[INDIETRO](#)



## **SETUP DELLE PASSWORD AVANZATO – CIFRATURA**



CIFRATURA FILE/TESTO – SETUP AVANZATO (4 PASSWORD+ESCA)

Insert main passwords (Min: 8, Max: 32)	
( A ) Cryptography	xxxxxxxx
( B ) Cryptography	xxxxxxxxxx
( C ) Scrambling	xxxxxx
Passwords Check	$H(A, B)H(A, C)H(B, C) = \{32\%, 38\%, 43\%\}$
H(X, Y) = Hamming distance( Passw X, Passw Y ) >= 25%	
( D ) Whitening	xxxxxx
	<input checked="" type="checkbox"/> Enable ( D )
Insert decoy passwords (Min: 8, Max: 32)	
	<input checked="" type="checkbox"/> Decoy Enable
( A ) Cryptography	xxxxxxxx
( B ) Cryptography	xxxxxx
( C ) Scrambling	xxxxxx
Passwords Check	$H(A, B)H(A, C)H(B, C) = \{35\%, 39\%, 34\%\}$
H(X, Y) = Hamming distance( Passw X, Passw Y ) >= 25%	

(I)	<i>(Cryptography A)</i>	La prima password (chiavi crittografiche)
	<i>(Cryptography B)</i>	La seconda password (CSPRNG crittografico)
	<i>(Scrambling C)</i>	La terza password (CSPRNG scrambling)
	<i>(Whitening D)</i>	La quarta password (CSPRNG whitening)
	<i>(Enable B)</i>	Abilita/disabilita la seconda password
	<i>(Enable C)</i>	Abilita/disabilita la terza password
	<i>(Enable D)</i>	Abilita/disabilita la quarta password
(II)	<i>(Decoy Enable!)</i>	Abilita/disabilita l'esca
	<i>(Cryptography A)</i>	La prima password esca
	<i>(Cryptography B)</i>	La seconda password esca
	<i>(Scrambling C)</i>	La terza password esca
	<i>(Enable B)</i>	Abilita/disabilita la seconda password esca
	<i>(Enable C)</i>	Abilita/disabilita la terza password esca

#### A) Disabilitare l'esca

- B.1) Abilitare tutte o solo qualcuna delle password opzionali (Main\_B / Main\_C / Main\_D)
  - B.2) Inserire password (Main\_A / Main\_B / Main\_C) differenti
  - B.3) Inserire una password (Main\_D) qualsiasi

*Le password (Main\_B / Main\_C / Main\_D) disabilitate diventeranno uguali alla password (Main\_A)!*

### C) Abilitare l'esca

- D.1) Abilitare tutte o solo qualcuna delle password opzionali (Decoy\_B / Decoy\_C)
  - D.2) Inserire password (Decoy\_A / Decoy\_B / Decoy\_C) differenti

*Le password (Decoy B / Decoy C) disabilitate diventeranno uguali alla password (Decoy A)!*

## Vincoli:

1.1)	Length (Main_A) $\geq 8$
1.2) Enabled? (Main_B)	$\rightarrow$ Length (Main_B) $\geq 8$
1.3) Enabled? (Main_C)	$\rightarrow$ Length (Main_C) $\geq 8$
1.4) Enabled? (Main_D)	$\rightarrow$ Length (Main_D) $\geq 8$
2.1) Enabled? (Main_B)	$\rightarrow$ <a href="#">HAMMING DISTANCE</a> (Main_A / Main_B) $\geq 25\%$
2.2) Enabled? (Main_C)	$\rightarrow$ <a href="#">HAMMING DISTANCE</a> (Main_A / Main_C) $\geq 25\%$
2.3) Enabled? (Main_B / Main_C)	$\rightarrow$ <a href="#">HAMMING DISTANCE</a> (Main_B / Main_C) $\geq 25\%$
3.1)	Length (Decoy_A) $\geq 8$
3.2) Enabled? (Decoy_B)	$\rightarrow$ Length (Decoy_B) $\geq 8$
3.3) Enabled? (Decoy_C)	$\rightarrow$ Length (Decoy_C) $\geq 8$
4.1) Enabled? (Decoy_B)	$\rightarrow$ <a href="#">HAMMING DISTANCE</a> (Decoy_A / Decoy_B) $\geq 25\%$
4.2) Enabled? (Decoy_C)	$\rightarrow$ <a href="#">HAMMING DISTANCE</a> (Decoy_A / Decoy_C) $\geq 25\%$
4.3) Enabled? (Decoy_B / Decoy_C)	$\rightarrow$ <a href="#">HAMMING DISTANCE</a> (Decoy_B / Decoy_C) $\geq 25\%$
5.1) Enabled? (Decoy_B)	$\rightarrow$ Enabled? (Main_B) $\rightarrow$ Main_B $\neq$ Decoy_B
5.2) Enabled? (Decoy_B)	$\rightarrow$ Disabled? (Main_B) $\rightarrow$ Main_A $\neq$ Decoy_B
5.3) Enabled? (Decoy_C)	$\rightarrow$ Enabled? (Main_C) $\rightarrow$ Main_C $\neq$ Decoy_C
5.4) Enabled? (Decoy_C)	$\rightarrow$ Disabled? (Main_C) $\rightarrow$ Main_A $\neq$ Decoy_C

## Esempio:

$H(A, B)H(A, C)H(B, C) = \{32\%, 38\%, 43\%\}$	<i>Main: ok</i>
Password(A)(B)(C) same as Main Setup	<i>Decoy: Main_A = Decoy_A, ...</i>
Main_A = "some_crypt_a" Main_B = "another_crypt_b" Main_C = "scramble_c" Main_D = "whiten_d"	Decoy_A = " <b>some_crypt_a</b> " Decoy_B = " <b>another_crypt_b</b> " Decoy_C = " <b>scramble_c</b> "
$H(A, B)H(A, C)H(B, C) = \{32\%, 38\%, 43\%\}$	<i>Main: ok</i>
$H(A, B)H(A, C)H(B, C) = \{35\%, 39\%, 34\%\}$	<i>Decoy: Main_A = Decoy_A, ...</i>
Main_A = "some_crypt_a" Main_B = "another_crypt_b" Main_C = "scramble_c" Main_D = "whiten_d"	Decoy_A = "12345678" Decoy_B = "qwertyui" Decoy_C = "zxcvbnm,"



## SETUP DELLE PASSWORD AVANZATO – DECIFRAZIONE



### DECIFRAZIONE FILE/TESTO – SETUP AVANZATO (4 PASSWORD+ESCA)

Insert main passwords (Min: 8, Max: 32)

(A) Cryptography	xxxxxxxxxx
(B) Cryptography	xxxxxxxxxxxx
(C) Scrambling	xxxxxxxx
Passwords Check	
H(A, B) H(A, C) H(B, C) = { 32%, 38%, 43% }	
H(X, Y) = Hamming distance( PasswX, PasswY ) >= 25%	
(D) Whitening	xxxxxx

(I)

Insert decoy passwords (Min: 8, Max: 32)

<input type="checkbox"/> Decoy Enable!	
(A) Cryptography	
(B) Cryptography	
(C) Scrambling	
Passwords Check	
Disabled	
H(X, Y) = Hamming distance( PasswX, PasswY ) >= 25%	

(II)

(I)	( <i>Cryptography A</i> )	La prima password (chiavi crittografiche)
	( <i>Cryptography B</i> )	La seconda password (CSPRNG crittografico)
	( <i>Scrambling C</i> )	La terza password (CSPRNG scrambling)
	( <i>Whitening D</i> )	La quarta password (CSPRNG whitening)
	( <i>Enable B</i> )	Abilita/disabilita la seconda password
	( <i>Enable C</i> )	Abilita/disabilita la terza password
	( <i>Enable D</i> )	Abilita/disabilita la quarta password
(II)	( <i>Decoy Enable!</i> )	Abilita/disabilita l'esca

#### Esempio:

Cifratura	
Main_A = "some_crypt_a"	Decoy_A = "12345678"
Decifrazione dei dati segreti	
Main_A = "some_crypt_a" Main_B = "another_crypt_b" Main_C = "scramble_c" Main_D = "whiten_d"	DISABLED
Decifrazione dell'esca	
Main_A = "12345678" Main_B = "qwertyui" Main_C = "zxcvbnm," Main_D = "whiten_d"	DISABLED

**OK** La password Main\_D è sempre condivisa dai dati principali ed esca

<b>Cifratura</b>	
Main_A = "some_crypt_a" Main_B = <b>DISABLED</b> Main_C = "scramble_c" Main_D = "whiten_d"	Decoy_A = "12345678" Decoy_B = "qwertyui" Decoy_C = <b>DISABLED</b>
<b>Decifrazione dei dati segreti</b>	
Main_A = "some_crypt_a" Main_B = <b>DISABLED</b> Main_C = "scramble_c" Main_D = "whiten_d"	DISABLED
<b>Decifrazione dell'esca</b>	
Main_A = "12345678" Main_B = "qwertyui" Main_C = <b>DISABLED</b> Main_D = "whiten_d"	DISABLED

**OK** Si possono disabilitare le password Main\_B / Main\_C / Decoy\_B / Decoy\_C indipendentemente

<b>Cifratura</b>	
Main_A = "some_crypt_a" Main_B = DISABLED Main_C = "scramble_c" Main_D = <b>DISABLED</b>	Decoy_A = "12345678" Decoy_B = "qwertyui" Decoy_C = DISABLED
<b>Decifrazione dei dati segreti</b>	
Main_A = "some_crypt_a" Main_B = DISABLED Main_C = "scramble_c" Main_D = DISABLED	DISABLED
<b>Decifrazione dell'esca</b>	
Main_A = "12345678" Main_B = "qwertyui" Main_C = DISABLED Main_D = <b>"some_crypt_a"</b>	DISABLED

Questa è una configurazione ERRATA:

- la password disabilitata Main\_D è uguale alla password Main\_A
- la password Main\_D è sempre condivisa dai dati principali ed esca
- la decifrazione dell'esca (quando si è sotto attacco...) rivelerà la password Main\_A all'attaccante

*Non disabilitare mai la password Main\_D se si pianifica di usare un'esca.*

[INDIETRO](#)

**INIZIO:**

[\(File Lock/Unlock\)](#)
[Vai al pannello file \(formato binario raw\)](#)

Selezionare *File Lock/Unlock*.

**PASSO 1:**

The screenshot shows two windows of the Multi-Obfuscator v2.00 software. Both windows have a blue header bar with tabs: Main Setup, Decoy Setup, Main File Lock, Decoy File Setup, and File Unlock. The left window (I) is titled 'Main Setup' and contains fields for inserting main passwords (Min: 8, Max: 32) for four methods: Cryptography (A), Cryptography (B), Scrambling (C), and Whitening (D). It also includes a 'Passwords Check' section with a green bar indicating 'A = B = C = D'. The right window (II) is titled 'Decoy Setup' and contains fields for inserting decoy passwords (Min: 8, Max: 32) for the same four methods. It includes a 'Decoy Enable!' checkbox which is checked in the screenshot. Both windows have icons for 'SECRET' and 'TOP SECRET' at the bottom.

(I) [\(Cryptography A\)](#)

La prima password

[\(Enable B\)](#)

Abilita/disabilita la seconda password

[\(Enable C\)](#)

Abilita/disabilita la terza password

[\(Enable D\)](#)

Abilita/disabilita la quarta password

(II) [\(Decoy Enable!\)](#)

Abilita/disabilita l'esca

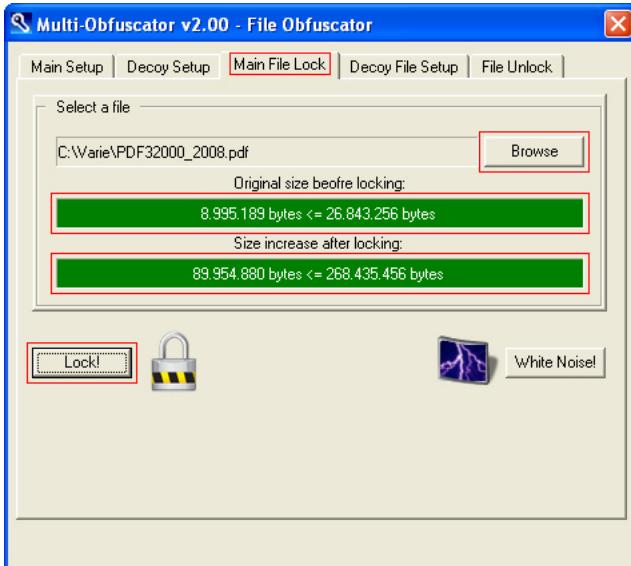
Inserire una password e selezionare un livello di rumore. I dettagli completi su password e rumore sono disponibili in speciali sezioni separate:

- [SETUP DELLE PASSWORD SEMPLICE](#)
- [OPZIONI: LIVELLO DI RUMORE](#)

*Il setup di base, sebbene simile ad un tradizionale software di sicurezza, si basa sulla stessa architettura di sicurezza multi livello del setup avanzato.*

[CARATTERISTICHE: ARCHITETTURA DEL PROGRAMMA](#)

## PASSO 2:



(Browse)	Selezionare un file
(Original size before locking)	Esempio: 8.995.189 byte
(Size increase after locking)	Esempio: 89.954.880 byte
(Lock!)	Inizio dell'operazione di cifratura

Selezionare i dati segreti da cifrare (un file singolo o un archivio zip/rar/...). I dati segreti non saranno sovrascritti e i dati cifrati verranno salvati in una directory differente. Il nome del file/archivio non verrà salvato all'interno dei dati cifrati, consentendo di rinominare e decifrare i dati segreti con un nome differente.

### Esempio:

- MultiObfuscator: C:\...\dir1\xxx.pdf [9 Mb] → C:\...\dir2\xxx.pdf [90 Mb]
- Rename: C:\...\dir2\xxx.pdf → UsbKey:\...\yyy.pdf
- MultiObfuscator: UsbKey:\...\yyy.pdf [90 Mb] → D:\...\yyy.pdf [9 Mb]

La dimensione massima cifrata è vincolata a 256 Mb e, a seconda del livello di rumore, lo è anche la dimensione massima originale. I file piccoli (fino a 4 Mb) consentiranno di selezionare liberamente qualsiasi livello di rumore. I file medi e grandi (fino a 64 Mb) restringeranno la scelta ad un minor livello di rumore compatibile (per dimensione).

### Esempio:

- Livello di rumore: 900%
- Dimensione originale prima della cifratura: 8.995.189 byte ≤ 25 Mb
- Dimensione dopo la cifratura:  $((8.995.189 + 256) / 96) * 960 = 89.954.880$  byte ≤ 256 Mb

Noise Level	Noise	Data	Min. Plain → Locked Size	Max. Plain → Locked Size
900%	864	<b>96</b>	1 B → 2880 B	<b>25 Mb → 256 Mb</b>

### OPZIONI: LIVELLO DI RUMORE

### INDIETRO



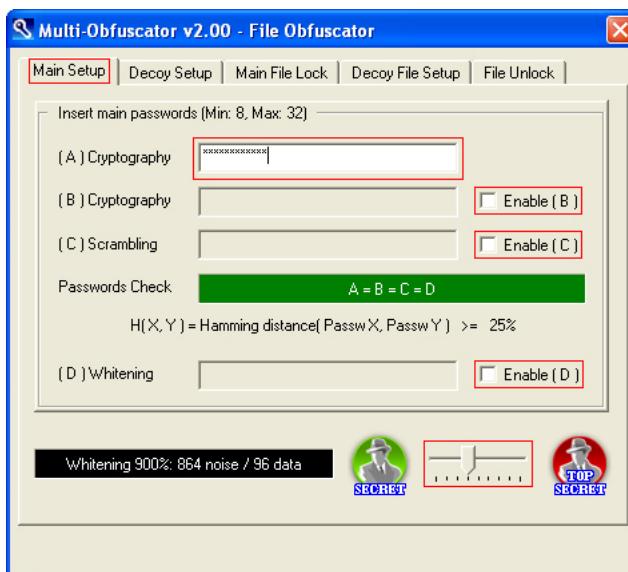
INIZIO:

[\(File Lock/Unlock\)](#)

Vai al pannello file (formato binario raw)

Selezionare *File Lock/Unlock*.

PASSO 1:

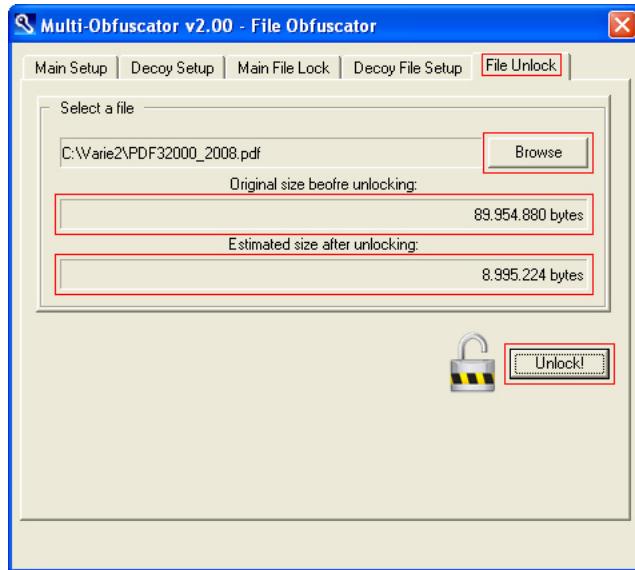


<a href="#"><u>(Cryptography A)</u></a>	La prima password
<a href="#"><u>(Enable B)</u></a>	Abilita/disabilita la seconda password
<a href="#"><u>(Enable C)</u></a>	Abilita/disabilita la terza password
<a href="#"><u>(Enable D)</u></a>	Abilita/disabilita la quarta password

Impostare la stessa password e livello di rumore usati al momento dell'operazione di cifratura.  
I dettagli completi su password e rumore sono disponibili in speciali sezioni separate:

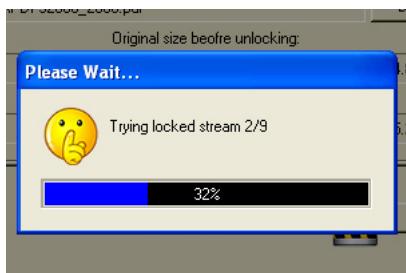
- [SETUP DELLE PASSWORD SEMPLICE](#)
- [OPZIONI: LIVELLO DI RUMORE](#)

## PASSO 2:



( <i>Browse</i> )	Selezionare un file cifrato
( <i>Original size before unlocking</i> )	Esempio: 89.954.880 byte
( <i>Estimated size after unlocking</i> )	Esempio: 8.995.224 byte
( <i>Unlock!</i> )	Inizio dell'operazione di decifrazione

Selezionare i dati cifrati da decifrare. I dati cifrati non saranno sovrascritti e i dati segreti decifrati verranno salvati in una directory differente.



**Numero di aspetti: (960 / Data) – 1  
-1 a causa dell'autoaggiustamento  $\chi^2$**

Noise Level	Noise	Data	Aspects
300%	720	<b>240</b>	4 - 1
400%	768	<b>192</b>	5 - 1
500%	800	<b>160</b>	6 - 1
900%	864	<b>96</b>	10 - 1
1100%	880	<b>80</b>	12 - 1
1400%	896	<b>64</b>	15 - 1
1900%	912	<b>48</b>	20 - 1
2900%	928	<b>32</b>	30 - 1
5900%	944	<b>16</b>	60 - 1

*La decifrazione, anche quando le password e i dati cifrati sono corretti, può richiedere molto tempo a causa del numero di aspetti. Maggiore è il livello di rumore, più aumentano gli aspetti. MultiObfuscator, per costruzione, non conosce quale aspetto è stato selezionato al momento della cifratura e deve indovinarlo lentamente per tentativi.*

[CARATTERISTICHE: ARCHITETTURA DEL PROGRAMMA](#)

[INDIETRO](#)



## CIFRATURA FILE – SETUP MEDIO (4 PASSWORD)

INIZIO:



[\(File Lock/Unlock\)](#)

Vai al pannello file (formato binario raw)

Selezionare *File Lock/Unlock*.

PASSO 1:

(I)

(II)

(I) <a href="#">(Cryptography A)</a>	La prima password (chiavi crittografiche)
<a href="#">(Cryptography B)</a>	La seconda password (CSPRNG crittografico)
<a href="#">(Scrambling C)</a>	La terza password (CSPRNG scrambling)
<a href="#">(Whitening D)</a>	La quarta password (CSPRNG whitening)
<a href="#">(Enable B)</a>	Abilita/disabilita la seconda password
<a href="#">(Enable C)</a>	Abilita/disabilita la terza password
<a href="#">(Enable D)</a>	Abilita/disabilita la quarta password
(II) <a href="#">(Decoy Enable!)</a>	Abilita/disabilita l'esca

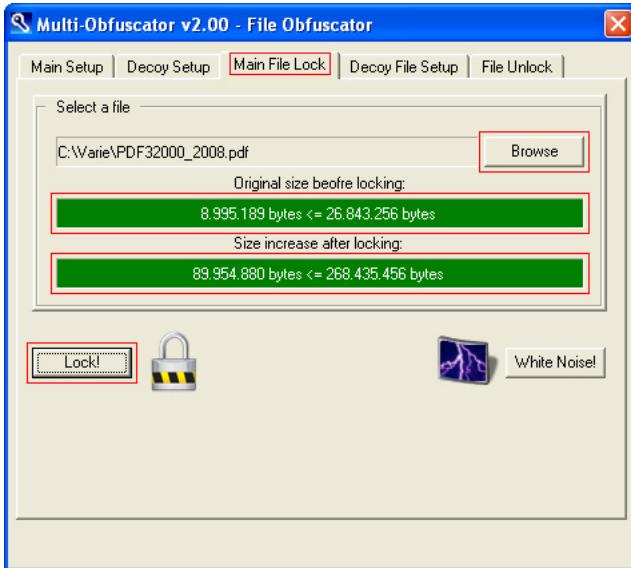
Inserire un'insieme di password e selezionare un livello di rumore. I dettagli completi su password e rumore sono disponibili in speciali sezioni separate:

- [SETUP DELLE PASSWORD MEDIO](#)
- [OPZIONI: LIVELLO DI RUMORE](#)

*Il setup medio consente un uso completo dell'architettura di sicurezza multi livello.*

[CARATTERISTICHE: ARCHITETTURA DEL PROGRAMMA](#)

## PASSO 2:



(Browse)	Selezionare un file
(Original size before locking)	Esempio: 8.995.189 byte
(Size increase after locking)	Esempio: 89.954.880 byte
(Lock!)	Inizio dell'operazione di cifratura

Selezionare i dati segreti da cifrare (un file singolo o un archivio zip/rar/...). I dati segreti non saranno sovrascritti e i dati cifrati verranno salvati in una directory differente. Il nome del file/archivio non verrà salvato all'interno dei dati cifrati, consentendo di rinominare e decifrare i dati segreti con un nome differente.

### Esempio:

- MultiObfuscator: C:\...\dir1\xxx.pdf [9 Mb] → C:\...\dir2\xxx.pdf [90 Mb]
- Rename: C:\...\dir2\xxx.pdf → UsbKey:\...\yyy.pdf
- MultiObfuscator: UsbKey:\...\yyy.pdf [90 Mb] → D:\...\yyy.pdf [9 Mb]

La dimensione massima cifrata è vincolata a 256 Mb e, a seconda del livello di rumore, lo è anche la dimensione massima originale. I file piccoli (fino a 4 Mb) consentiranno di selezionare liberamente qualsiasi livello di rumore. I file medi e grandi (fino a 64 Mb) restringeranno la scelta ad un minor livello di rumore compatibile (per dimensione).

### Esempio:

- Livello di rumore: 900%
- Dimensione originale prima della cifratura: 8.995.189 byte ≤ 25 Mb
- Dimensione dopo la cifratura:  $((8.995.189 + 256) / 96) * 960 = 89.954.880$  byte ≤ 256 Mb

Noise Level	Noise	Data	Min. Plain → Locked Size	Max. Plain → Locked Size
900%	864	<b>96</b>	1 B → 2880 B	<b>25 Mb → 256 Mb</b>

### OPZIONI: LIVELLO DI RUMORE

### INDIETRO



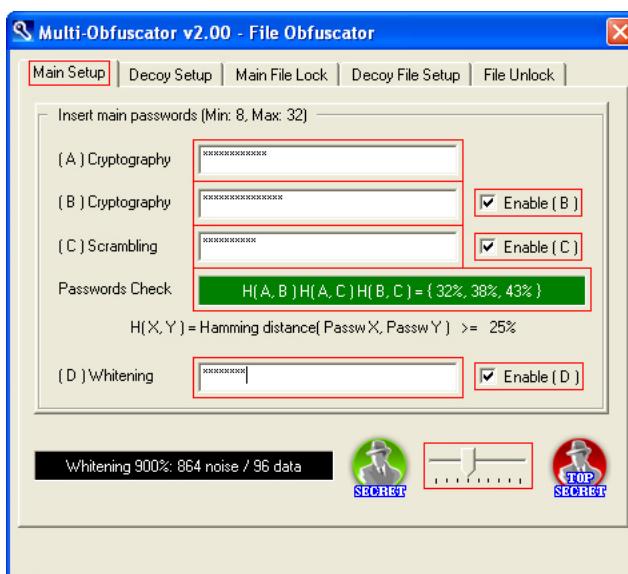
INIZIO:

[\(File Lock/Unlock\)](#)

Vai al pannello file (formato binario raw)

Selezionare *File Lock/Unlock*.

PASSO 1:

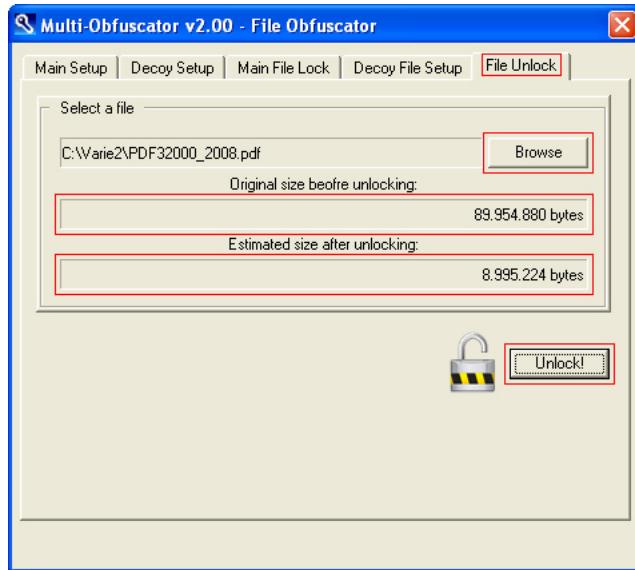


<a href="#"><u>(Cryptography A)</u></a>	La prima password (chiavi crittografiche)
<a href="#"><u>(Cryptography B)</u></a>	La seconda password (CSPRNG crittografico)
<a href="#"><u>(Scrambling C)</u></a>	La terza password (CSPRNG scrambling)
<a href="#"><u>(Whitening D)</u></a>	La quarta password (CSPRNG whitening)
<a href="#"><u>(Enable B)</u></a>	Abilita/disabilita la seconda password
<a href="#"><u>(Enable C)</u></a>	Abilita/disabilita la terza password
<a href="#"><u>(Enable D)</u></a>	Abilita/disabilita la quarta password

Impostare lo stesso insieme di password e livello di rumore usati al momento dell'operazione di cifratura. I dettagli completi su password e rumore sono disponibili in speciali sezioni separate:

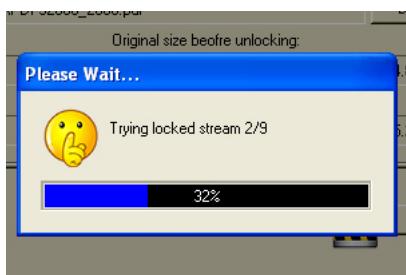
- [SETUP DELLE PASSWORD MEDIO](#)
- [OPZIONI: LIVELLO DI RUMORE](#)

## PASSO 2:



( <i>Browse</i> )	Selezionare un file cifrato
( <i>Original size before unlocking</i> )	Esempio: 89.954.880 byte
( <i>Estimated size after unlocking</i> )	Esempio: 8.995.224 byte
( <i>Unlock!</i> )	Inizio dell'operazione di decifrazione

Selezionare i dati cifrati da decifrare. I dati cifrati non saranno sovrascritti e i dati segreti decifrati verranno salvati in una directory differente.



**Numero di aspetti: (960 / Data) – 1  
-1 a causa dell'autoaggiustamento  $\chi^2$**

Noise Level	Noise	Data	Aspects
300%	720	<b>240</b>	4 - 1
400%	768	<b>192</b>	5 - 1
500%	800	<b>160</b>	6 - 1
900%	864	<b>96</b>	10 - 1
1100%	880	<b>80</b>	12 - 1
1400%	896	<b>64</b>	15 - 1
1900%	912	<b>48</b>	20 - 1
2900%	928	<b>32</b>	30 - 1
5900%	944	<b>16</b>	60 - 1

*La decifrazione, anche quando le password e i dati cifrati sono corretti, può richiedere molto tempo a causa del numero di aspetti. Maggiore è il livello di rumore, più aumentano gli aspetti. MultiObfuscator, per costruzione, non conosce quale aspetto è stato selezionato al momento della cifratura e deve indovinarlo lentamente per tentativi.*

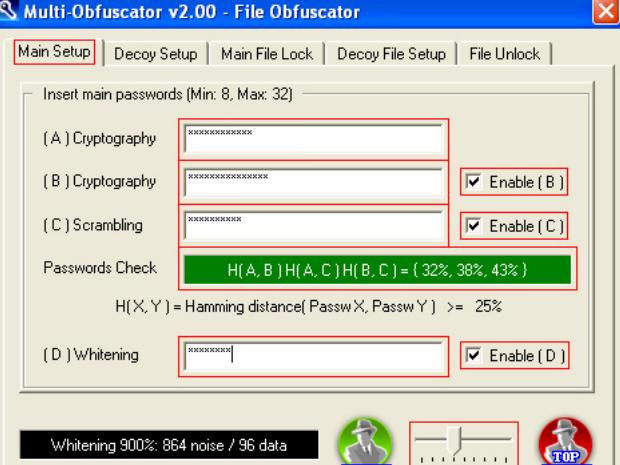
[CARATTERISTICHE: ARCHITETTURA DEL PROGRAMMA](#)

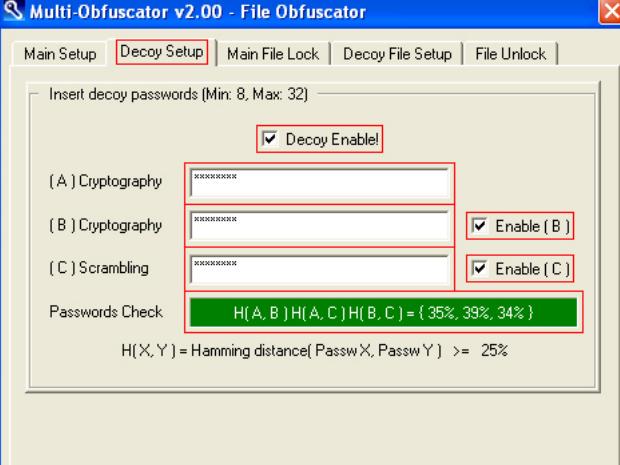
[INDIETRO](#)

**INIZIO:**[\(File Lock/Unlock\)](#)

Vai al pannello file (formato binario raw)

Selezionare *File Lock/Unlock*.**PASSO 1:**

(I) 

(II) 

(I) [\(Cryptography A\)](#)

La prima password (chiavi crittografiche)

[\(Cryptography B\)](#) La seconda password (CSPRNG crittografico)[\(Scrambling C\)](#) La terza password (CSPRNG scrambling)[\(Whitening D\)](#) La quarta password (CSPRNG whitening)[\(Enable B\)](#) Abilita/disabilita la seconda password[\(Enable C\)](#) Abilita/disabilita la terza password[\(Enable D\)](#) Abilita/disabilita la quarta password(II) [\(Decoy Enable!\)](#)

Abilita/disabilita l'esca

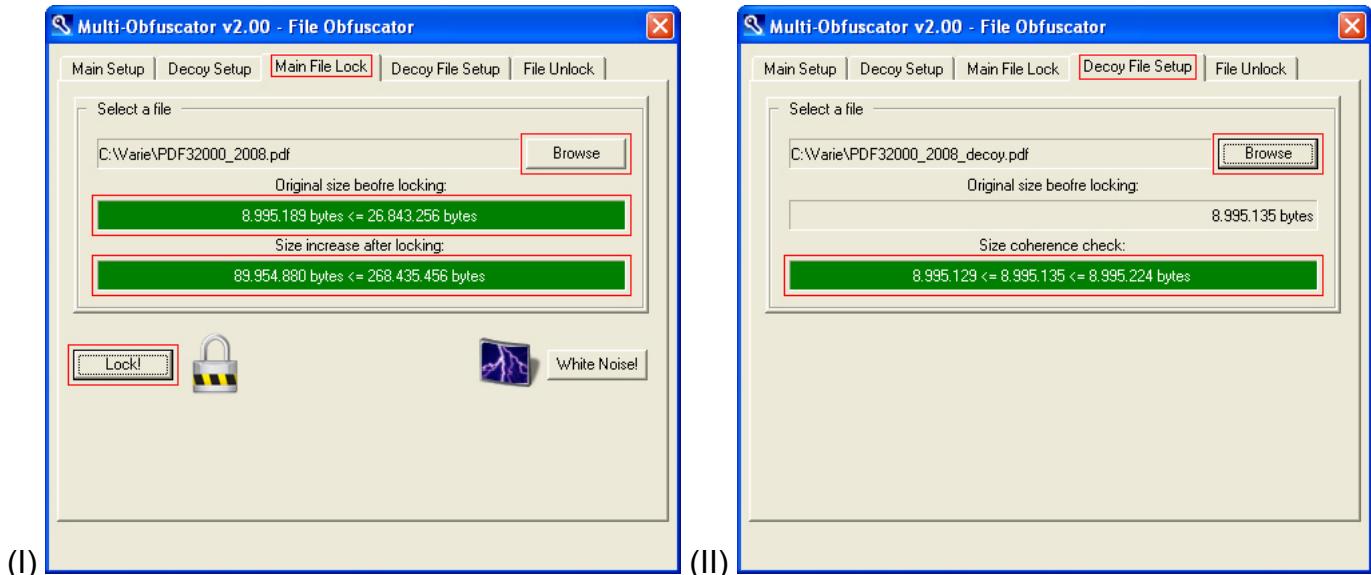
[\(Cryptography A\)](#) La prima password esca[\(Cryptography B\)](#) La seconda password esca[\(Scrambling C\)](#) La terza password esca[\(Enable B\)](#) Abilita/disabilita la seconda password esca[\(Enable C\)](#) Abilita/disabilita la terza password esca

Inserire un'insieme di password, un'insieme di password esca e selezionare un livello di rumore. I dettagli completi su password e rumore sono disponibili in speciali sezioni separate:

- [SETUP DELLE PASSWORD AVANZATO – CIFRATURA](#)
- [OPZIONI: LIVELLO DI RUMORE](#)

*Il setup avanzato consente un uso completo dell'architettura di sicurezza multi livello e multi aspetto.*  
[CARATTERISTICHE: ARCHITETTURA DEL PROGRAMMA](#)

## PASSO 2:



(I)	<b>(Browse)</b>	Selezionare un file
	<b>(Original size before locking)</b>	Esempio: 8.995.189 byte
	<b>(Size increase after locking)</b>	Esempio: 89.954.880 byte
	<b>(Lock!)</b>	Inizio dell'operazione di cifratura
(II)	<b>(Browse)</b>	Selezionare un file esca
	<b>(Size coherence check)</b>	Esempio: 8.995.135 byte

Selezionare i dati segreti e un'esca compatibile (per dimensione) da cifrare.

### Esempio:

- Livello di rumore: 900%
- Dimensione originale prima della cifratura: 8.995.189 byte  $\leq$  25 Mb
- Dimensione dopo la cifratura:  $((8.995.189 + 256) / 96) * 960 = 89.954.880$  byte  $\leq$  256 Mb
- Dimensione dell'esca:  $((8.995.129 \leq x \leq 8.995.224) + 256) / 96 * 960 = 89.954.880$  byte  $\leq$  256 Mb

Noise Level	Noise	Data	Min. Plain $\rightarrow$ Locked Size	Max. Plain $\rightarrow$ Locked Size
900%	864	<b>96</b>	1 B $\rightarrow$ 2880 B	<b>25 Mb <math>\rightarrow</math> 256 Mb</b>

Fare attenzione:

- maggiore è il livello di rumore, più diminuiscono i byte di dati per blocco
- più diminuiscono i byte di dati per blocco, più ristretto è il range di dimensione dell'esca

*Minimum (300%)  $\rightarrow$  Data = 240  $\rightarrow$  inf  $\leq$  x  $\leq$  sup  $\rightarrow$  sup - inf + 1 = 240 bytes*

*Maximum (5900%)  $\rightarrow$  Data = 16  $\rightarrow$  inf  $\leq$  x  $\leq$  sup  $\rightarrow$  sup - inf + 1 = 16 bytes*

Assicurarsi di leggere anche la sezione intermedia

[CIFRATURA FILE – SETUP MEDIO \(4 PASSWORD\)](#)

[INDIETRO](#)



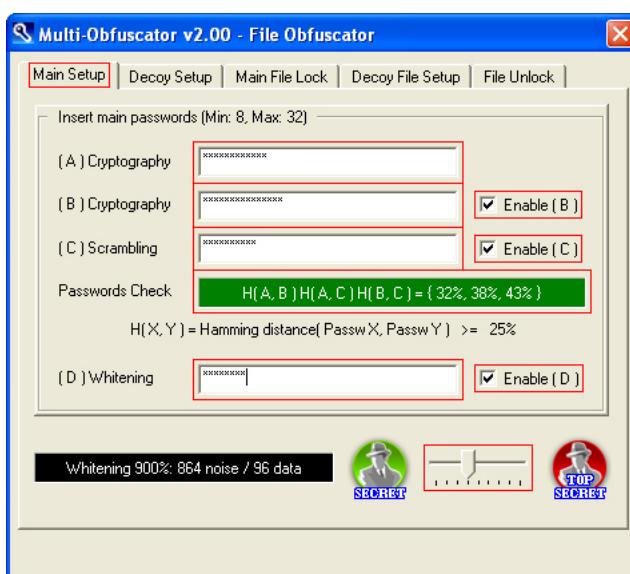
INIZIO:

[\(File Lock/Unlock\)](#)

Vai al pannello file (formato binario raw)

Selezionare *File Lock/Unlock*.

PASSO 1:



<a href="#">(Cryptography A)</a>	La prima password (chiavi crittografiche)
<a href="#">(Cryptography B)</a>	La seconda password (CSPRNG crittografico)
<a href="#">(Scrambling C)</a>	La terza password (CSPRNG scrambling)
<a href="#">(Whitening D)</a>	La quarta password (CSPRNG whitening)
<a href="#">(Enable B)</a>	Abilita/disabilita la seconda password
<a href="#">(Enable C)</a>	Abilita/disabilita la terza password
<a href="#">(Enable D)</a>	Abilita/disabilita la quarta password

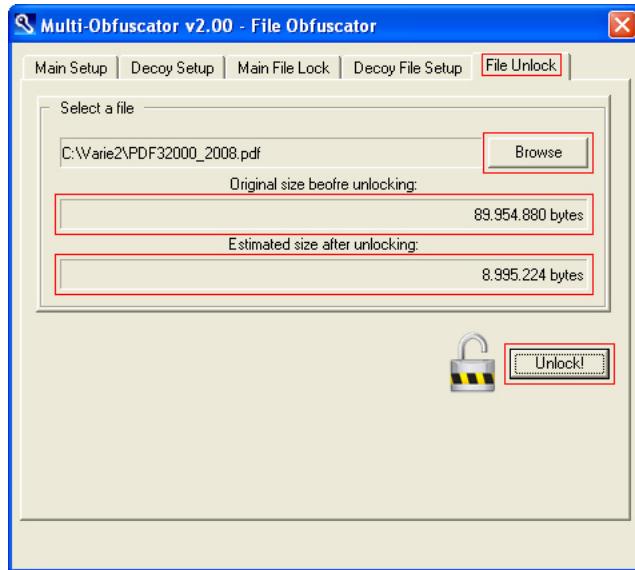
Impostare lo stesso insieme di password (secrete per estrarre i dati segreti, esca per estrarre i dati esca) e livello di rumore usati al momento dell'operazione di cifratura. I dettagli completi su password e rumore sono disponibili in speciali sezioni separate:

- [SETUP DELLE PASSWORD AVANZATO – DECIFRAZIONE](#)
- [OPZIONI: LIVELLO DI RUMORE](#)

I dettagli completi sull'esca sono disponibili qui:

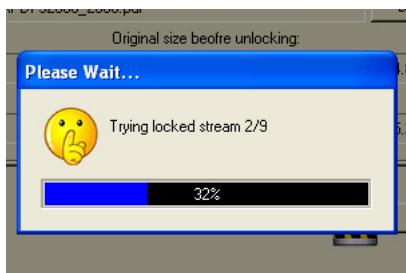
[COSA È LA CRITTOGRAFIA NEGABILE?](#)

## PASSO 2:



( <i>Browse</i> )	Selezionare un file cifrato
( <i>Original size before unlocking</i> )	Esempio: 89.954.880 byte
( <i>Estimated size after unlocking</i> )	Esempio: 8.995.224 byte
( <i>Unlock!</i> )	Inizio dell'operazione di decifrazione

Selezionare i dati cifrati da decifrare. I dati cifrati non saranno sovrascritti e i dati decifrati (segreti o esca, a seconda dell'insieme di password) verranno salvati in una directory differente.



**Numero di aspetti: (960 / Data) – 1  
-1 a causa dell'autoaggiustamento  $\chi^2$**

Noise Level	Noise	Data	Aspects
300%	720	<b>240</b>	4 - 1
400%	768	<b>192</b>	5 - 1
500%	800	<b>160</b>	6 - 1
900%	864	<b>96</b>	10 - 1
1100%	880	<b>80</b>	12 - 1
1400%	896	<b>64</b>	15 - 1
1900%	912	<b>48</b>	20 - 1
2900%	928	<b>32</b>	30 - 1
5900%	944	<b>16</b>	60 - 1

*La decifrazione, anche quando le password e i dati cifrati sono corretti, può richiedere molto tempo a causa del numero di aspetti. Maggiore è il livello di rumore, più aumentano gli aspetti. MultiObfuscator, per costruzione, non conosce quale aspetto è stato selezionato al momento della cifratura e deve indovinarlo lentamente per tentativi.*

[CARATTERISTICHE: ARCHITETTURA DEL PROGRAMMA](#)

[INDIETRO](#)



## RUMORE RANDOM COME ESCA (FILE)

INIZIO:

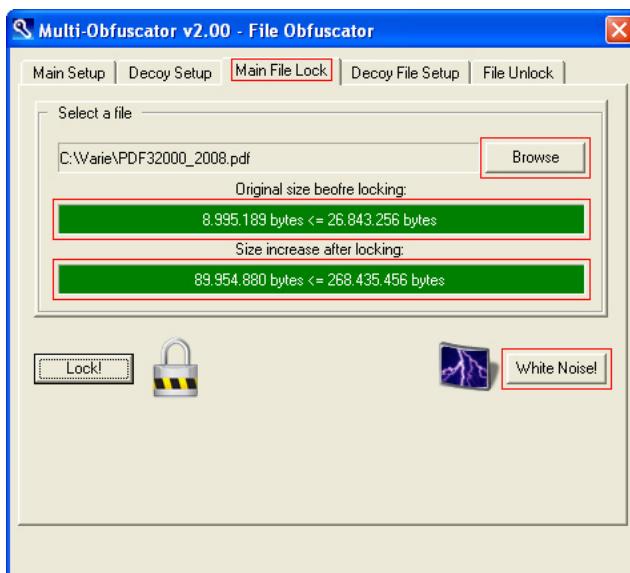


[\(File Lock/Unlock\)](#)

Vai al pannello file (formato binario raw)

Selezionare *File Lock/Unlock*.

PASSO 1:



<a href="#">(Browse)</a>	Selezionare un file
<a href="#">(Original size before locking)</a>	Esempio: 8.995.189 byte
<a href="#">(Size increase after locking)</a>	Esempio: 89.954.880 byte
<a href="#">(White Noise!)</a>	Inizio dell'operazione di randomizzazione

I file cifrati sono statisticamente indistinguibili da quelli randomizzati. Gli utenti avanzati potranno aggiungere contenitori vuoti/fasulli a quelli sensibili, per rallentare gli attaccanti. L'operazione salverà esclusivamente rumore in un contenitore fasullo compatibile (per dimensione) con il file selezionato.

[CARATTERISTICHE: ARCHITETTURA DEL PROGRAMMA](#)

**Esempio:**

- Livello di rumore: 900%
- Dimensione dopo la cifratura:  $((8.995.189 + 256) / 96) * 960 = \mathbf{89.954.880}$  byte  $\leq 256$  Mb
- Dimensione del rumore random: **89.954.880** byte

Noise Level	Noise	Data	Min. Plain → Locked Size	Max. Plain → Locked Size
900%	864	<b>96</b>	1 B → 2880 B	25 Mb → 256 Mb

[OPZIONI: LIVELLO DI RUMORE](#)

[INDIETRO](#)



## CIFRATURA TESTO – SETUP DI BASE (1 PASSWORD)

INIZIO:



[\(Text Lock/Unlock\)](#)

Vai al pannello testo (formato email)

Selezionare *Text Lock/Unlock*.

PASSO 1:

(I)

(II)

(I) <a href="#">(Cryptography A)</a>	La prima password
<a href="#">(Enable B)</a>	Abilita/disabilita la seconda password
<a href="#">(Enable C)</a>	Abilita/disabilita la terza password
<a href="#">(Enable D)</a>	Abilita/disabilita la quarta password
(II) <a href="#">(Decoy Enable!)</a>	Abilita/disabilita l'esca

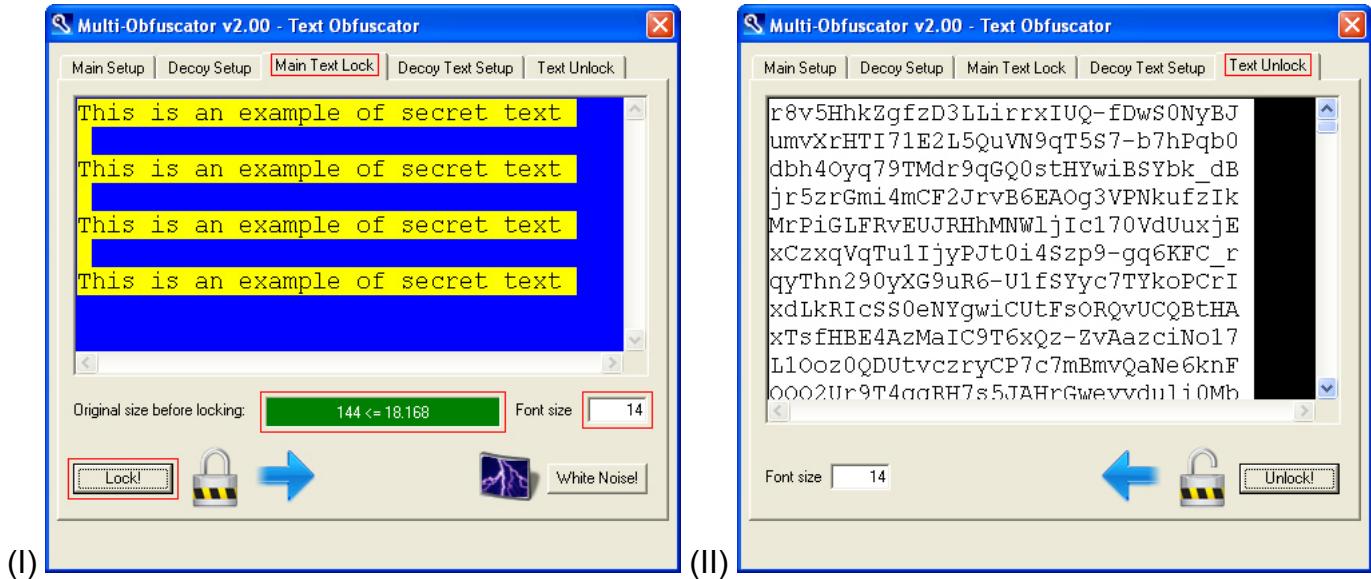
Inserire una password e selezionare un livello di rumore. I dettagli completi su password e rumore sono disponibili in speciali sezioni separate:

- [SETUP DELLE PASSWORD SEMPLICE](#)
- [OPZIONI: LIVELLO DI RUMORE](#)

*Il setup di base, sebbene simile ad un tradizionale software di sicurezza, si basa sulla stessa architettura di sicurezza multi livello del setup avanzato.*

[CARATTERISTICHE: ARCHITETTURA DEL PROGRAMMA](#)

## PASSO 2:



(I)	<TextEdit – finestra blu >	Inserire/incollare un testo
	(Original size before locking)	Esempio: 144 byte
	(Font size)	Dimensione dei caratteri del testo
	(Lock!)	Inizio dell'operazione di cifratura

Selezionare il testo segreto da cifrare. Il testo segreto non sarà sovrascritto e il testo cifrato sarà salvato nella finestra *Text Unlock*, pronto per essere copiato e incollato.

La dimensione massima cifrata è vincolata a 256 Kb e, a seconda del livello di rumore, lo è anche la dimensione massima originale. I file piccoli (fino a 3 Kb) consentiranno di selezionare liberamente qualsiasi livello di rumore. I file medi e grandi (fino a 46 Kb) restringeranno la scelta ad un minor livello di rumore compatibile (per dimensione).

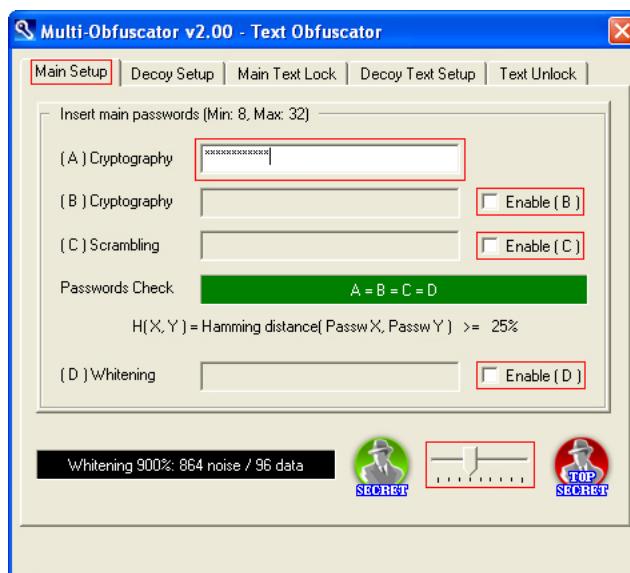
### Esempio:

- Livello di rumore: 900%
- Dimensione originale prima della cifratura: 144 byte  $\leq$  18 Kb
- Dimensione dopo la cifratura:  $((144 + 256) / 96) * 1280 = 6.400$  byte  $\leq$  256 Kb

Noise Level	Noise	Data	Min. Plain $\rightarrow$ Locked Size	Max. Plain $\rightarrow$ Locked Size
900%	864	<b>96</b>	1 B $\rightarrow$ 3840 B	18 Kb $\rightarrow$ 256 Kb

### OPZIONI: LIVELLO DI RUMORE

[INDIETRO](#)

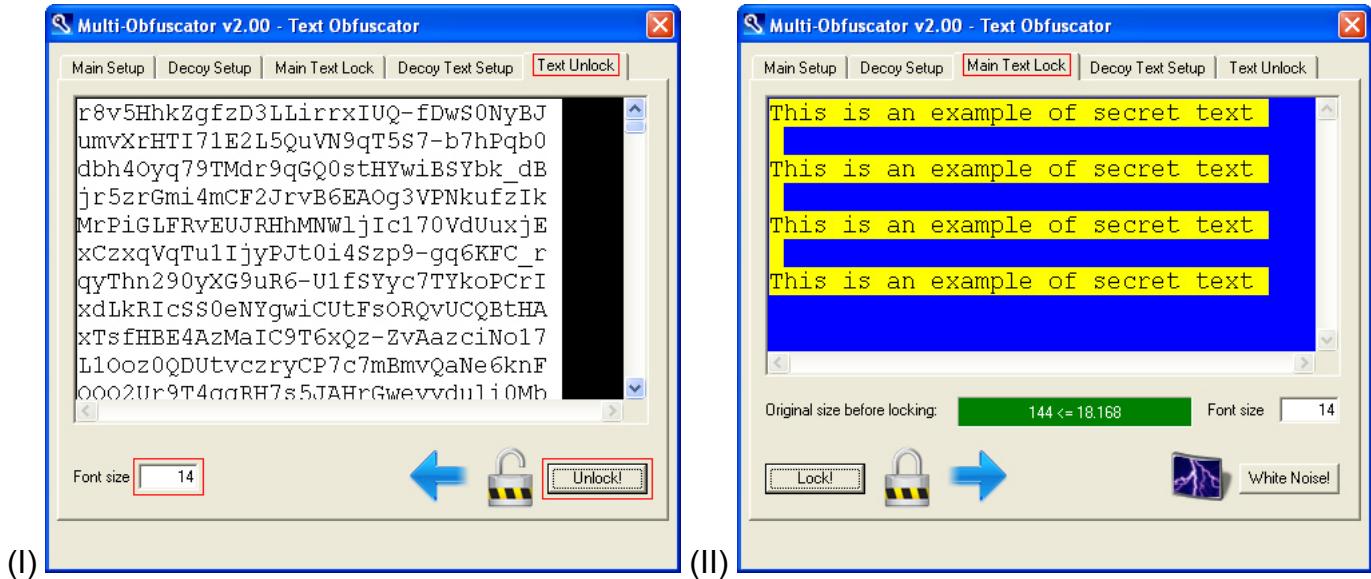
**INIZIO:**[\*\(Text Lock/Unlock\)\*](#)[Vai al pannello testo \(formato email\)](#)Selezionare *Text Lock/Unlock*.**PASSO 1:**

<a href="#"><i>(Cryptography A)</i></a>	La prima password
<a href="#"><i>(Enable B)</i></a>	Abilita/disabilita la seconda password
<a href="#"><i>(Enable C)</i></a>	Abilita/disabilita la terza password
<a href="#"><i>(Enable D)</i></a>	Abilita/disabilita la quarta password

Impostare la stessa password e livello di rumore usati al momento dell'operazione di cifratura.  
I dettagli completi su password e rumore sono disponibili in speciali sezioni separate:

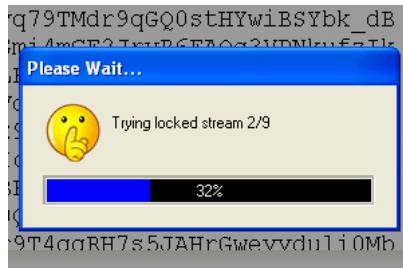
- [SETUP DELLE PASSWORD SEMPLICE](#)
- [OPZIONI: LIVELLO DI RUMORE](#)

## PASSO 2:



(I)	<TextEdit – finestra nera >	Inserire/incollare un testo cifrato
	(Font size)	Dimensione dei caratteri del testo
	(Unlock!)	Inizio dell'operazione di decifrazione

Selezionare il testo cifrato da decifrare. Il testo cifrato non sarà sovrascritto e il testo segreto decifrato sarà salvato nella finestra *Main Text Lock*, pronto per essere copiato e incollato.



**Numero di aspetti: (960 / Data) – 1  
-1 a causa dell'autoaggiustamento  $\chi^2$**

Noise Level	Noise	Data	Aspects
300%	720	<b>240</b>	4 - 1
400%	768	<b>192</b>	5 - 1
500%	800	<b>160</b>	6 - 1
900%	864	<b>96</b>	10 - 1
1100%	880	<b>80</b>	12 - 1
1400%	896	<b>64</b>	15 - 1
1900%	912	<b>48</b>	20 - 1
2900%	928	<b>32</b>	30 - 1
5900%	944	<b>16</b>	60 - 1

La decifrazione, anche quando le password e il testo cifrato sono corretti, può richiedere molto tempo a causa del numero di aspetti. Maggiore è il livello di rumore, più aumentano gli aspetti. MultiObfuscator, per costruzione, non conosce quale aspetto è stato selezionato al momento della cifratura e deve indovinarlo lentamente per tentativi.

[CARATTERISTICHE: ARCHITETTURA DEL PROGRAMMA](#)

[INDIETRO](#)



MEDIUM



## CIFRATURA TESTO – SETUP MEDIO (4 PASSWORD)

**INIZIO:**[\(Text Lock/Unlock\)](#)

Vai al pannello testo (formato email)

Selezionare *Text Lock/Unlock*.**PASSO 1:**

(I)
(II)

(I)	<a href="#">(Cryptography A)</a>	La prima password (chiavi crittografiche)
	<a href="#">(Cryptography B)</a>	La seconda password (CSPRNG crittografico)
	<a href="#">(Scrambling C)</a>	La terza password (CSPRNG scrambling)
	<a href="#">(Whitening D)</a>	La quarta password (CSPRNG whitening)
	<a href="#">(Enable B)</a>	Abilita/disabilita la seconda password
	<a href="#">(Enable C)</a>	Abilita/disabilita la terza password
	<a href="#">(Enable D)</a>	Abilita/disabilita la quarta password
(II)	<a href="#">(Decoy Enable!)</a>	Abilita/disabilita l'esca

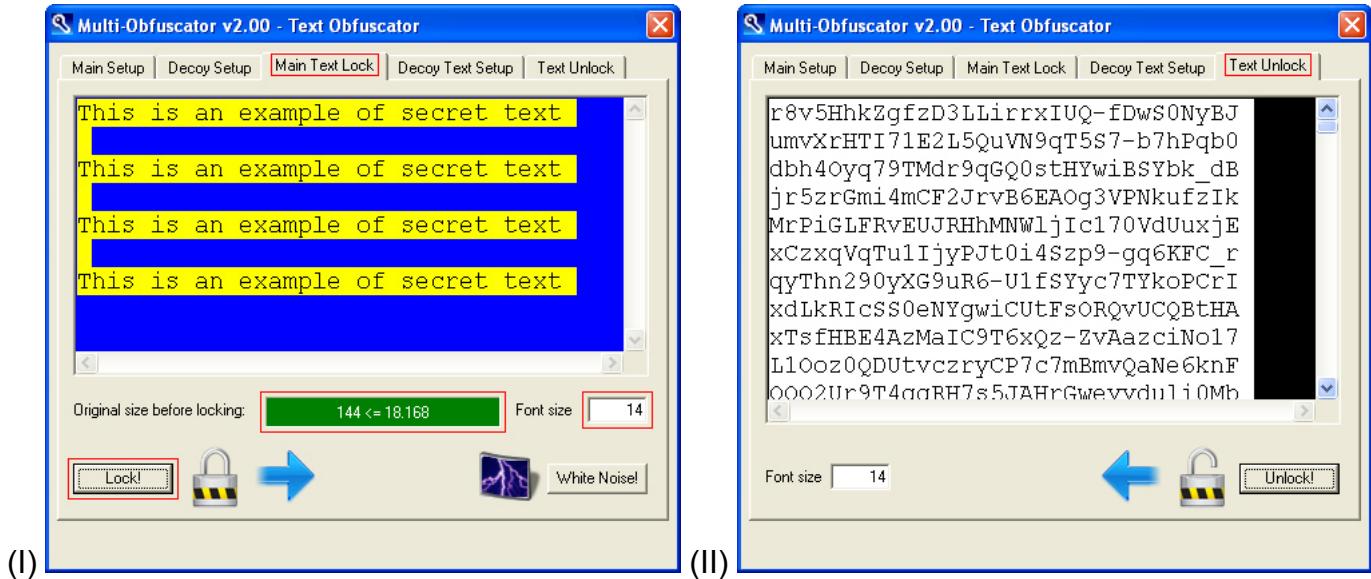
Inserire un'insieme di password e selezionare un livello di rumore. I dettagli completi su password e rumore sono disponibili in speciali sezioni separate:

- [SETUP DELLE PASSWORD MEDIO](#)
- [OPZIONI: LIVELLO DI RUMORE](#)

*Il setup medio consente un uso completo dell'architettura di sicurezza multi livello.*

[CARATTERISTICHE: ARCHITETTURA DEL PROGRAMMA](#)

## PASSO 2:



(I)	<TextEdit – finestra blu >	Inserire/incollare un testo
	(Original size before locking)	Esempio: 144 byte
	(Font size)	Dimensione dei caratteri del testo
	(Lock!)	Inizio dell'operazione di cifratura

Selezionare il testo segreto da cifrare. Il testo segreto non sarà sovrascritto e il testo cifrato sarà salvato nella finestra *Text Unlock*, pronto per essere copiato e incollato.

La dimensione massima cifrata è vincolata a 256 Kb e, a seconda del livello di rumore, lo è anche la dimensione massima originale. I file piccoli (fino a 3 Kb) consentiranno di selezionare liberamente qualsiasi livello di rumore. I file medi e grandi (fino a 46 Kb) restringeranno la scelta ad un minor livello di rumore compatibile (per dimensione).

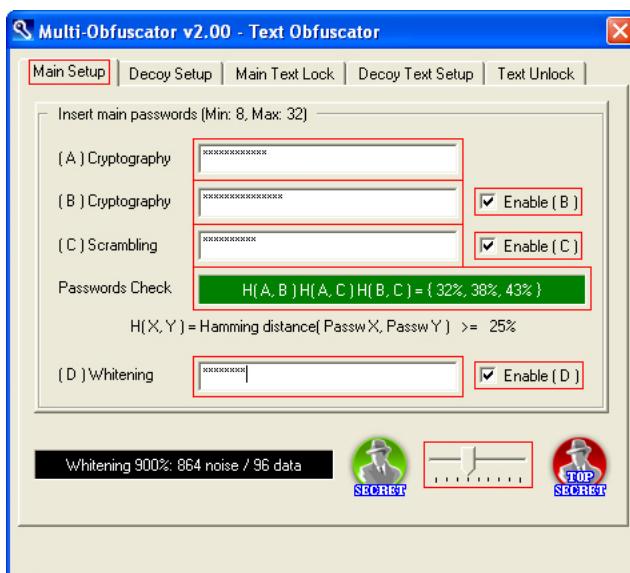
### Esempio:

- Livello di rumore: 900%
- Dimensione originale prima della cifratura: 144 byte  $\leq$  18 Kb
- Dimensione dopo la cifratura:  $((144 + 256) / 96) * 1280 = 6.400$  byte  $\leq$  256 Kb

Noise Level	Noise	Data	Min. Plain $\rightarrow$ Locked Size	Max. Plain $\rightarrow$ Locked Size
900%	864	<b>96</b>	1 B $\rightarrow$ 3840 B	18 Kb $\rightarrow$ 256 Kb

### OPZIONI: LIVELLO DI RUMORE

[INDIETRO](#)

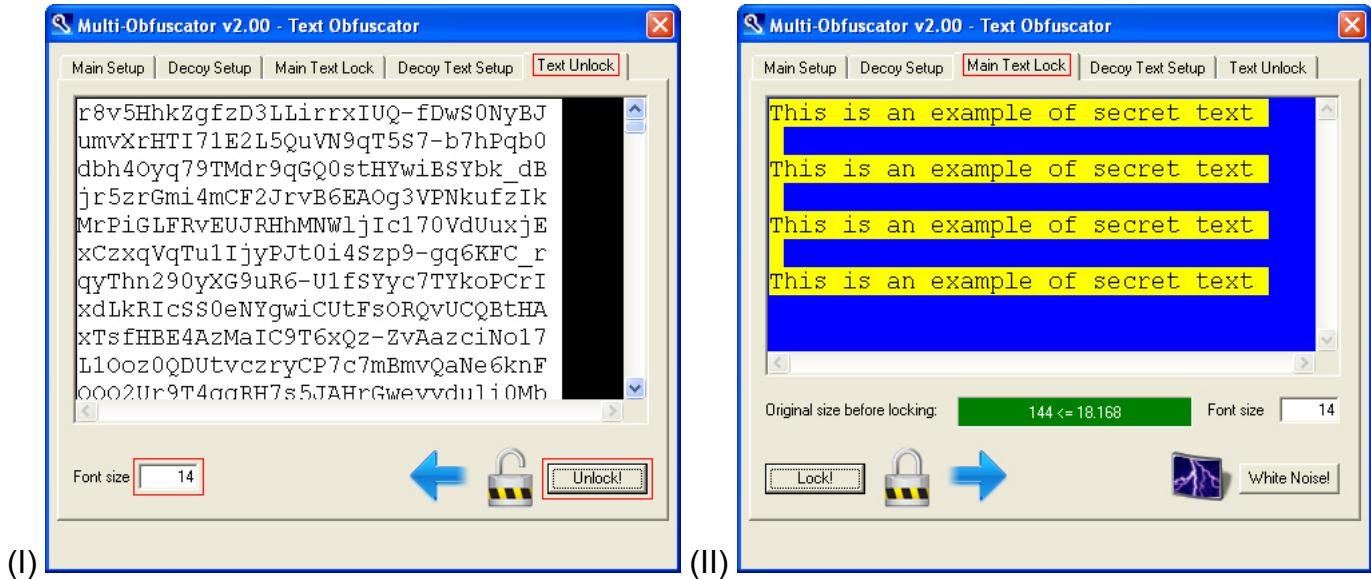
**INIZIO:**[\*\(Text Lock/Unlock\)\*](#)[Vai al pannello testo \(formato email\)](#)Selezionare *Text Lock/Unlock*.**PASSO 1:**

<a href="#"><i>(Cryptography A)</i></a>	La prima password (chiavi crittografiche)
<a href="#"><i>(Cryptography B)</i></a>	La seconda password (CSPRNG crittografico)
<a href="#"><i>(Scrambling C)</i></a>	La terza password (CSPRNG scrambling)
<a href="#"><i>(Whitening D)</i></a>	La quarta password (CSPRNG whitening)
<a href="#"><i>(Enable B)</i></a>	Abilita/disabilita la seconda password
<a href="#"><i>(Enable C)</i></a>	Abilita/disabilita la terza password
<a href="#"><i>(Enable D)</i></a>	Abilita/disabilita la quarta password

Impostare lo stesso insieme di password e livello di rumore usati al momento dell'operazione di cifratura. I dettagli completi su password e rumore sono disponibili in speciali sezioni separate:

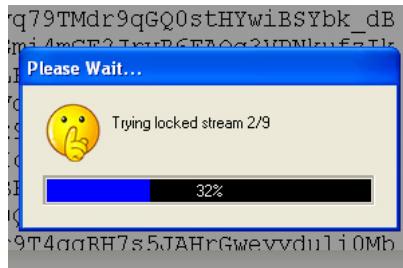
- [SETUP DELLE PASSWORD MEDIO](#)
- [OPZIONI: LIVELLO DI RUMORE](#)

## PASSO 2:



(I)	<TextEdit – finestra nera >	Inserire/incollare un testo cifrato
	(Font size)	Dimensione dei caratteri del testo
	(Unlock!)	Inizio dell'operazione di decifrazione

Selezionare il testo cifrato da decifrare. Il testo cifrato non sarà sovrascritto e il testo segreto decifrato sarà salvato nella finestra *Main Text Lock*, pronto per essere copiato e incollato.



**Numero di aspetti: (960 / Data) – 1  
-1 a causa dell'autoaggiustamento  $\chi^2$**

Noise Level	Noise	Data	Aspects
300%	720	<b>240</b>	4 - 1
400%	768	<b>192</b>	5 - 1
500%	800	<b>160</b>	6 - 1
900%	864	<b>96</b>	10 - 1
1100%	880	<b>80</b>	12 - 1
1400%	896	<b>64</b>	15 - 1
1900%	912	<b>48</b>	20 - 1
2900%	928	<b>32</b>	30 - 1
5900%	944	<b>16</b>	60 - 1

*La decifrazione, anche quando le password e il testo cifrato sono corretti, può richiedere molto tempo a causa del numero di aspetti. Maggiore è il livello di rumore, più aumentano gli aspetti. MultiObfuscator, per costruzione, non conosce quale aspetto è stato selezionato al momento della cifratura e deve indovinarlo lentamente per tentativi.*

[CARATTERISTICHE: ARCHITETTURA DEL PROGRAMMA](#)

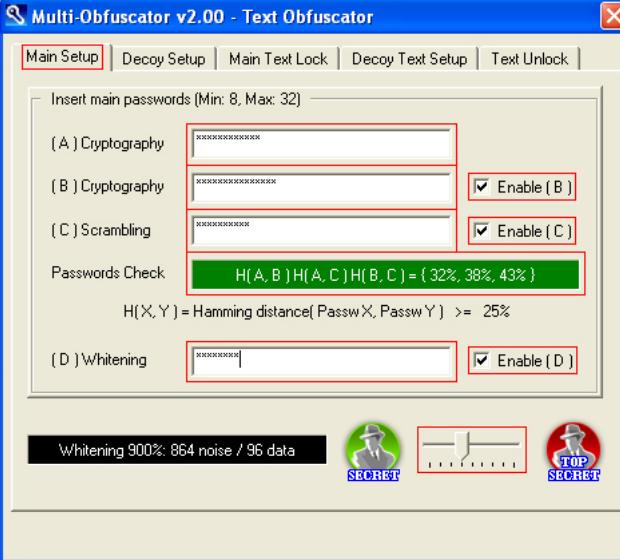
[INDIETRO](#)

**INIZIO:**

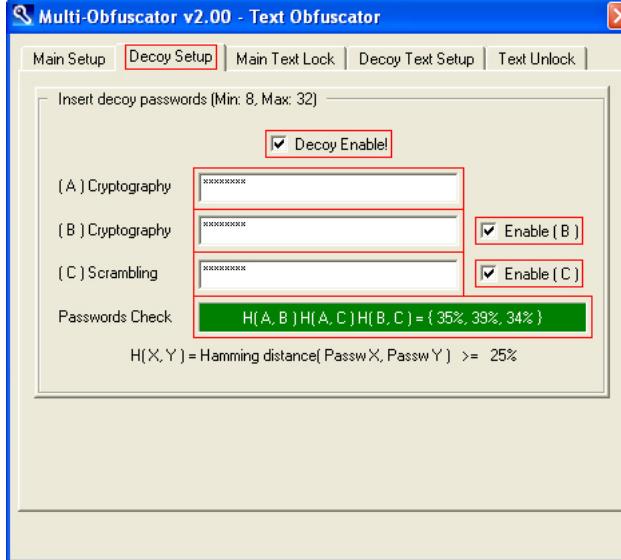
[\(Text Lock/Unlock\)](#)
[Vai al pannello testo \(formato email\)](#)

 Selezionare *Text Lock/Unlock*.

**PASSO 1:**



(I)



(II)

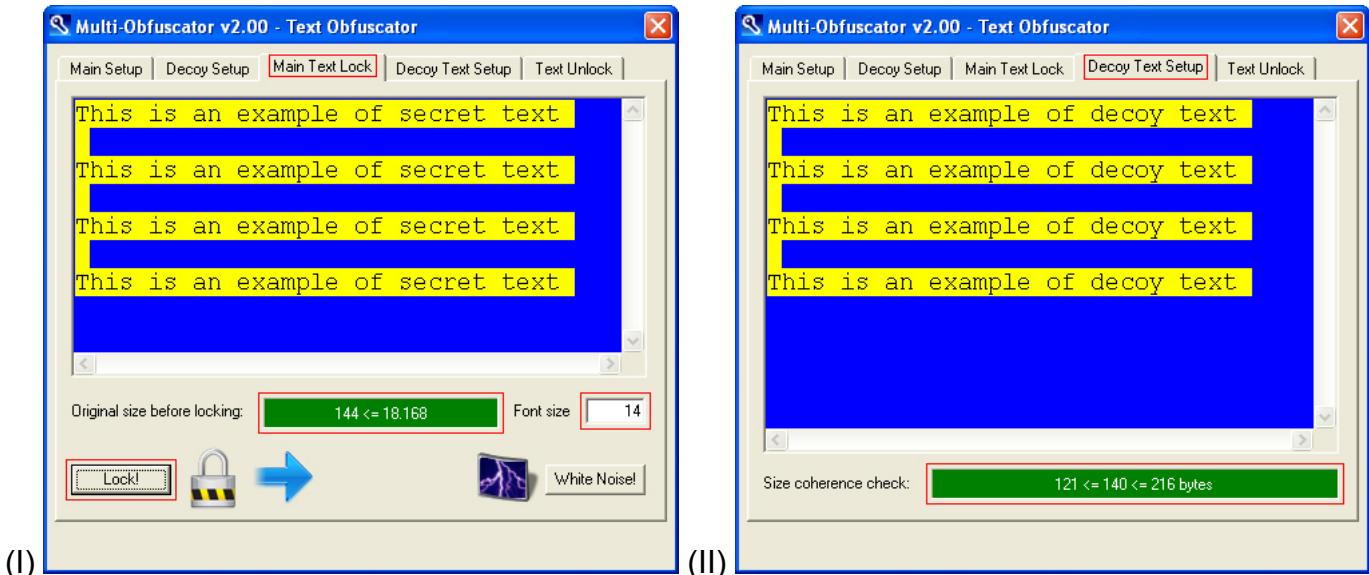
(I) <a href="#">(Cryptography A)</a>	La prima password (chiavi crittografiche)
<a href="#">(Cryptography B)</a>	La seconda password (CSPRNG crittografico)
<a href="#">(Scrambling C)</a>	La terza password (CSPRNG scrambling)
<a href="#">(Whitening D)</a>	La quarta password (CSPRNG whitening)
<a href="#">(Enable B)</a>	Abilita/disabilita la seconda password
<a href="#">(Enable C)</a>	Abilita/disabilita la terza password
<a href="#">(Enable D)</a>	Abilita/disabilita la quarta password
(II) <a href="#">(Decoy Enable!)</a>	Abilita/disabilita l'esca
<a href="#">(Cryptography A)</a>	La prima password esca
<a href="#">(Cryptography B)</a>	La seconda password esca
<a href="#">(Scrambling C)</a>	La terza password esca
<a href="#">(Enable B)</a>	Abilita/disabilita la seconda password esca
<a href="#">(Enable C)</a>	Abilita/disabilita la terza password esca

Inserire un'insieme di password, un'insieme di password esca e selezionare un livello di rumore. I dettagli completi su password e rumore sono disponibili in speciali sezioni separate:

- [SETUP DELLE PASSWORD AVANZATO – CIFRATURA](#)
- [OPZIONI: LIVELLO DI RUMORE](#)

*Il setup avanzato consente un uso completo dell'architettura di sicurezza multi livello e multi aspetto.*
[CARATTERISTICHE: ARCHITETTURA DEL PROGRAMMA](#)

## PASSO 2:



(I)	<TextEdit – finestra blu >	Inserire/incollare un testo
	(Original size before locking)	Esempio: 144 byte
	(Font size)	Dimensione dei caratteri del testo
	(Lock!)	Inizio dell'operazione di cifratura
(II)	<TextEdit – finestra blu >	Inserire/incollare un testo esca
	(Size coherence check)	Esempio: 140 byte

Selezionare il testo segreto e un'esca compatibile (per dimensione) da cifrare.

### Esempio:

- Livello di rumore: 900%
- Dimensione originale prima della cifratura: 144 byte  $\leq$  18 Kb
- Dimensione dopo la cifratura:  $((144 + 256) / 96) * 1280 = 6.400$  byte  $\leq$  256 Kb
- Dimensione dell'esca:  $((121 \leq x \leq 216) + 256) / 96 * 1280 = 6.400$  byte  $\leq$  256 Kb

Noise Level	Noise	Data	Min. Plain $\rightarrow$ Locked Size	Max. Plain $\rightarrow$ Locked Size
900%	864	96	1 B $\rightarrow$ 3840 B	18 Kb $\rightarrow$ 256 Kb

Fare attenzione:

- maggiore è il livello di rumore, più diminuiscono i byte di dati per blocco
- più diminuiscono i byte di dati per blocco, più ristretto è il range di dimensione dell'esca

*Minimum (300%)  $\rightarrow$  Data = 240  $\rightarrow$  inf  $\leq$  x  $\leq$  sup  $\rightarrow$  sup - inf + 1 = 240 bytes*

*Maximum (5900%)  $\rightarrow$  Data = 16  $\rightarrow$  inf  $\leq$  x  $\leq$  sup  $\rightarrow$  sup - inf + 1 = 16 bytes*

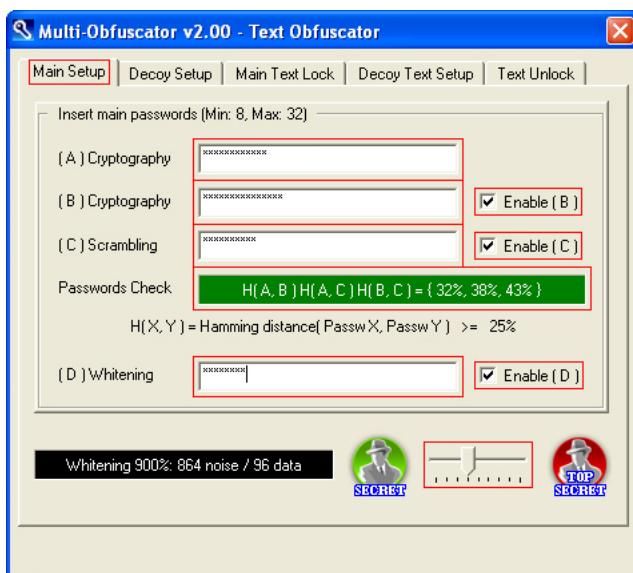
Assicurarsi di leggere anche la sezione intermedia

[CIFRATURA TESTO – SETUP MEDIO \(4 PASSWORD\)](#)

[INDIETRO](#)

**INIZIO:**[\*\(Text Lock/Unlock\)\*](#)

Vai al pannello testo (formato email)

Selezionare *Text Lock/Unlock*.**PASSO 1:**

<a href="#"><i>(Cryptography A)</i></a>	La prima password (chiavi crittografiche)
<a href="#"><i>(Cryptography B)</i></a>	La seconda password (CSPRNG crittografico)
<a href="#"><i>(Scrambling C)</i></a>	La terza password (CSPRNG scrambling)
<a href="#"><i>(Whitening D)</i></a>	La quarta password (CSPRNG whitening)
<a href="#"><i>(Enable B)</i></a>	Abilita/disabilita la seconda password
<a href="#"><i>(Enable C)</i></a>	Abilita/disabilita la terza password
<a href="#"><i>(Enable D)</i></a>	Abilita/disabilita la quarta password

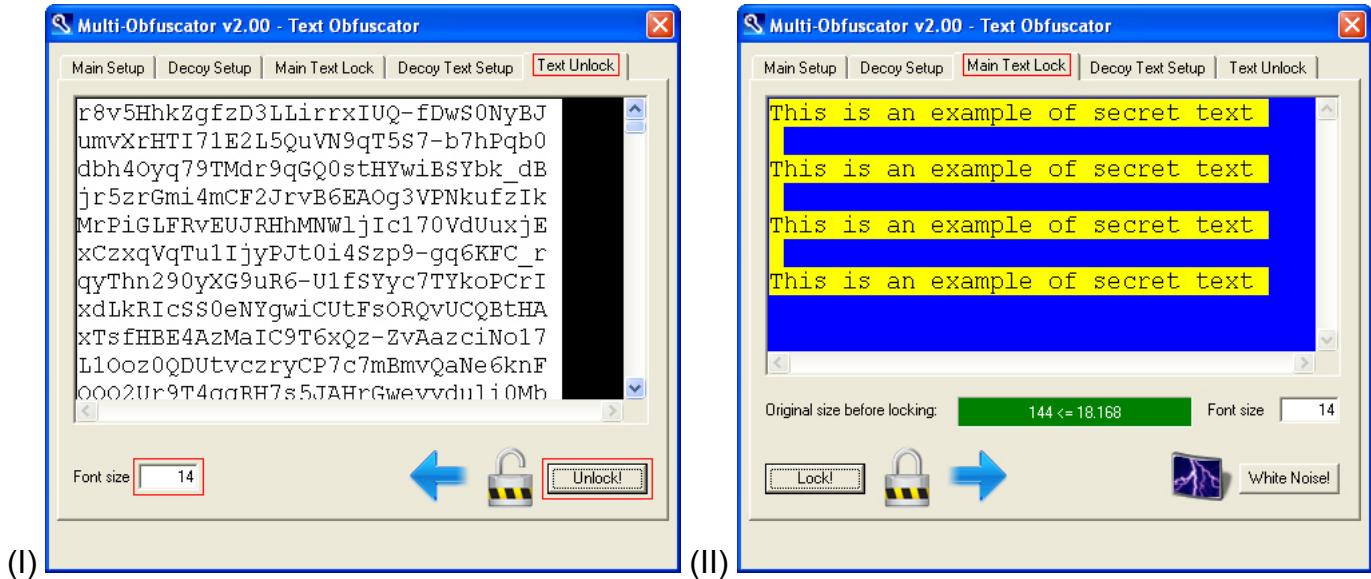
Impostare lo stesso insieme di password (secrete per estrarre i dati segreti, esca per estrarre i dati esca) e livello di rumore usati al momento dell'operazione di cifratura. I dettagli completi su password e rumore sono disponibili in speciali sezioni separate:

- [SETUP DELLE PASSWORD AVANZATO – DECIFRAZIONE](#)
- [OPZIONI: LIVELLO DI RUMORE](#)

I dettagli completi sull'esca sono disponibili qui:

[COSA È LA CRITTOGRAFIA NEGABILE?](#)

## PASSO 2:



(I)	<TextEdit – finestra nera >	Inserire/incollare un testo cifrato
	(Font size)	Dimensione dei caratteri del testo
	(Unlock!)	Inizio dell'operazione di decifrazione

Selezionare il testo cifrato da decifrare. Il testo cifrato non sarà sovrascritto e il testo decifrato (segreto o esca, a seconda dell'insieme di password) sarà salvato nella finestra *Main Text Lock*, pronto per essere copiato e incollato.



**Numero di aspetti: (960 / Data) – 1**  
-1 a causa dell'autoaggiustamento  $\chi^2$

Noise Level	Noise	Data	Aspects
300%	720	<b>240</b>	4 - 1
400%	768	<b>192</b>	5 - 1
500%	800	<b>160</b>	6 - 1
900%	864	<b>96</b>	10 - 1
1100%	880	<b>80</b>	12 - 1
1400%	896	<b>64</b>	15 - 1
1900%	912	<b>48</b>	20 - 1
2900%	928	<b>32</b>	30 - 1
5900%	944	<b>16</b>	60 - 1

La decifrazione, anche quando le password e il testo cifrato sono corretti, può richiedere molto tempo a causa del numero di aspetti. Maggiore è il livello di rumore, più aumentano gli aspetti. MultiObfuscator, per costruzione, non conosce quale aspetto è stato selezionato al momento della cifratura e deve indovinarlo lentamente per tentativi.

[CARATTERISTICHE: ARCHITETTURA DEL PROGRAMMA](#)

[INDIETRO](#)



## RUMORE RANDOM COME ESCA (TESTO)

INIZIO:

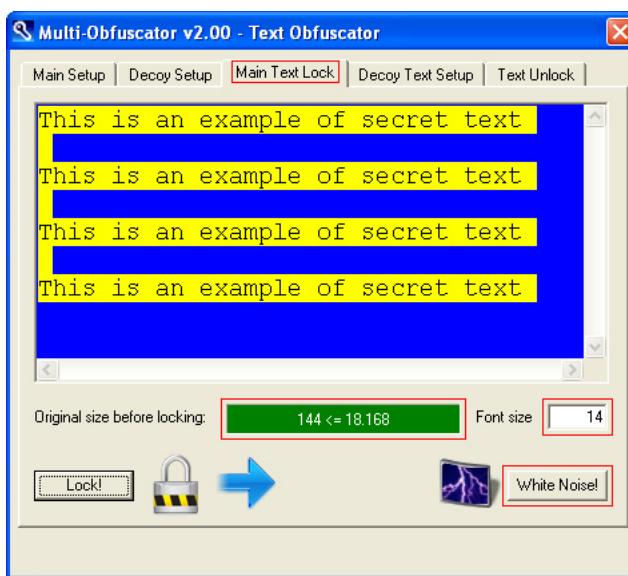


[\(Text Lock/Unlock\)](#)

Vai al pannello testo (formato email)

Selezionare *Text Lock/Unlock*.

PASSO 1:



<TextEdit – finestra blu >	Inserire/incollare un testo
(Original size before locking)	Esempio: 144 byte
(Font size)	Dimensione dei caratteri del testo
(White Noise!)	Inizio dell'operazione di randomizzazione

I testi cifrati sono statisticamente indistinguibili da quelli randomizzati. Gli utenti avanzati potranno aggiungere contenitori vuoti/fasulli a quelli sensibili, per rallentare gli attaccanti. L'operazione salverà esclusivamente rumore in un contenitore fasullo compatibile (per dimensione) con il testo selezionato.

[CARATTERISTICHE: ARCHITETTURA DEL PROGRAMMA](#)

**Esempio:**

- Livello di rumore: 900%
- Dimensione dopo la cifratura:  $((144 + 256) / 96) * 1280 = \mathbf{6.400} \text{ byte} \leq 256 \text{ Kb}$
- Dimensione del rumore random: **6.400** byte

Noise Level	Noise	Data	Min. Plain → Locked Size	Max. Plain → Locked Size
900%	864	<b>96</b>	1 B → 3840 B	18 Kb → 256 Kb

[OPZIONI: LIVELLO DI RUMORE](#)

[INDIETRO](#)