MultiObfuscator v2.00 Crittografia & Offuscamento

Sicurezza avanzata di file & testo, semplice, sicura e gratuita
EmbeddedSW © 2018
Inviate i vostri suggerimenti, commenti, segnalazioni, richieste
a *embedded@embeddedsw.net* – *Skype "embeddedsw.company"*

MultiObfuscator HomePage

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 FREE SOFTWARE:

Questo software è rilasciato con licenza LGPL 3.0

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

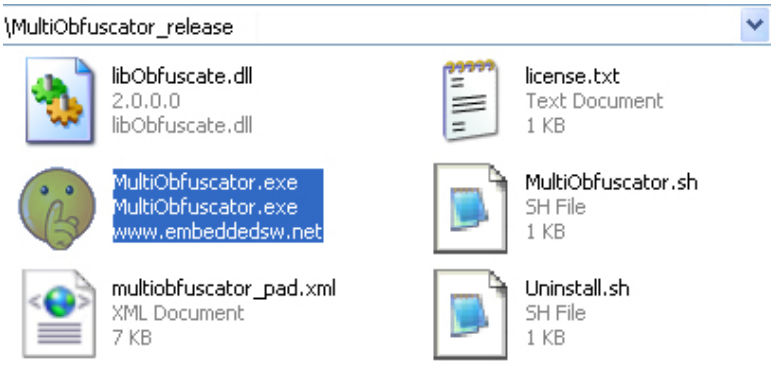
- Dovete citare l'autore (e detentore del copyright): WWW.EMBEDDEDSW.NET
- Dovete fornire un link alla Homepage dell'autore: WWW.EMBEDDEDSW.NET/MULTIOBFUSCATOR.HTML

INDIETRO

INSTALLARE MULTIOBFUSCATOR: WINDOWS

Questo programma è stato scritto per la massima privacy e compatibilità:

- APPLICAZIONE PORTABLE, non è necessaria alcuna procedura di installazione
- Nessuna dipendenza da altri software/librerie
- Supportato da WinNT fino a Win10, architetture 32bit e 64bit



Estrarre la release compressa ed eseguire OpenPuff.exe

Accesso diretto al pannello pricincipale

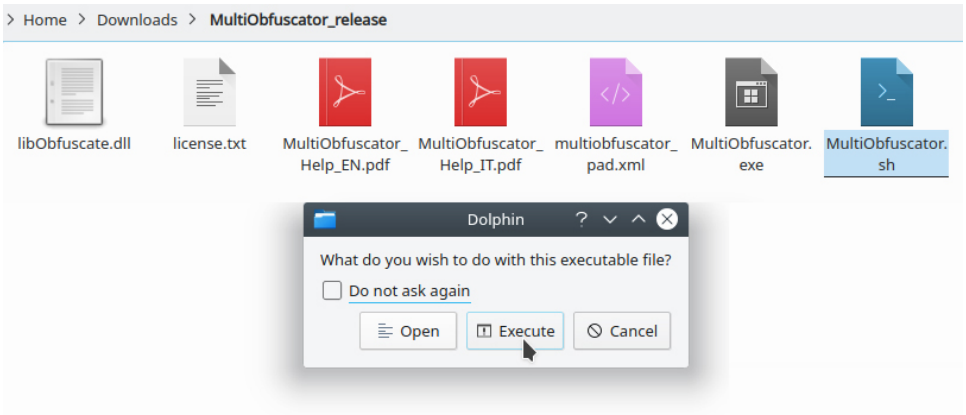
INDIETRO

INSTALLARE MULTIOBFUSCATOR: LINUX

Questo programma è stato scritto per la massima privacy e compatibilità:

- La sola dipendenza è WINE
- Shell automatizzato per installare/eseguire in UBUNTU (*MultiObfuscator.sh*)
- Shell automatizzato per disinstallare/cleanup in Ubuntu (*Uninstall.sh*)

INSTALLARE/ESEGUIRE:



Estrarre la release compressa ed eseguire MultiObfuscator.sh

```
user@user:~/Downloads/MultiObfuscator_release$ ./MultiObfuscator.sh
```

Si può eseguire MultiObfuscator.sh a riga di comando

WINE NON INSTALLATO:

In caso Wine non sia installato nel vostro sistema, lo shell automatizzato vi avviserà.
Premere [y] per confermare l'installazione di Wine e continuare.

```
Wine is required to run MultiObfuscator. Install now? [y/n]
```

Confermare [y] per accettare di installare Wine e continuare

```
0 upgraded, 145 newly installed, 0 to remove and 0 not upgraded.
Need to get 96,3 MB of archives.
After this operation, 716 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Confermare [y] per consentire a linux il download e l'installazione da internet dei package richiesti

```
Selecting previously unselected package libjpeg-turbo8:i386.
Preparing to unpack .../006-libjpeg-turbo8_1.5.2-0ubuntu5.18.04.1_i386.deb ...
Unpacking libjpeg-turbo8:i386 (1.5.2-0ubuntu5.18.04.1) ...
Selecting previously unselected package libogg0:i386.
Preparing to unpack .../007-libogg0_1.3.2-1_i386.deb ...
Unpacking libogg0:i386 (1.3.2-1) ...
Selecting previously unselected package libxinerama1:i386.
Preparing to unpack .../008-libxinerama1_2%3a1.1.3-1_i386.deb ...
Unpacking libxinerama1:i386 (2:1.1.3-1) ...

Progress: [  3%] [###.....................................................
```

Attendere fino al 100%

```
Setting up libtheora0:i386 (1.1.1+dfsg.1-14) ...
Setting up libglx0:i386 (1.0.0-2ubuntu2.1) ...
Setting up gstreamer1.0-plugins-base:i386 (1.14.1-1ubuntu1~ubuntu18.04.1) ...
Setting up wine32:i386 (3.0-1ubuntu1) ...
Setting up libgl1:i386 (1.0.0-2ubuntu2.1) ...
Setting up libglu1-mesa:i386 (9.0.0-2.1build1) ...
Setting up libgl1-mesa-glx:i386 (18.0.5-0ubuntu0~18.04.1) ...
Processing triggers for libc-bin (2.27-3ubuntu1) ...
Processing triggers for wine-stable (3.0-1ubuntu1) ...
Now run ./MultiObfuscator.sh
user@user:~/Downloads/MultiObfuscator_release$
```

Wine è stato installato con successo. Eseguire MultiObfuscator.sh nuovamente

WINE INSTALLATO:

La prima esecuzione di Wine + MultiObfuscator può richiedere tempo per configurare l'ambiente Wine.

```
user@user:~/Downloads/MultiObfuscator_release$ ./MultiObfuscator.sh
** Starting Wine + MultiObfuscator. **
** If this is the first time you run MultiObfuscator, it may take some time to initialize. **
wine: created the configuration directory '/home/user/.wine'
0012:err:ole:marshal_object couldn't get IPSFactory buffer for interface {00000131-0000-0000-c000-000000000046}
0012:err:ole:marshal_object couldn't get IPSFactory buffer for interface {6d5140c1-7436-11ce-8034-00aa006009fa}
0012:err:ole:StdMarshalImpl_MarshalInt                                    ub, hres=0x80004002
0012:err:ole:CoMarshalInterface Failed                                    d5140c1-7436-11ce-8034-00aa006009fa}, 80004002
0012:err:ole:get_local_server_stream F
0014:err:ole:marshal_object couldn't g                                    erface {00000131-0000-0000-c000-000000000046}
0014:err:ole:marshal_object couldn't g                                    erface {6d5140c1-7436-11ce-8034-00aa006009fa}
0014:err:ole:StdMarshalImpl_MarshalInterface Failed to create ifstub, hres=0x80004002
0014:err:ole:CoMarshalInterface Failed to marshal the interface {6d5140c1-7436-11ce-8034-00aa006009fa}, 80004002
0014:err:ole:get_local_server_stream Failed: 80004002
```

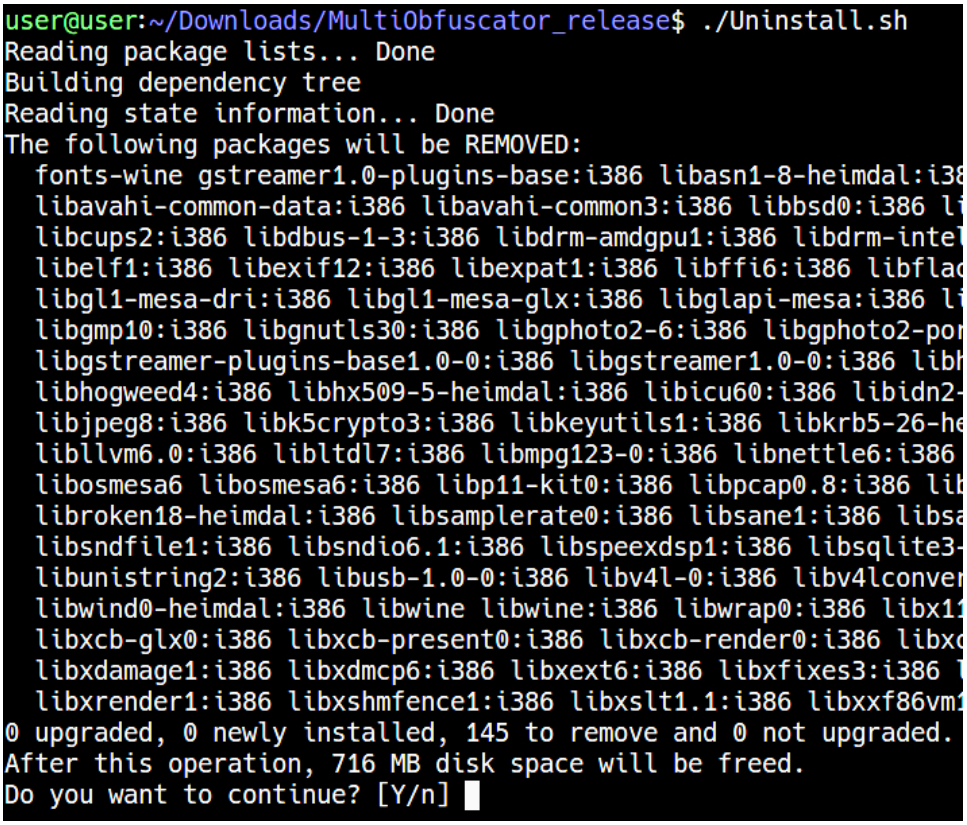

Wine richiede tempo per configurare l'ambiente, alla prima esecuzione di MultiObfuscator.sh

Accesso diretto al pannello pricincipale

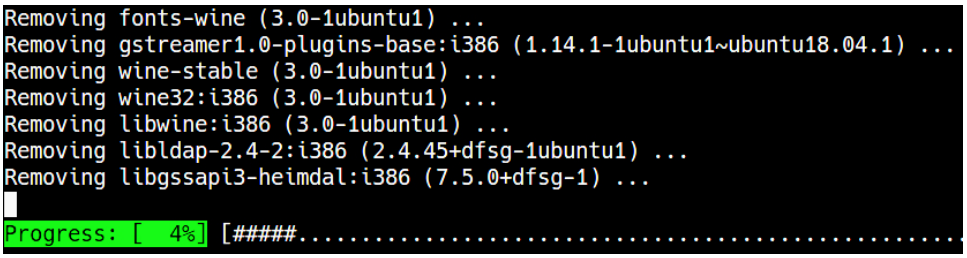
DISINSTALLARE/CLEANUP

Per rimuovere completamente questo programma, assicuratevi di eseguire lo shell automatizzato:

- Rimuovendo le impostazioni di Wine (*~/.wine*)
- Disinstallando Wine e i package dipendenti



Eseguire Uninstall.sh e confermare [y] per consentire a linux la disinstallazione



Attendere fino al 100%

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 CRITTORGRAFIA NEGABILE

- MultiObfuscator supporta dati e un'esca (un primo livello di crittografia negabile)
- MultiObfuscator non può, per costruzione, ricostruire l'associazione *Dati* ↔ *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.

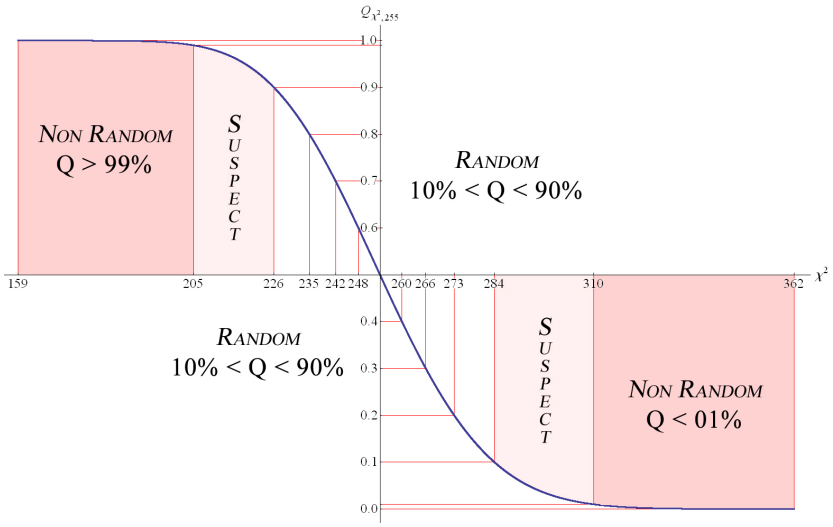
Rubberhose *è stato* (a causa dell'abbandono) un progetto avanzato che ha introdotto nuovi concetti

- 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-χ^2:

- eccede la DISTRIBUZIONE-χ^2 il 50% delle volte (Q = 0.5), come un vera sequenza random creata da EVENTI DI DECADIMENTO RADIATTIVO
- ottiene un punteggio ≥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 crittorgrafia 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.

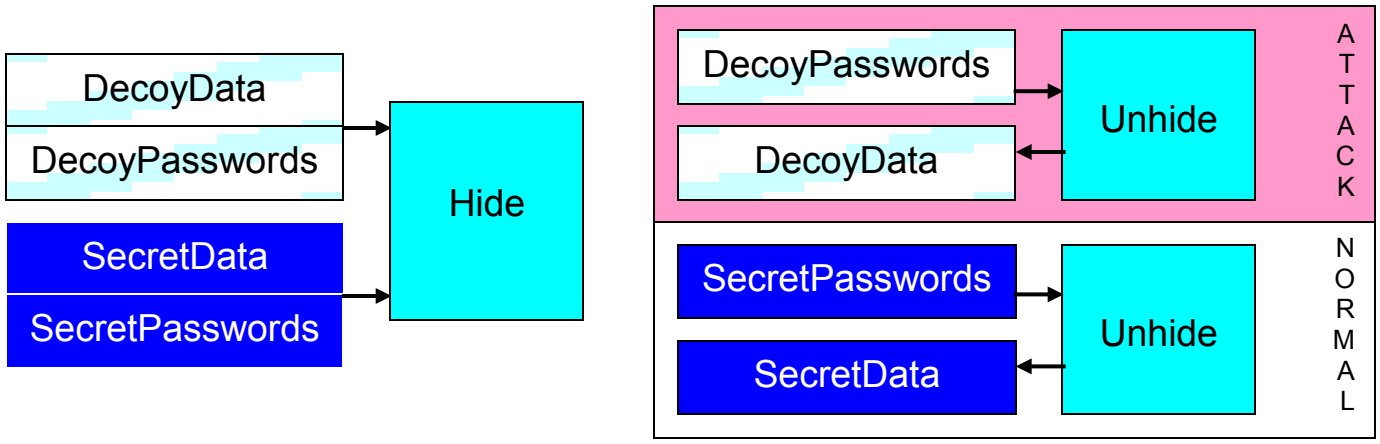
MultiObfuscator si basa unicamente sulla moderna crittografia stabile e open-source.

CARATTERISTICHE: ARCHITETTURA DEL PROGRAMMA

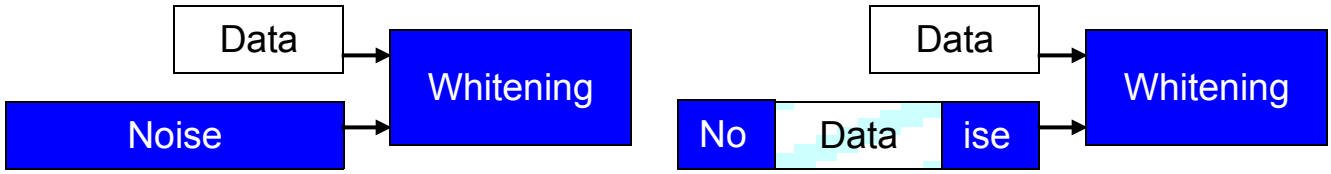
INDIETRO

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.



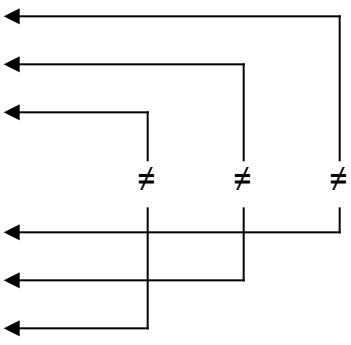
Come è possibile? I dati crittografati e sottoposti a scrambling, sono sottoposti a whitening (CARATTERISTICHE: ARCHITETTURA DEL PROGRAMMA) con una grande quantità di rumore. I dati esca possono sostituire un po' del rumore senza compromettere le proprietà finali di RESISTENZA ALLA CRITTANALISI.



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

Esempio:

Sensibile data: Password (A) "*FirstDataPssw1*"
Password (B) "*SecondDataPssw2*"
Password (C) "*AnotherDataPssw3*"
(A ∩ B) 70%, (A ∩ C) 67%, (B ∩ C) 68%, HAMMING DISTANCE ≥ 25%



Decoy data: Password (A') "*FirstDecoyPssw1*"
Password (B') "*SecondDecoyPssw2*"
Password (C') "*AnotherDecoyPssw3*"
(A' ∩ B') 72%, (A' ∩ C') 60%, (B' ∩ C') 70%, Hamming distance ≥ 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
  $\sum_{k \in \{1, N-1\}} used\_bytes(whiteBlock_k) < Sizeof(Decoy) \leq \sum_{k \in \{1, N\}} used\_bytes(whiteBlock_k)$

Esempio:

Carriers	Carrier bytes	SensibleData	DecoyData
+Carr (1/N)	32	X	Used
…	2688	X	Used
+Carr (N-1/N)	48	X	Used
+Carr (N/N)	**64**		**Not used**
	Total = 2832	Total = 2795	2720 < Size ≤ 2768

INDIETRO

OPZIONI: LIVELLO DI RUMORE

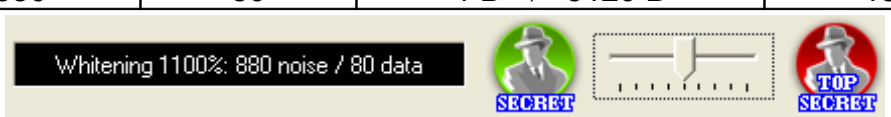
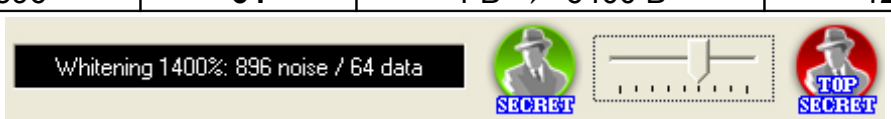
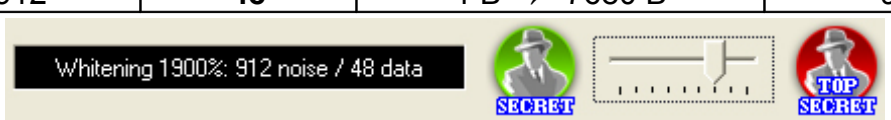
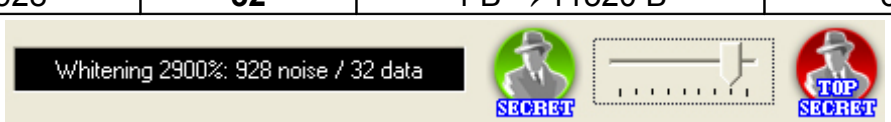
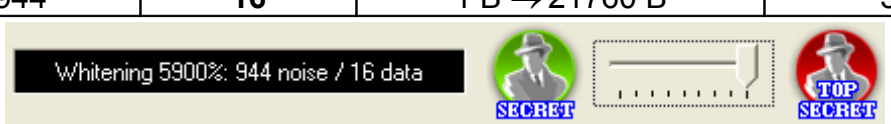
MODALITÀ FILE:

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

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

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

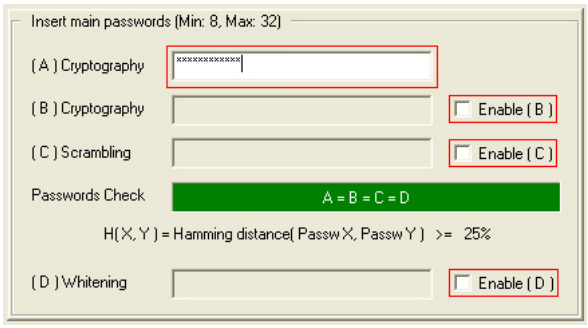
Noise Level	Noise	Data	Min. Plain → Locked Size	Max. Plain → Locked Size
300%	720	**240**	1 B → 2560 B	46 Kb → 256 Kb
				
400%	768	**192**	1 B → 2560 B	36 Kb → 256 Kb
				
500%	800	**160**	1 B → 2560 B	30 Kb → 256 Kb
				
900%	864	**96**	1 B → 3840 B	18 Kb → 256 Kb
				
1100%	880	**80**	1 B → 5120 B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

INDIETRO

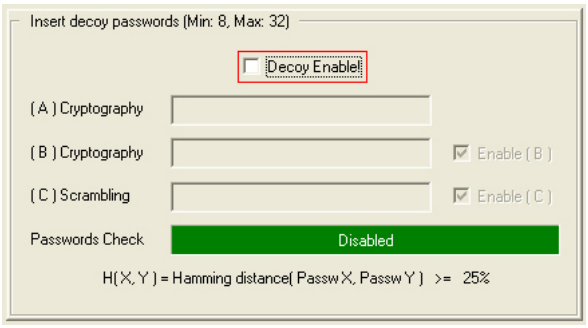
SETUP DELLE PASSWORD SEMPLICE

SEMPLICE — CIFRATURA/DEFICFRAZIONE FILE/TESTO – SETUP DI BASE (1 PASSWORD)

(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

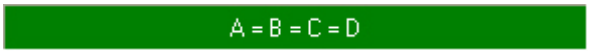
B.1) Disabilitare le password (Main_B / Main_C / Main_D)
B.2) Inserire una password (Main_A) qualsiasi

Le password (Main_B / Main_C / Main_D) disabilitate diventeranno uguali alla password (Main_A)!

VINCOLI:

1) Length (Main_A) ≥ 8

ESEMPIO:



Main: ok

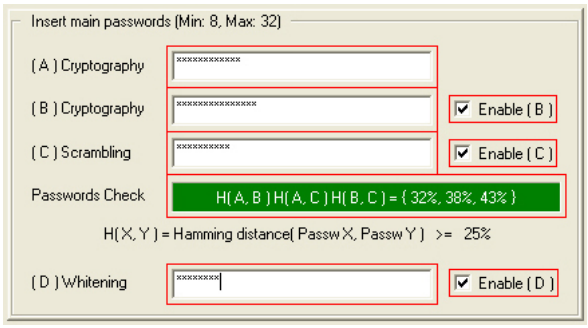
Main_A = "any password"

INDIETRO

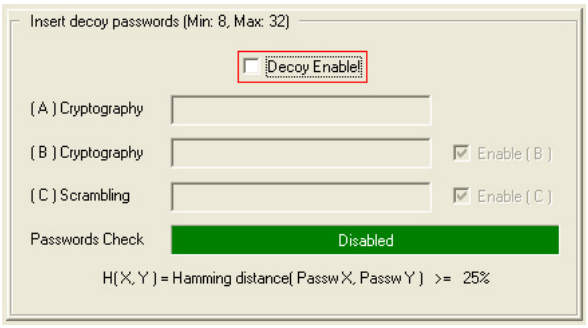
SETUP DELLE PASSWORD MEDIO

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

(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

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) ≥ 8
1.2) Enabled? (Main_B) → Length (Main_B) ≥ 8
1.3) Enabled? (Main_C) → Length (Main_C) ≥ 8
1.4) Enabled? (Main_D) → Length (Main_D) ≥ 8

2.1) Enabled? (Main_B) → HAMMING DISTANCE (Main_A / Main_B) ≥ 25%
2.2) Enabled? (Main_C) → Hamming distance (Main_A / Main_C) ≥ 25%
2.3) Enabled? (Main_B / Main_C) → Hamming distance (Main_B / Main_C) ≥ 25%

ESEMPIO:

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”

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”

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”

Main: ok

Main_A = “some_crypt_a”
Main_B = “another_crypt_b”
Main_C = “scramble_c”
Main_D = “whiten_d”

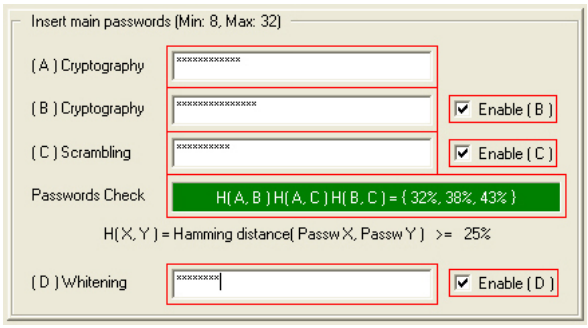
INDIETRO

SETUP DELLE PASSWORD AVANZATO – CIFRATURA

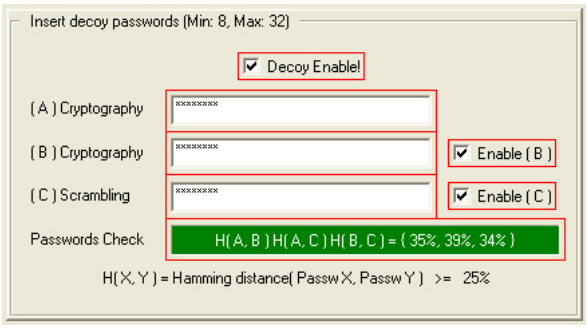
ESPERTO

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

(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

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

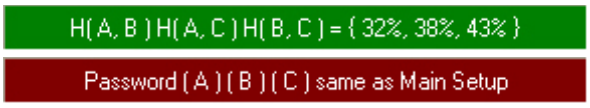
Le password (Decoy_B / Decoy_C) disabilitate diventeranno uguali alla password (Decoy_A)!

VINCOLI:

1.1)			Length (Main_A) ≥ 8
1.2)	Enabled? (Main_B)	→	Length (Main_B) ≥ 8
1.3)	Enabled? (Main_C)	→	Length (Main_C) ≥ 8
1.4)	Enabled? (Main_D)	→	Length (Main_D) ≥ 8
2.1)	Enabled? (Main_B)	→	HAMMING DISTANCE (Main_A / Main_B) ≥ 25%
2.2)	Enabled? (Main_C)	→	Hamming distance (Main_A / Main_C) ≥ 25%
2.3)	Enabled? (Main_B / Main_C)	→	Hamming distance (Main_B / Main_C) ≥ 25%
3.1)			Length (Decoy_A) ≥ 8
3.2)	Enabled? (Decoy_B)	→	Length (Decoy_B) ≥ 8
3.3)	Enabled? (Decoy_C)	→	Length (Decoy_C) ≥ 8
4.1)	Enabled? (Decoy_B)	→	Hamming distance (Decoy_A / Decoy_B) ≥ 25%
4.2)	Enabled? (Decoy_C)	→	Hamming distance (Decoy_A / Decoy_C) ≥ 25%
4.3)	Enabled? (Decoy_B / Decoy_C)	→	Hamming distance (Decoy_B / Decoy_C) ≥ 25%

5.1)	Enabled? (Decoy_B)	→ Enabled? (Main_B)	→ Main_B ≠ Decoy_B
5.2)	Enabled? (Decoy_B)	→ Disabled? (Main_B)	→ Main_A ≠ Decoy_B
5.3)	Enabled? (Decoy_C)	→ Enabled? (Main_C)	→ Main_C ≠ Decoy_C
5.4)	Enabled? (Decoy_C)	→ Disabled? (Main_C)	→ Main_A ≠ Decoy_C

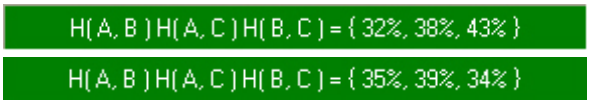
ESEMPIO:



Main: ok

Decoy: Main_A = Decoy_A, …

Main_A = “some_crypt_a” Decoy_A = “**some_crypt_a**”
Main_B = “another_crypt_b” Decoy_B = “**another_crypt_b**”
Main_C = “scramble_c” Decoy_C = “**scramble_c**”
Main_D = “whiten_d”



Main: ok

Decoy: Main_A = Decoy_A, …

Main_A = “some_crypt_a” Decoy_A = “12345678”
Main_B = “another_crypt_b” Decoy_B = “qwertyui”
Main_C = “scramble_c” Decoy_C = “zxcvbnm,”
Main_D = “whiten_d”

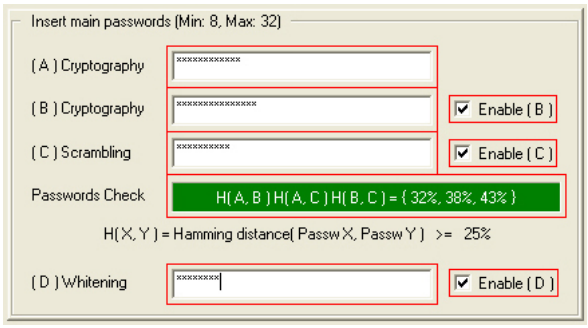
INDIETRO

SETUP DELLE PASSWORD AVANZATO – DECIFRAZIONE

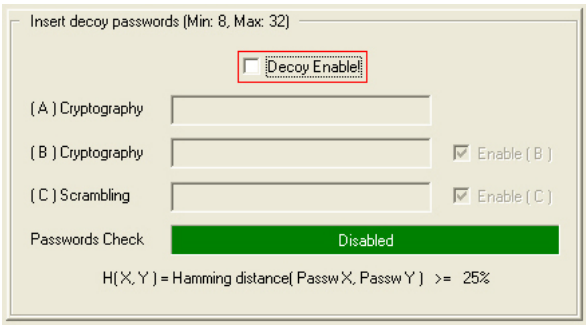
ESPERTO

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

(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

ESEMPIO:

Cifratura	
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,"
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*

Cifratura	
Main_A = “some_crypt_a” Main_B = **DISABLED** Main_C = “scramble_c” Main_D = “whiten_d”	Decoy_A = “12345678” Decoy_B = “qwertyui” Decoy_C = **DISABLED**
Decifrazione dei dati segreti	
Main_A = “some_crypt_a” Main_B = **DISABLED** Main_C = “scramble_c” Main_D = “whiten_d”	DISABLED
Decifrazione dell’esca	
Main_A = “12345678” Main_B = “qwertyui” Main_C = **DISABLED** Main_D = “whiten_d”	DISABLED

OK *Si possono disabilitare le password Main_B / Main_C / Decoy_B / Decoy_C indipendentemente*

Cifratura	
Main_A = “some_crypt_a” Main_B = DISABLED Main_C = “scramble_c” Main_D = **DISABLED**	Decoy_A = “12345678” Decoy_B = “qwertyui” Decoy_C = DISABLED
Decifrazione dei dati segreti	
Main_A = “some_crypt_a” Main_B = DISABLED Main_C = “scramble_c” Main_D = DISABLED	DISABLED
Decifrazione dell’esca	
Main_A = “12345678” Main_B = “qwertyui” Main_C = DISABLED Main_D = “**some_crypt_a**”	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

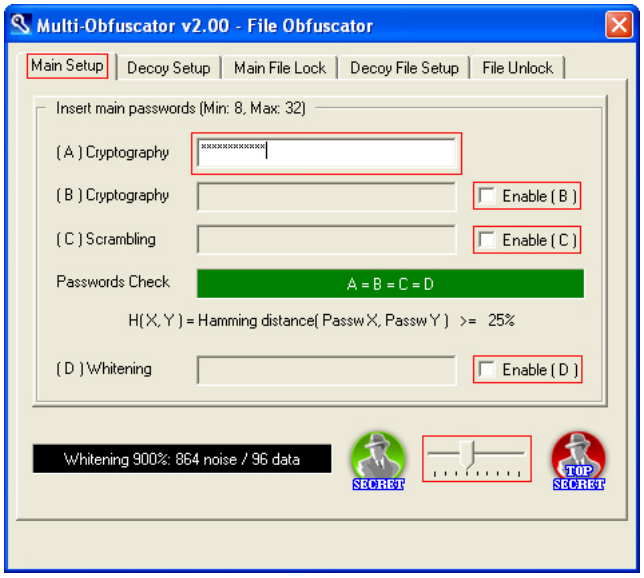
SEMPLICE  **CIFRATURA FILE – SETUP DI BASE (1 PASSWORD)**

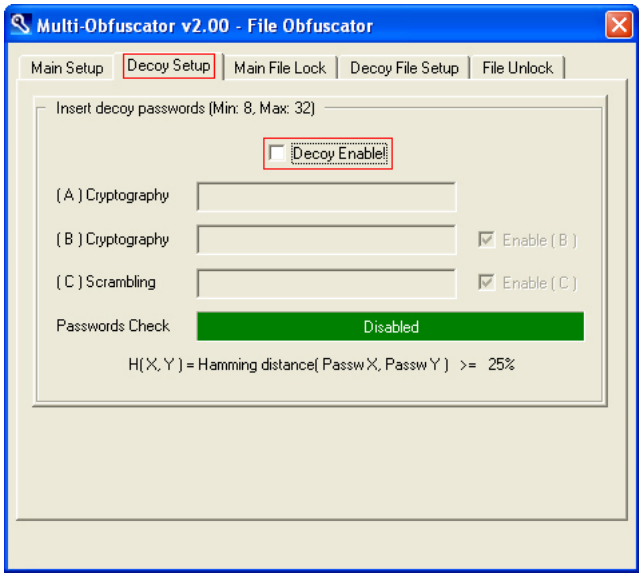
INIZIO:

(*File Lock/Unlock*)	Vai al pannello file (formato binario raw)

Selezionare *File Lock/Unlock*.

PASSO 1 – SCELTA DELLA PASSWORD:

(I) 

(II) 

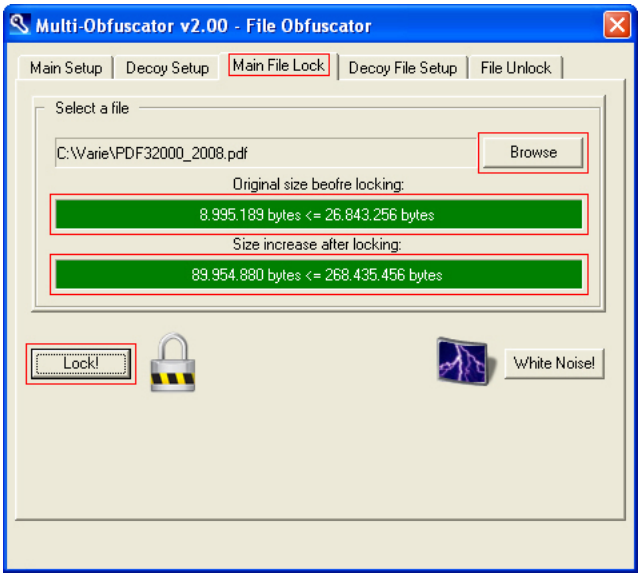
(I)	(*Cryptography A*)	La prima password
	(*Enable B*)	Abilita/disabilita la seconda password
	(*Enable C*)	Abilita/disabilita la terza password
	(*Enable D*)	Abilita/disabilita la quarta password
(II)	(*Decoy Enable!*)	Abilita/disabilita l'esca

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 – SCELTA DEI DATI:



(*Browse*)	Selezionare un file
(*Original size before locking*)	Esempio: 8.995.189
(*Size increase after locking*)	Esempio: 89.954.880
(*Lock!*)	Inizio della 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	**96**	1 B → 2880 B	**25 Mb → 256 Mb**

OPZIONI: LIVELLO DI RUMORE

INDIETRO

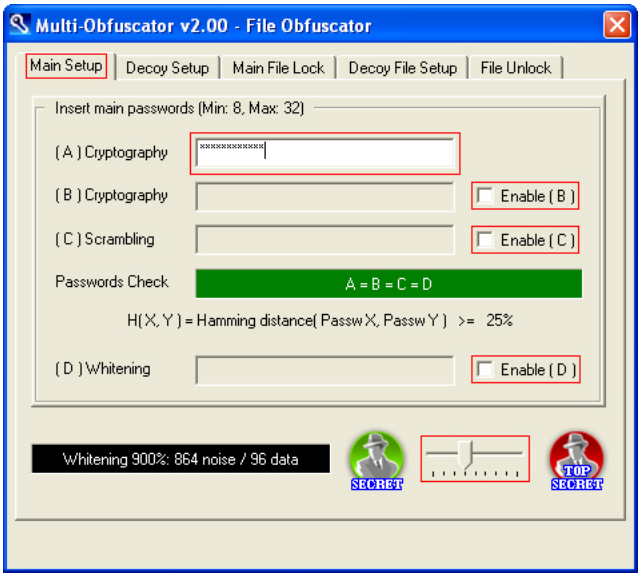
DECIFRAZIONE FILE – SETUP DI BASE (1 PASSWORD)

INIZIO:

(*File Lock/Unlock*)	Vai al pannello file (formato binario raw)

Selezionare *File Lock/Unlock*.

PASSO 1 – SCELTA DELLA PASSWORD:

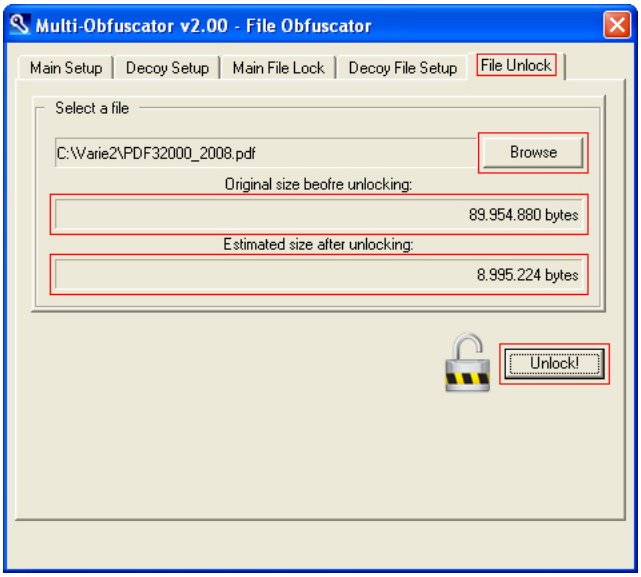


(*Cryptography A*)	La prima password
(*Enable B*)	Abilita/disabilita la seconda password
(*Enable C*)	Abilita/disabilita la terza password
(*Enable D*)	Abilita/disabilita la quarta password

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:

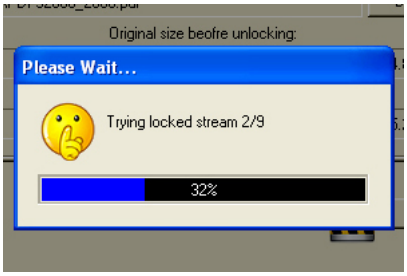
- SETUP DELLE PASSWORD SEMPLICE
- OPZIONI: LIVELLO DI RUMORE

PASSO 2 – SCELTA DEI DATI:



(*Browse*)	Selezionare un file cifrato
(*Original size before unlocking*)	Esempio: 89.954.880
(*Estimated size after unlocking*)	Esempio: 8.995.224
(*Unlock!*)	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 χ^2

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

MEDIO		CIFRATURA FILE – SETUP MEDIO (4 PASSWORD)

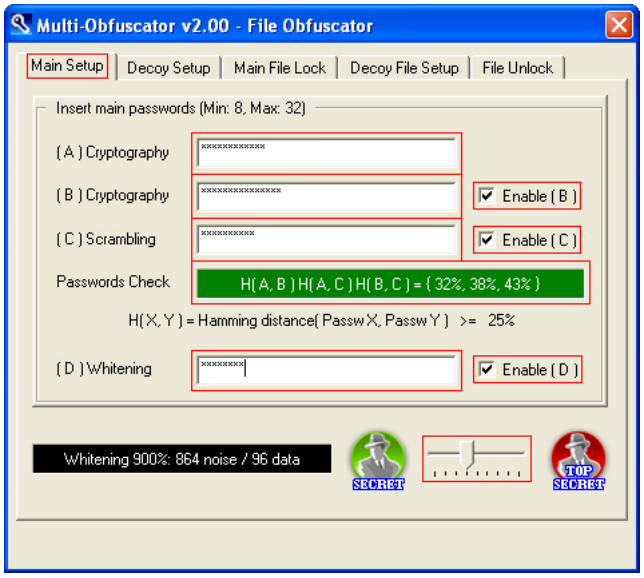
INIZIO:

(*File Lock/Unlock*)	Vai al pannello file (formato binario raw)

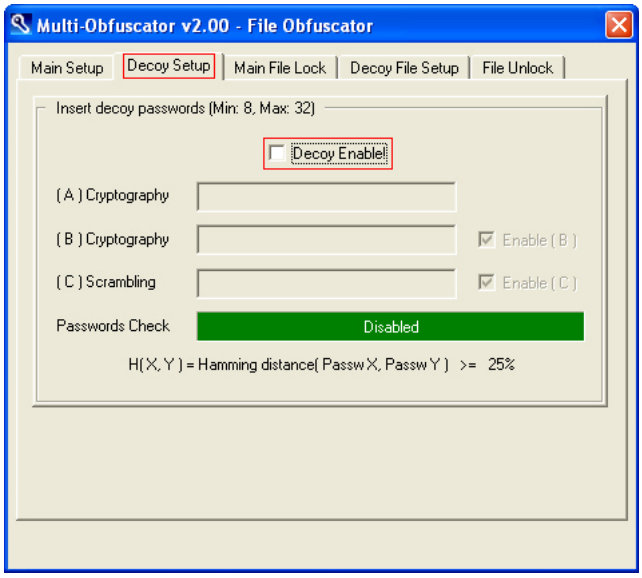
Selezionare *File Lock/Unlock*.

PASSO 1 – SCELTA DELLE PASSWORD:

(I)



(II)



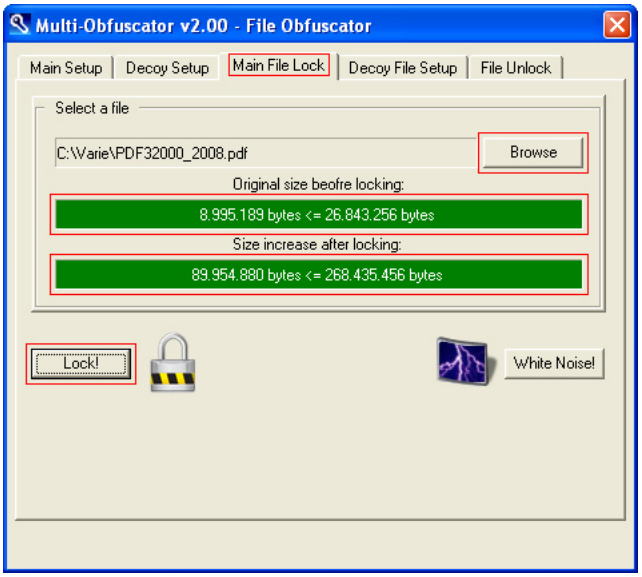
(I)	(*Cryptography A*)	La prima password (chiavi crittografiche)
	(*Cryptography B*)	La seconda password (CSPRNG crittografico)
	(*Scrambling C*)	La terza password (CSPRNG scrambling)
	(*Whitening D*)	La quarta password (CSPRNG whitening)
	(*Enable B*)	Abilita/disabilita la seconda password
	(*Enable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

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 – SCELTA DEI DATI:



(*Browse*)	Selezionare un file
(*Original size before locking*)	Esempio: 8.995.189
(*Size increase after locking*)	Esempio: 89.954.880
(*Lock!*)	Inizio della 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	**96**	1 B → 2880 B	**25 Mb → 256 Mb**

OPZIONI: LIVELLO DI RUMORE

INDIETRO

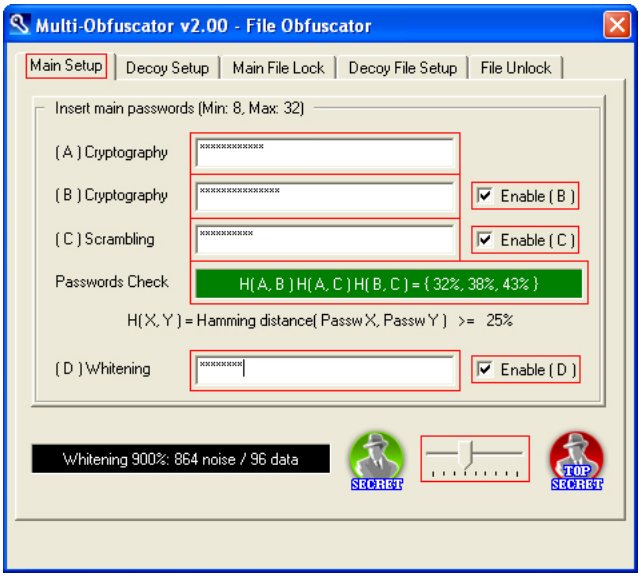
DECIFRAZIONE FILE – SETUP MEDIO (4 PASSWORD)

INIZIO:

(*File Lock/Unlock*)	Vai al pannello file (formato binario raw)

Selezionare *File Lock/Unlock*.

PASSO 1 – SCELTA DELLE PASSWORD:

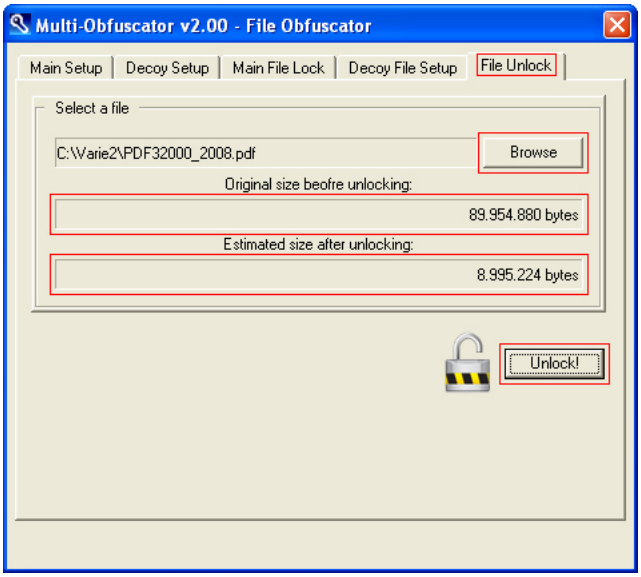


(*Cryptography A*)	La prima password (chiavi crittografiche)
(*Cryptography B*)	La seconda password (CSPRNG crittografico)
(*Scrambling C*)	La terza password (CSPRNG scrambling)
(*Whitening D*)	La quarta password (CSPRNG whitening)
(*Enable B*)	Abilita/disabilita la seconda password
(*Enable C*)	Abilita/disabilita la terza password
(*Enable D*)	Abilita/disabilita la quarta password

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:

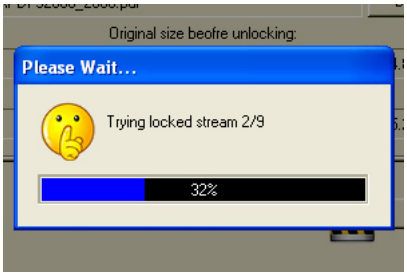
- SETUP DELLE PASSWORD MEDIO
- OPZIONI: LIVELLO DI RUMORE

PASSO 2 – SCELTA DEI DATI:



(*Browse*)	Selezionare un file cifrato
(*Original size before unlocking*)	Esempio: 89.954.880
(*Estimated size after unlocking*)	Esempio: 8.995.224
(*Unlock!*)	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 χ^2

Noise Level	Noise	Data	Aspects
300%	720	**240**	4 - 1
400%	768	**192**	5 - 1
500%	800	**160**	6 - 1
900%	864	**96**	10 - 1
1100%	880	**80**	12 - 1
1400%	896	**64**	15 - 1
1900%	912	**48**	20 - 1
2900%	928	**32**	30 - 1
5900%	944	**16**	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 AVANZATO (4 PASSWORD+ESCA)

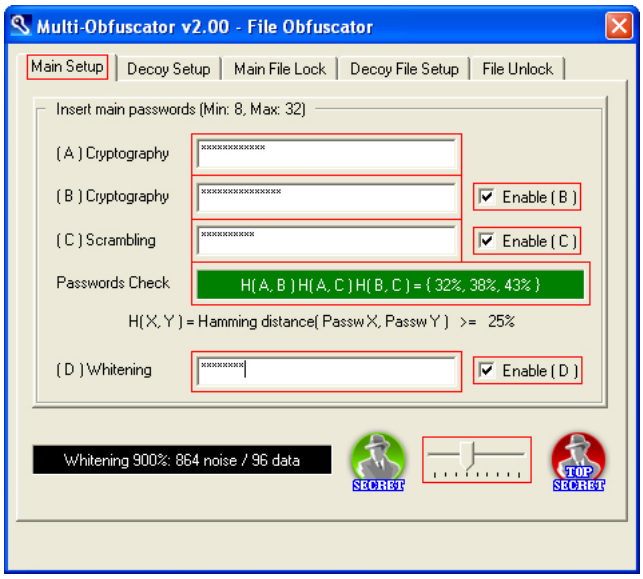
INIZIO:

(*File Lock/Unlock*)	Vai al pannello file (formato binario raw)

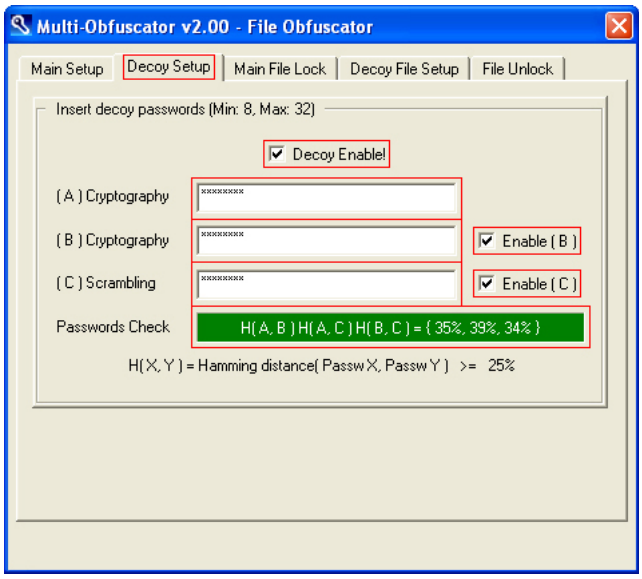
Selezionare *File Lock/Unlock*.

PASSO 1 – SCELTA DELLE PASSWORD:

(I)



(II)



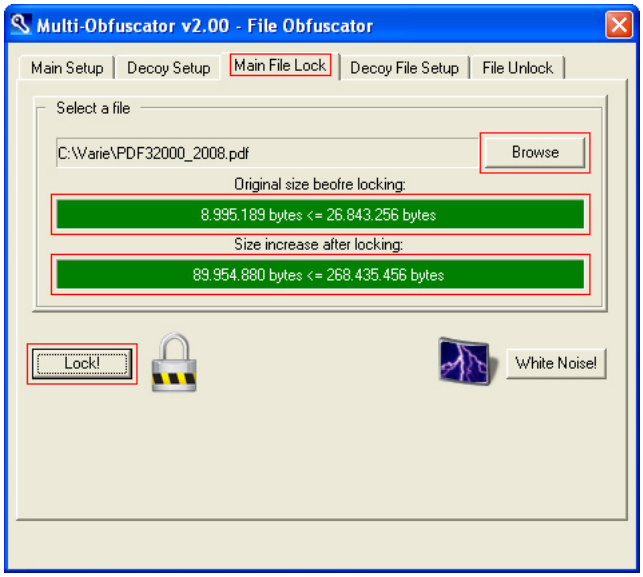
(I)	(*Cryptography A*)	La prima password (chiavi crittografiche)
	(*Cryptography B*)	La seconda password (CSPRNG crittografico)
	(*Scrambling C*)	La terza password (CSPRNG scrambling)
	(*Whitening D*)	La quarta password (CSPRNG whitening)
	(*Enable B*)	Abilita/disabilita la seconda password
	(*Enable 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:

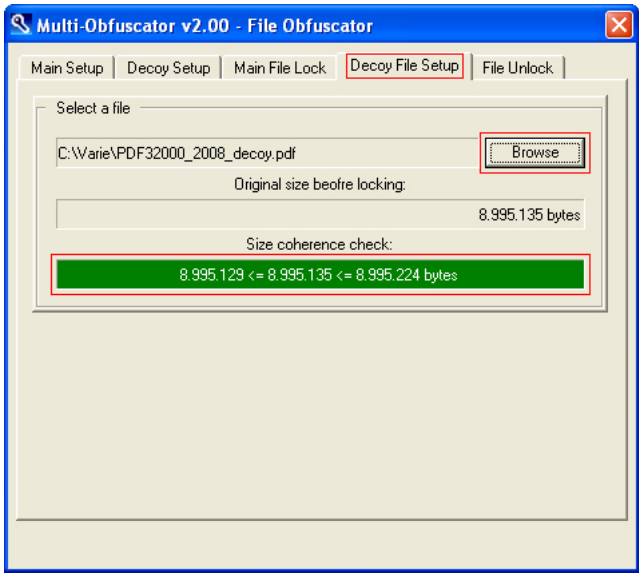
- SETUP DELLE PASSWORD AVANZATO – CIFRATURA
- OPZIONI: LIVELLO DI RUMORE
- CARATTERISTICHE: ARCHITETTURA DEL PROGRAMMA

PASSO 2 – SCELTA DEI DATI:

(I)



(II)



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

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 ≤ 25 Mb
- Dimensione dopo la cifratura: ((8.995.189 + 256) / 96) * 960 = 89.954.880 byte ≤ 256 Mb
- Dimensione dell'esca: (((8.995.129 ≤ x ≤ 8.995.224) + 256) / 96) * 960 = 89.954.880 byte ≤ 256 Mb

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

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%) → *Data = 240* → *inf ≤ x ≤ sup* → *sup - inf + 1 = 240 bytes*
Maximum (5900%) → *Data = 16* → *inf ≤ x ≤ sup* → *sup - inf + 1 = 16 bytes*

Assicurarsi di leggere anche la sezione intermedia
CIFRATURA FILE – SETUP MEDIO (4 PASSWORD)

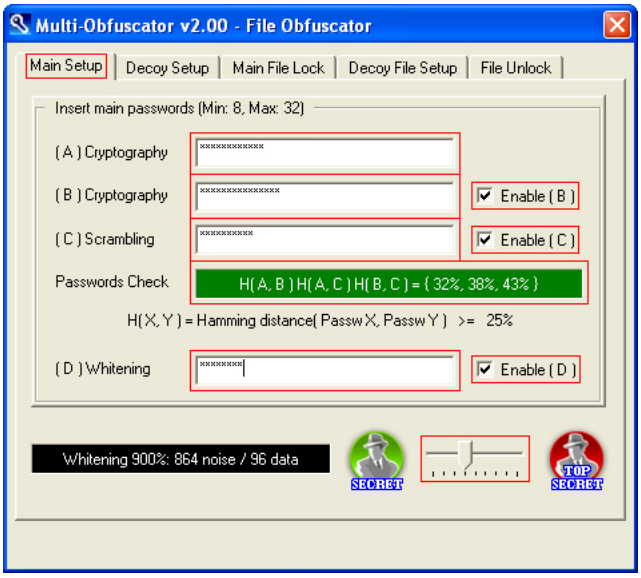
INDIETRO

INIZIO:

(*File Lock/Unlock*)	Vai al pannello file (formato binario raw)

Selezionare *File Lock/Unlock*.

PASSO 1 – SCELTA DELLE PASSWORD:



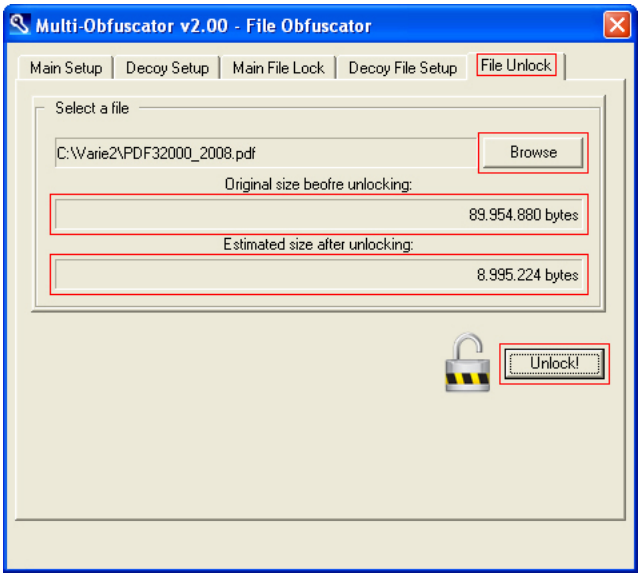
(*Cryptography A*)	La prima password (chiavi crittografiche)
(*Cryptography B*)	La seconda password (CSPRNG crittografico)
(*Scrambling C*)	La terza password (CSPRNG scrambling)
(*Whitening D*)	La quarta password (CSPRNG whitening)
(*Enable B*)	Abilita/disabilita la seconda password
(*Enable C*)	Abilita/disabilita la terza password
(*Enable D*)	Abilita/disabilita la quarta password

Impostare lo stesso insieme di password (segrete 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

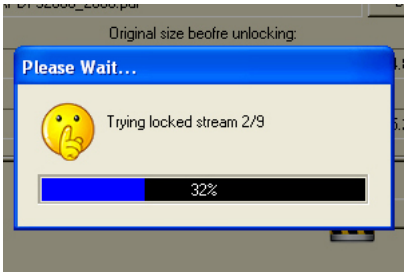
I dettagli completi sull'esca sono disponibili qui:
COSA È LA CRITTOGRAFIA NEGABILE?

PASSO 2 – SCELTA DEI DATI:



(*Browse*)	Selezionare un file cifrato
(*Original size before unlocking*)	Esempio: 89.954.880
(*Estimated size after unlocking*)	Esempio: 8.995.224
(*Unlock!*)	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 χ^2

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

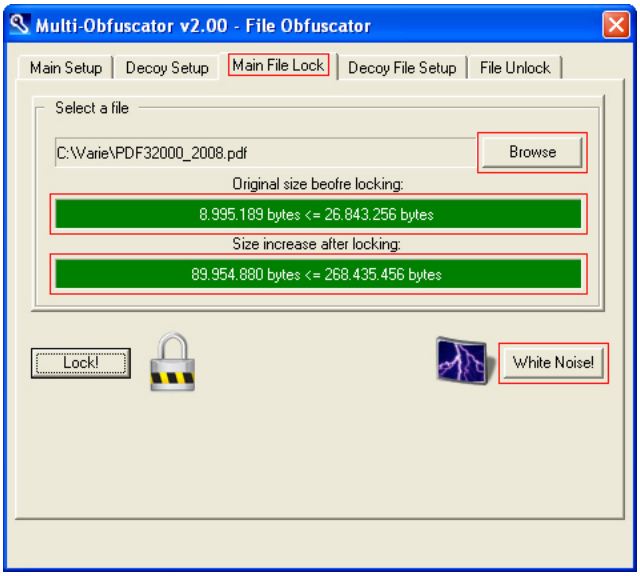
ESPERTO    **RUMORE RANDOM COME ESCA (FILE)**

INIZIO:

(*File Lock/Unlock*)	Vai al pannello file (formato binario raw)

Selezionare *File Lock/Unlock*.

PASSO 1 – SCELTA DEI DATI:



(*Browse*)	Selezionare un file
(*Original size before locking*)	Esempio: 8.995.189
(*Size increase after locking*)	Esempio: 89.954.880
(*White Noise!*)	Inizio 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 = **89.954.880** byte ≤ 256 Mb
- Dimensione del rumore random: **89.954.880** byte

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

OPZIONI: LIVELLO DI RUMORE

INDIETRO

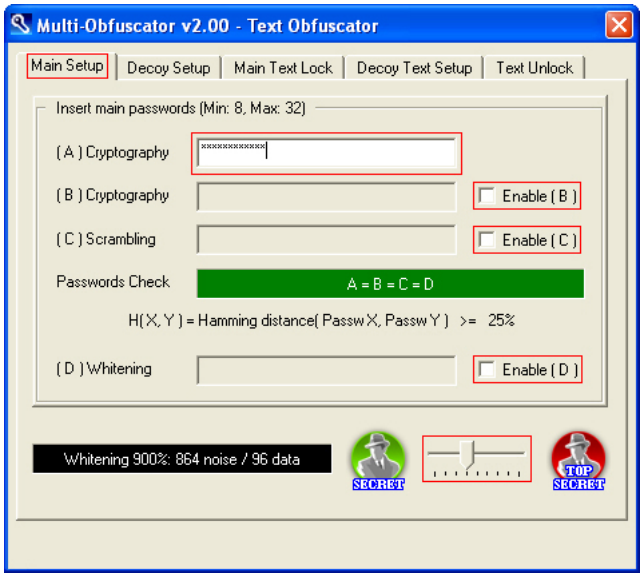
SEMPLICE  **CIFRATURA TESTO – SETUP DI BASE (1 PASSWORD)**

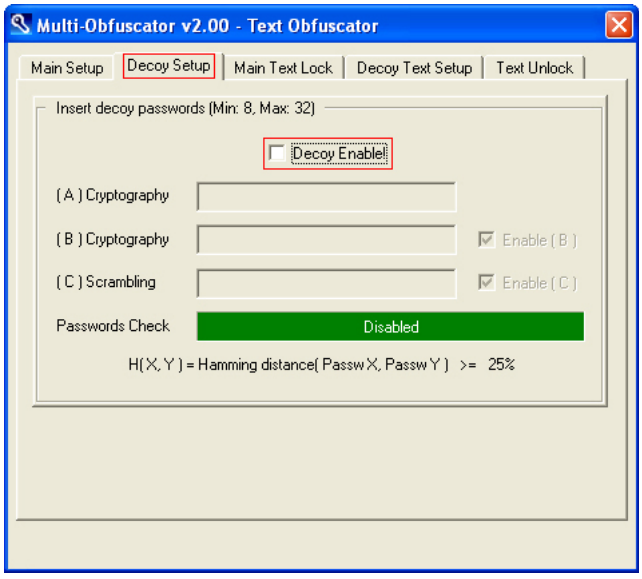
INIZIO:

(*Text Lock/Unlock*)	Vai al pannello testo (formato email)

Selezionare *Text Lock/Unlock*.

PASSO 1 – SCELTA DELLA PASSWORD:

(I) 

(II) 

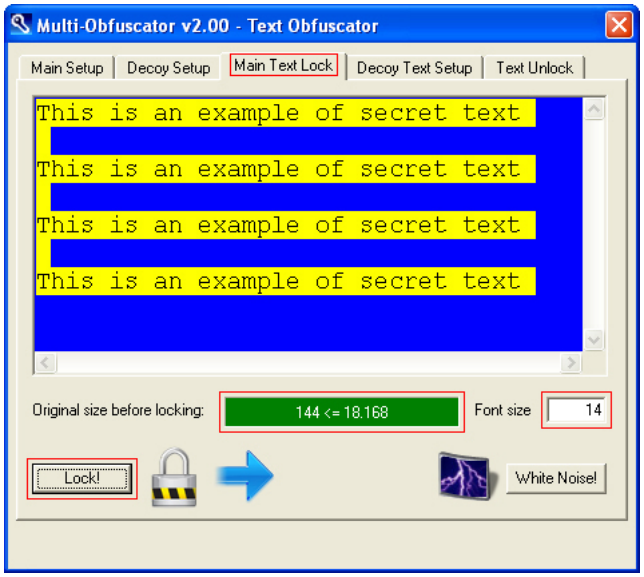
(I)	(*Cryptography A*)	La prima password
	(*Enable B*)	Abilita/disabilita la seconda password
	(*Enable C*)	Abilita/disabilita la terza password
	(*Enable D*)	Abilita/disabilita la quarta password
(II)	(*Decoy Enable!*)	Abilita/disabilita l'esca

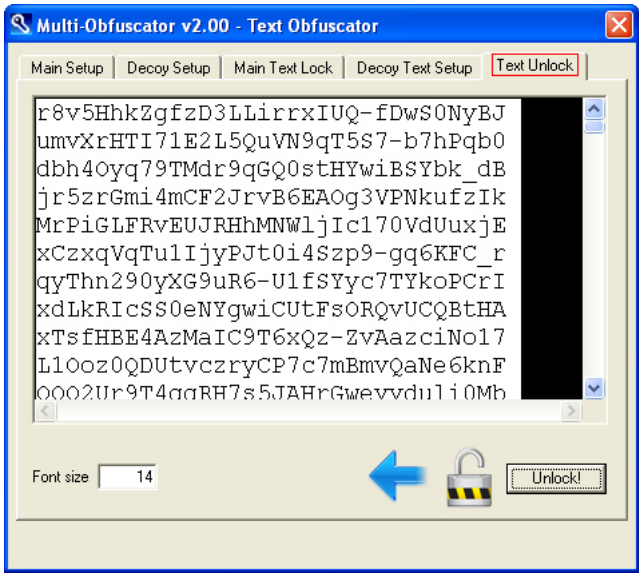
Inserire una password e selezionare un livello di rumore. I dettagli completi su password e rumore sono disponibili in speciali sezioni separate:

- 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 – SCELTA DEL TESTO:

(I) 

(II) 

(I)	< TextEdit – finestra blu >	Inserire/incollare un testo
	(*Original size before locking*)	Esempio: 144
	(*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 ≤ 18 Kb
- Dimensione dopo la cifratura: ((144 + 256) / 96) * 1280 = 6.400 byte ≤ 256 Kb

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

OPZIONI: LIVELLO DI RUMORE

INDIETRO

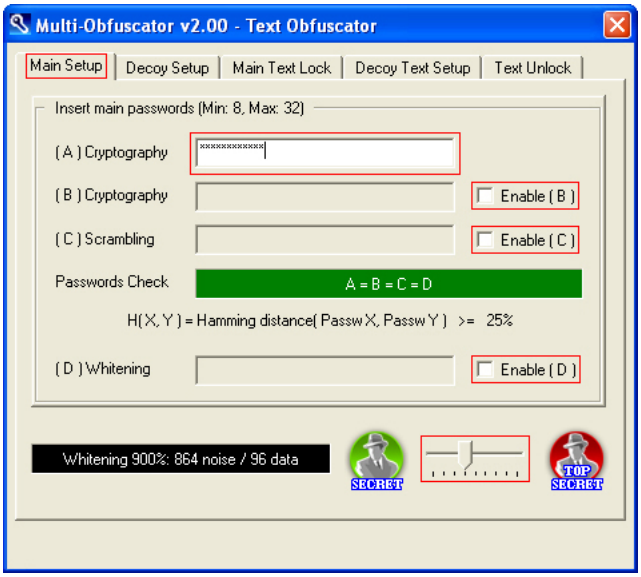
DECIFRAZIONE TESTO – SETUP DI BASE (1 PASSWORD)

INIZIO:

(*Text Lock/Unlock*)	Vai al pannello testo (formato email)

Selezionare *Text Lock/Unlock*.

PASSO 1 – SCELTA DELLA PASSWORD:



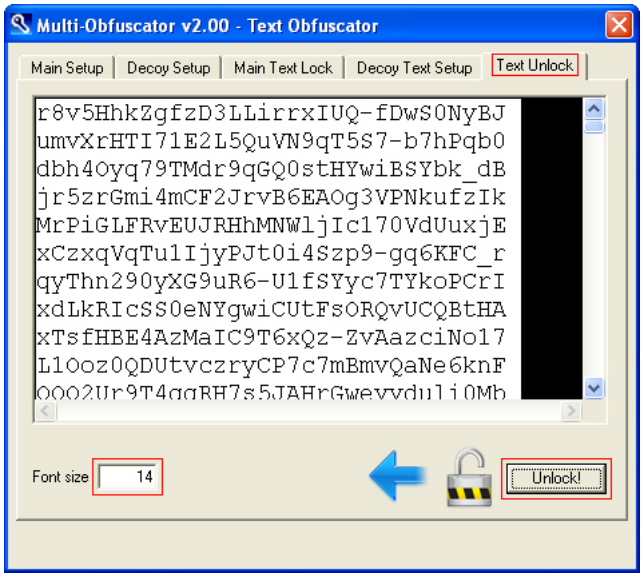
(*Cryptography A*)	La prima password
(*Enable B*)	Abilita/disabilita la seconda password
(*Enable C*)	Abilita/disabilita la terza password
(*Enable D*)	Abilita/disabilita la quarta password

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:

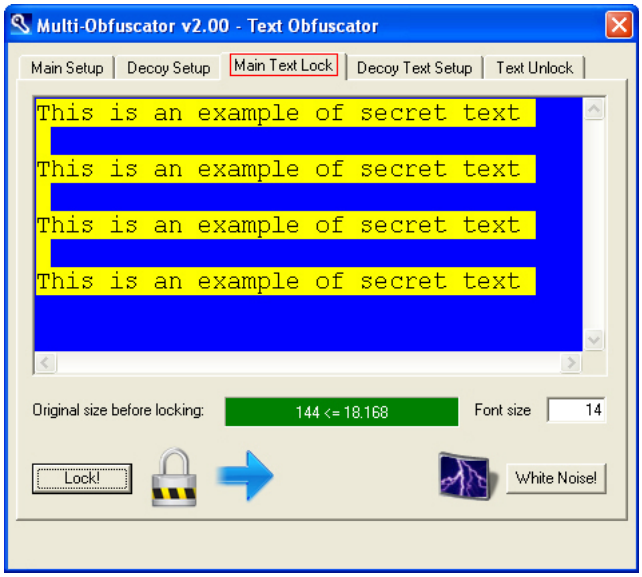
- SETUP DELLE PASSWORD SEMPLICE
- OPZIONI: LIVELLO DI RUMORE

PASSO 2 – SCELTA DEL TESTO:

(I)

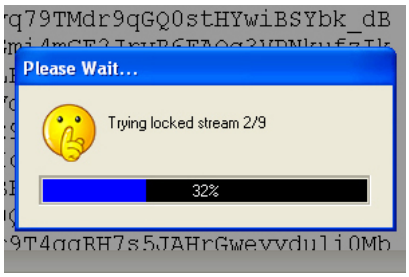


(II)



(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 χ^2

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

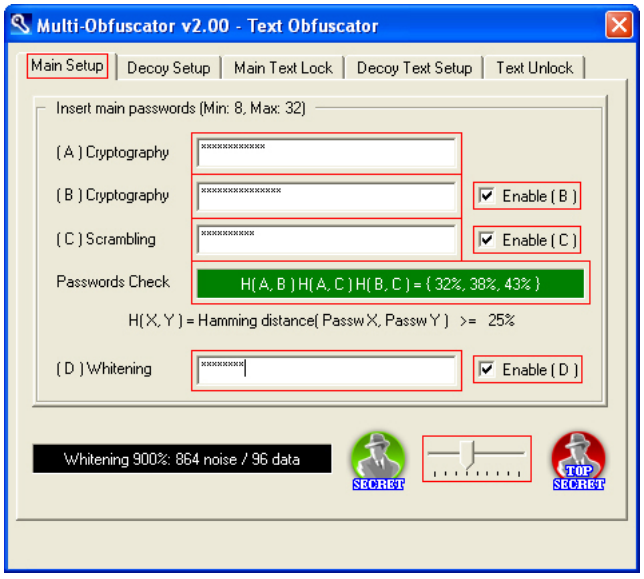
INIZIO:

(*Text Lock/Unlock*)	Vai al pannello testo (formato email)

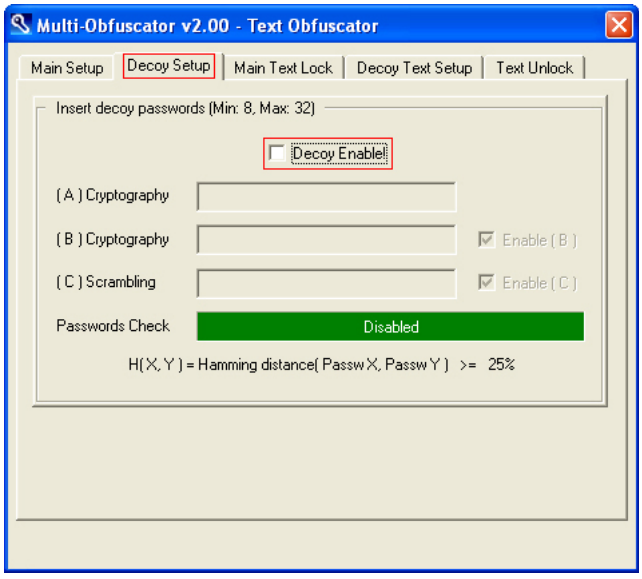
Selezionare *Text Lock/Unlock*.

PASSO 1 – SCELTA DELLE PASSWORD:

(I)



(II)



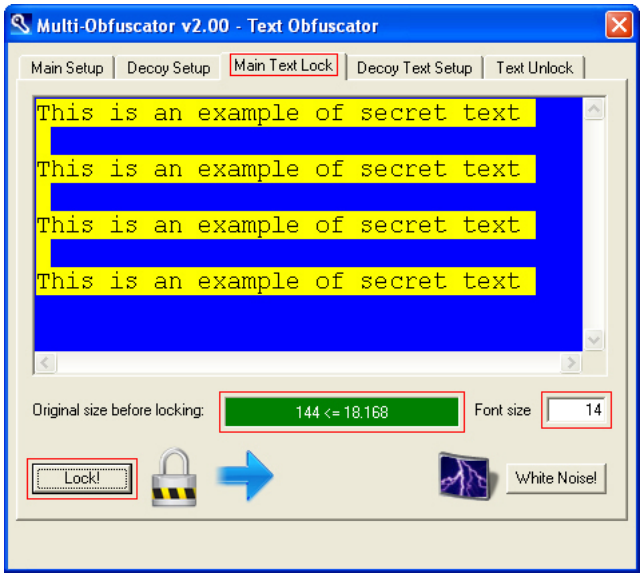
(I)	(*Cryptography A*)	La prima password (chiavi crittografiche)
	(*Cryptography B*)	La seconda password (CSPRNG crittografico)
	(*Scrambling C*)	La terza password (CSPRNG scrambling)
	(*Whitening D*)	La quarta password (CSPRNG whitening)
	(*Enable B*)	Abilita/disabilita la seconda password
	(*Enable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

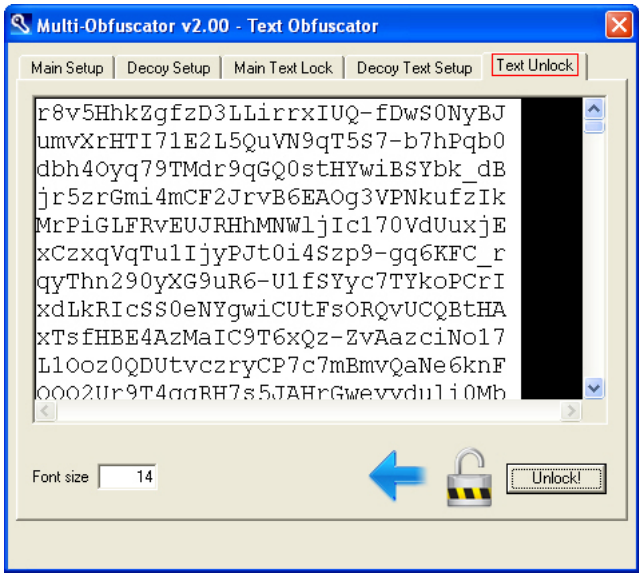
Inserire un'insieme di password e selezionare un livello di rumore. I dettagli completi su password e rumore sono disponibili in speciali sezioni separate:

- 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 – SCELTA DEL TESTO:

(I) 

(II) 

(I)	< TextEdit – finestra blu >	Inserire/incollare un testo
	(*Original size before locking*)	Esempio: 144
	(*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 ≤ 18 Kb
- Dimensione dopo la cifratura: ((144 + 256) / 96) * 1280 = 6.400 byte ≤ 256 Kb

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

OPZIONI: LIVELLO DI RUMORE

INDIETRO

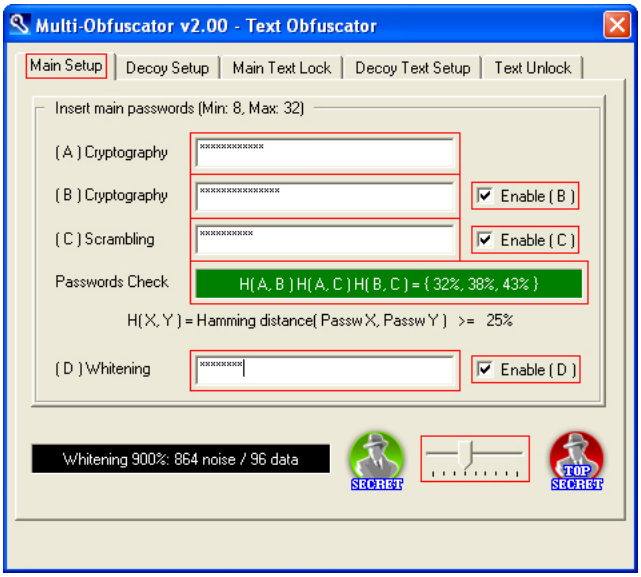
DECIFRAZIONE TESTO – SETUP MEDIO (4 PASSWORD)

INIZIO:

(*Text Lock/Unlock*)	Vai al pannello testo (formato email)

Selezionare *Text Lock/Unlock*.

PASSO 1 – SCELTA DELLE PASSWORD:



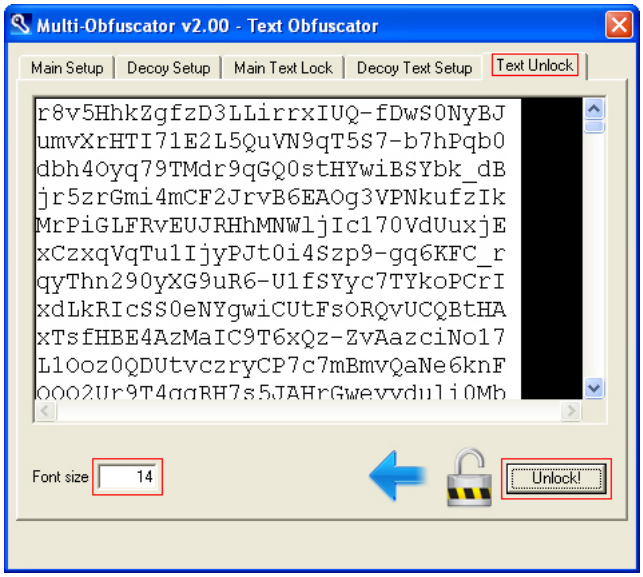
(*Cryptography A*)	La prima password (chiavi crittografiche)
(*Cryptography B*)	La seconda password (CSPRNG crittografico)
(*Scrambling C*)	La terza password (CSPRNG scrambling)
(*Whitening D*)	La quarta password (CSPRNG whitening)
(*Enable B*)	Abilita/disabilita la seconda password
(*Enable C*)	Abilita/disabilita la terza password
(*Enable D*)	Abilita/disabilita la quarta password

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:

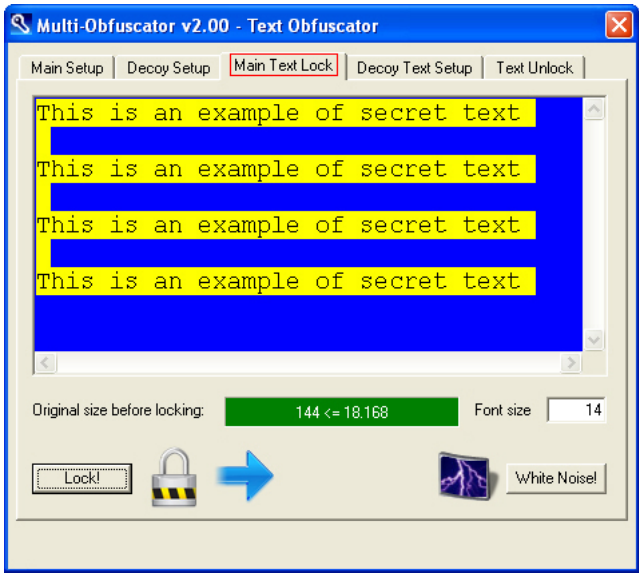
- SETUP DELLE PASSWORD MEDIO
- OPZIONI: LIVELLO DI RUMORE

PASSO 2 – SCELTA DEL TESTO:

(I)

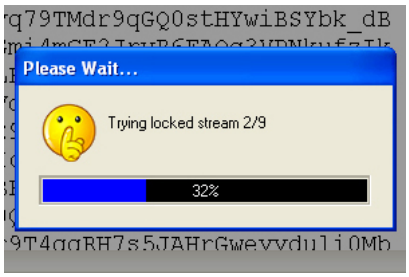


(II)



(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 χ^2

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

ESPERTO  **CIFRATURA TESTO – SETUP AVANZATO (4 PASSWORD+ESCA)**

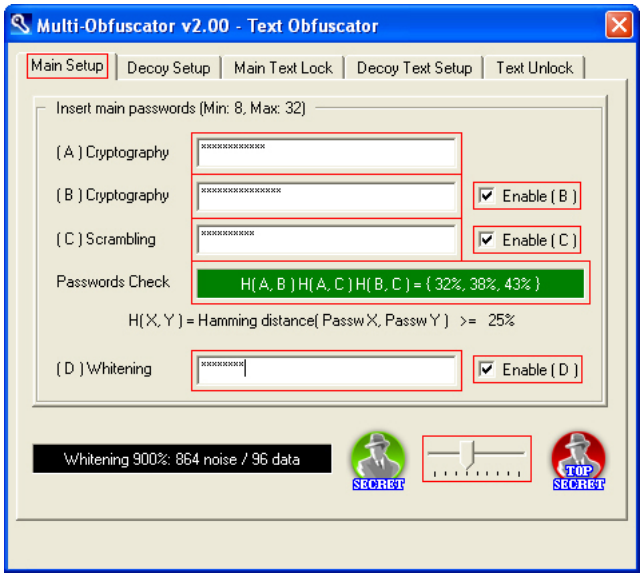
INIZIO:

(*Text Lock/Unlock*)	Vai al pannello testo (formato email)

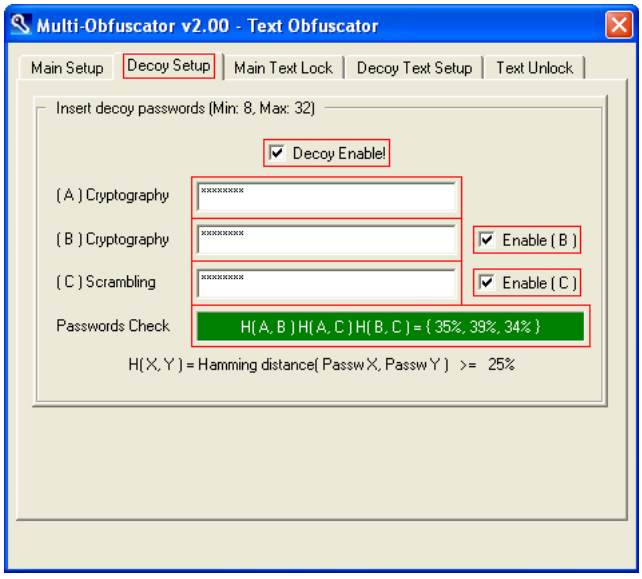
Selezionare *Text Lock/Unlock*.

PASSO 1 – SCELTA DELLE PASSWORD:

(I)



(II)

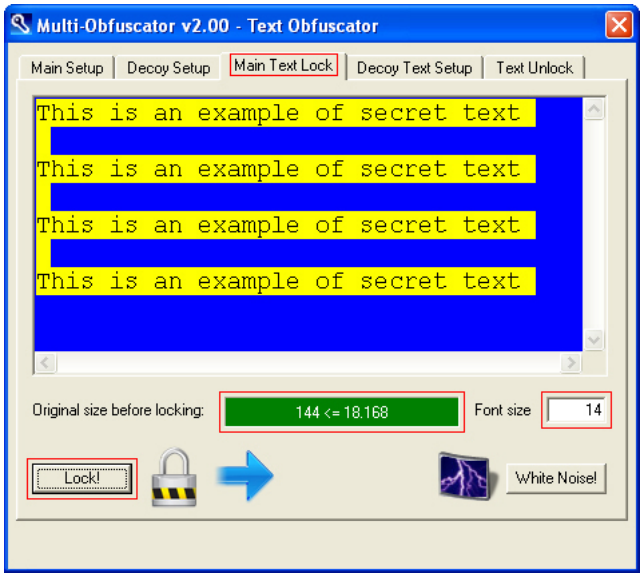


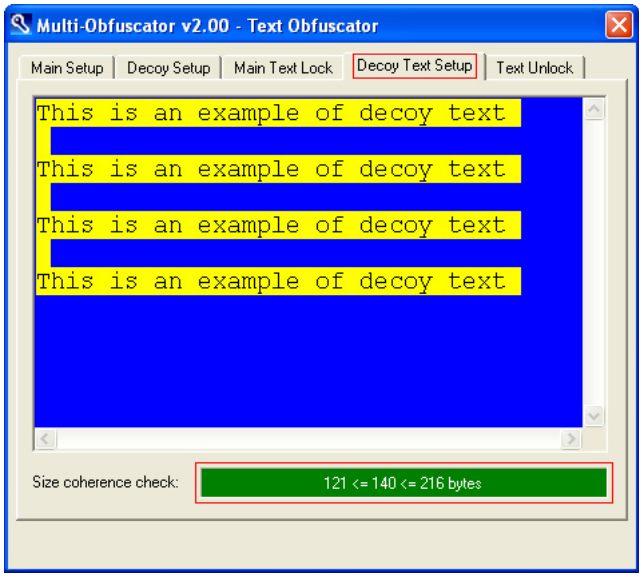
(I)	(*Cryptography A*)	La prima password (chiavi crittografiche)
	(*Cryptography B*)	La seconda password (CSPRNG crittografico)
	(*Scrambling C*)	La terza password (CSPRNG scrambling)
	(*Whitening D*)	La quarta password (CSPRNG whitening)
	(*Enable B*)	Abilita/disabilita la seconda password
	(*Enable 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
- CARATTERISTICHE: ARCHITETTURA DEL PROGRAMMA

PASSO 2 – SCELTA DEL TESTO:

(I) 

(II) 

(I)	< TextEdit – finestra blu >	Inserire/incollare un testo
	(*Original size before locking*)	Esempio: 144
	(*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

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

ESEMPIO:

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

Noise Level	Noise	Data	Min. Plain → Locked Size	Max. Plain → Locked Size
900%	864	**96**	1 B → 3840 B	18 Kb → 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%) → Data = 240 → inf ≤ x ≤ sup → sup - inf + 1 = 240 bytes
Maximum (5900%) → Data = 16 → inf ≤ x ≤ sup → sup - inf + 1 = 16 bytes

Assicurarsi di leggere anche la sezione intermedia
CIFRATURA TESTO – SETUP MEDIO (4 PASSWORD)

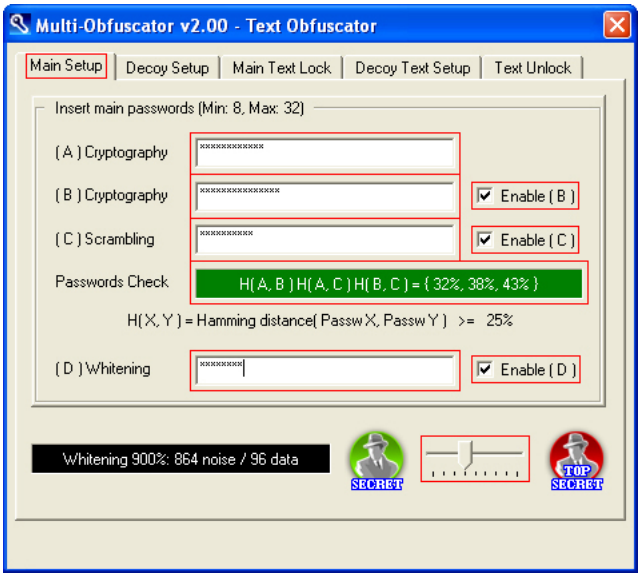
INDIETRO

INIZIO:

(*Text Lock/Unlock*)	Vai al pannello testo (formato email)

Selezionare *Text Lock/Unlock*.

PASSO 1 – SCELTA DELLE PASSWORD:



(*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

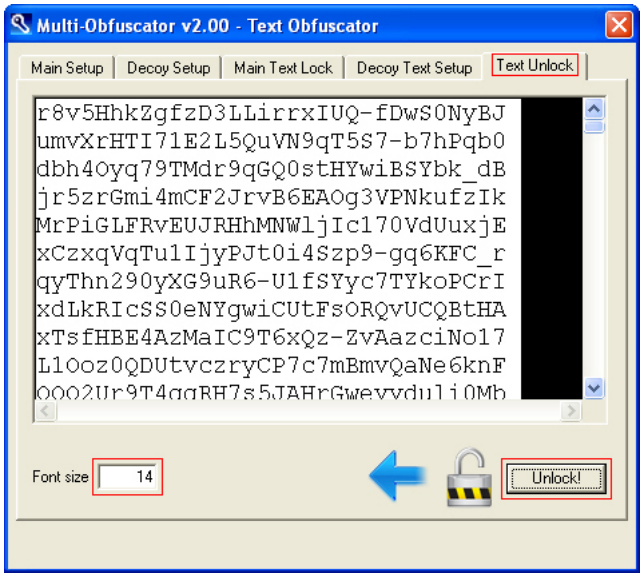
Impostare lo stesso insieme di password (segrete per estrarre i dati segreti, esca per estrarre i dati esca) e livello di rumore usati al momento dell'operazione di cifratura. I dettagli completi su password e rumore sono disponibili in speciali sezioni separate:

- SETUP DELLE PASSWORD AVANZATO – DECIFRAZIONE
- OPZIONI: LIVELLO DI RUMORE

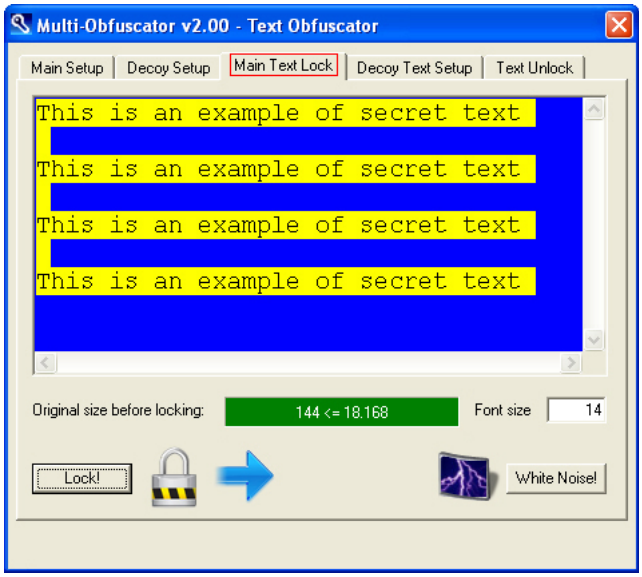
I dettagli completi sull'esca sono disponibili qui:
COSA È LA CRITTOGRAFIA NEGABILE?

PASSO 2 – SCELTA DEL TESTO:

(I)

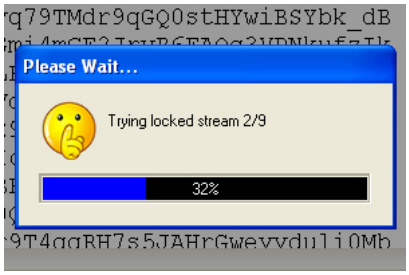


(II)



(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 χ^2

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

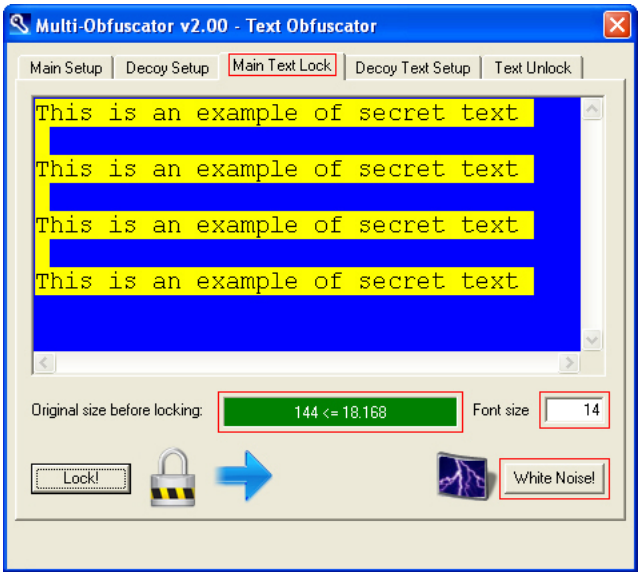
ESPERTO		RUMORE RANDOM COME ESCA (TESTO)

INIZIO:

(*Text Lock/Unlock*)	Vai al pannello testo (formato email)

Selezionare *Text Lock/Unlock*.

PASSO 1 – SCELTA DEL TESTO:



< TextEdit – finestra blu >	Inserire/incollare testo
(*Original size before locking*)	Esempio: 144
(*Font size*)	Dimensione caratteri
(*White Noise!*)	Inizio 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 = **6.400** byte ≤ 256 Kb
- Dimensione del rumore random: **6.400** byte

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

OPZIONI: LIVELLO DI RUMORE

INDIETRO