MultiObfuscator v2.00 Crittografia & Offuscamento

Sicurezza avanzata di file & testo, semplice, sicura e gratuita
Ing. Cosimo Oliboni, Italia, 2012
Inviate i vostri suggerimenti, commenti, segnalazioni, richieste
a *oliboni@embeddedsw.net*

MultiObfuscator HomePage

Semplice	
Medio	
Esperto	
Esperto	

Semplice	
Medio	
Esperto	
Esperto	

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

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?

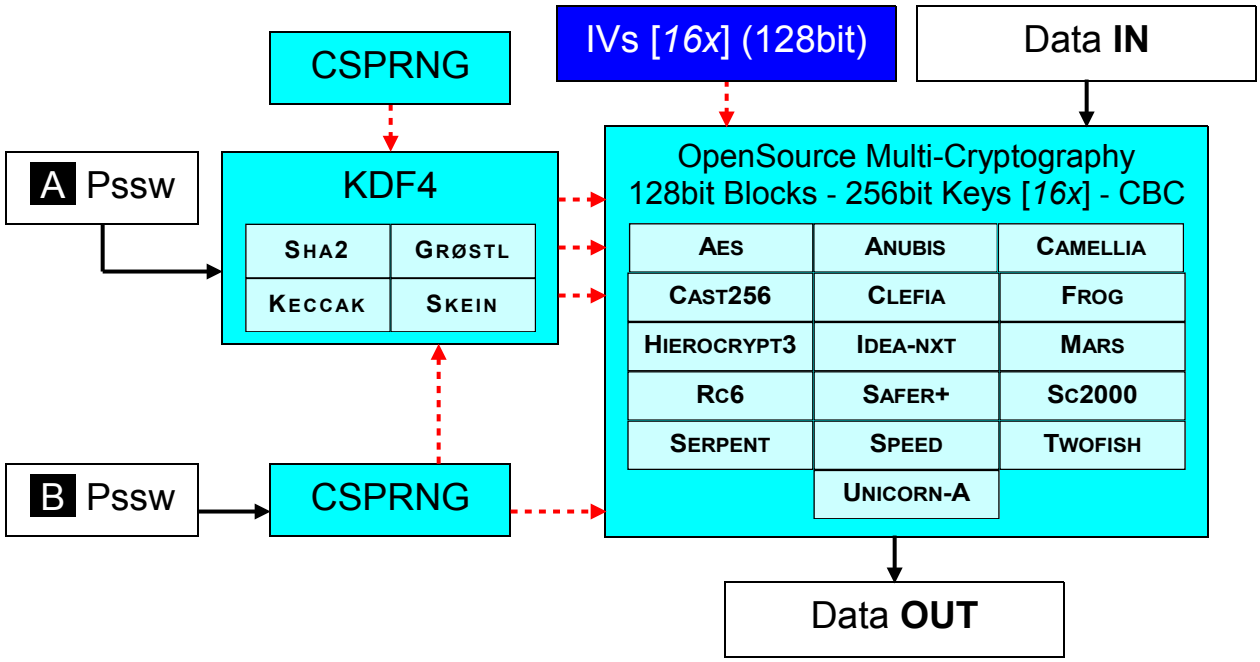
- [CODICE SORGENTE]
  Questo programma può essere considerato come una semplice GUI per Windows della libreria LIBOBFUSCATE, indipendente dal sistema e open-source. Gli utenti e gli sviluppatori sono assolutamente liberi di utilizzare la libreria di base (100% del codice di crittografia e offuscamento),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

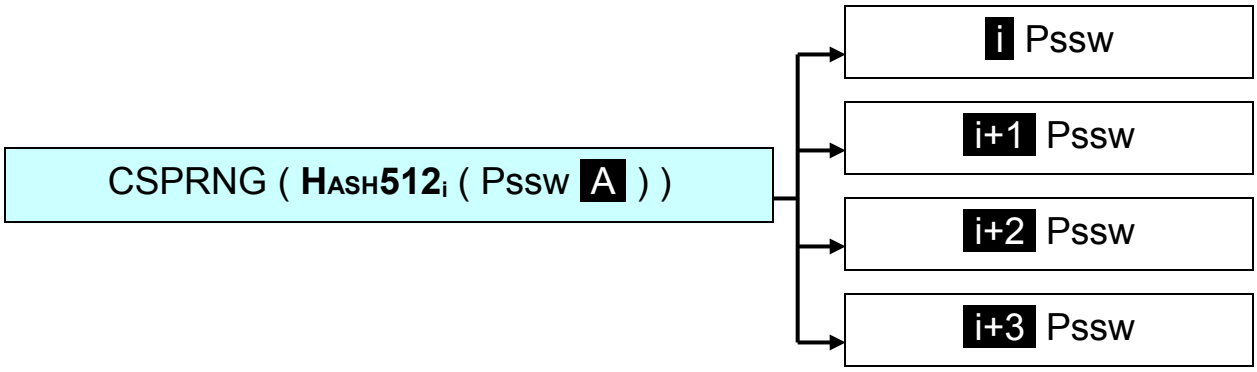
CARATTERISTICHE: ARCHITETTURA DEL PROGRAMMA

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.



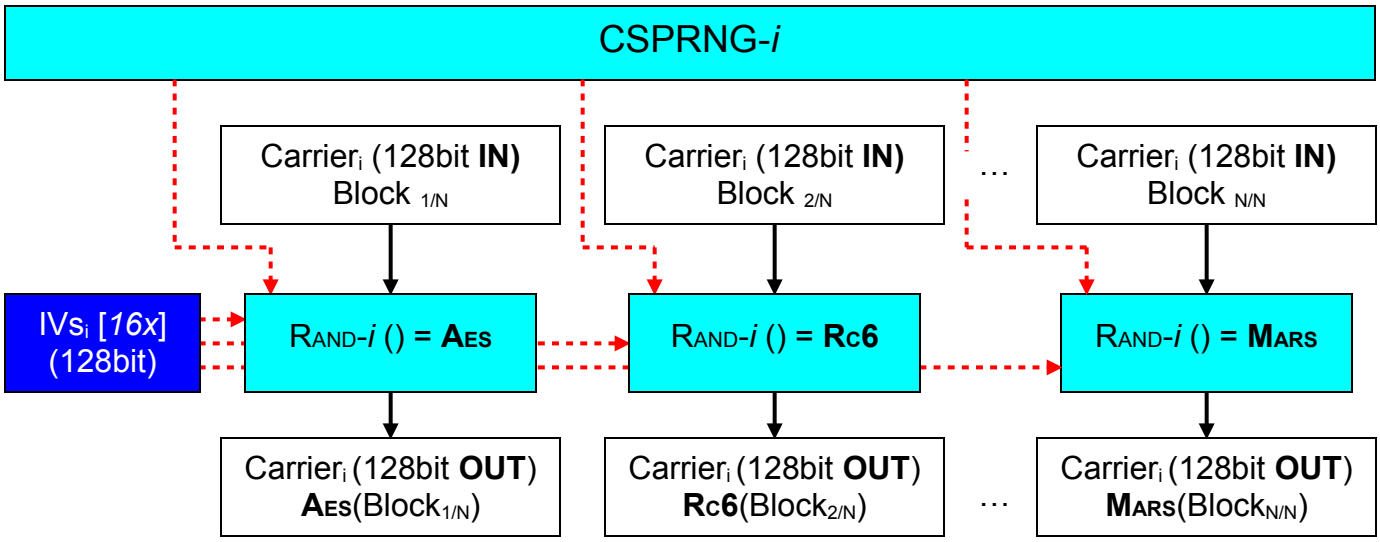
Il setup della multi crittorgrafia è un processo in 4 passi

- un array di vettori random di inizializzazione (16 x 128bit) è associato ad ogni carrier
- un motore pseudo random (CSPRNG) viene inizializzato usando la password (**B**)
- la password (**A**) viene estesa (KDF4) usando 4 moderni algoritmi open-source di hashing a 512bit, provenienti dallo SHA2 e dallo SHA3. Ogni hash genera quattro chiavi a 256bit
  Pssw (**1**) | (**2**) | (**3**) | (**4**) = *Rand* (*Sha2* (*Pssw* (**A**)))
  Pssw (**5**) | (**6**) | (**7**) | (**8**) = *Rand* (*Grøstl* (*Pssw* (**A**)))
  Pssw (**9**) | (**10**) | (**11**) | (**12**) = *Rand* (*Keccak* (*Pssw* (**A**)))
  Pssw (**13**) | (**14**) | (**15**) | (**16**) = *Rand* (*Skein* (*Pssw* (**A**)))
- l'array di chiavi risultante (16 x 256bit) è associato ad ogni algoritmo usando il CSPRNG



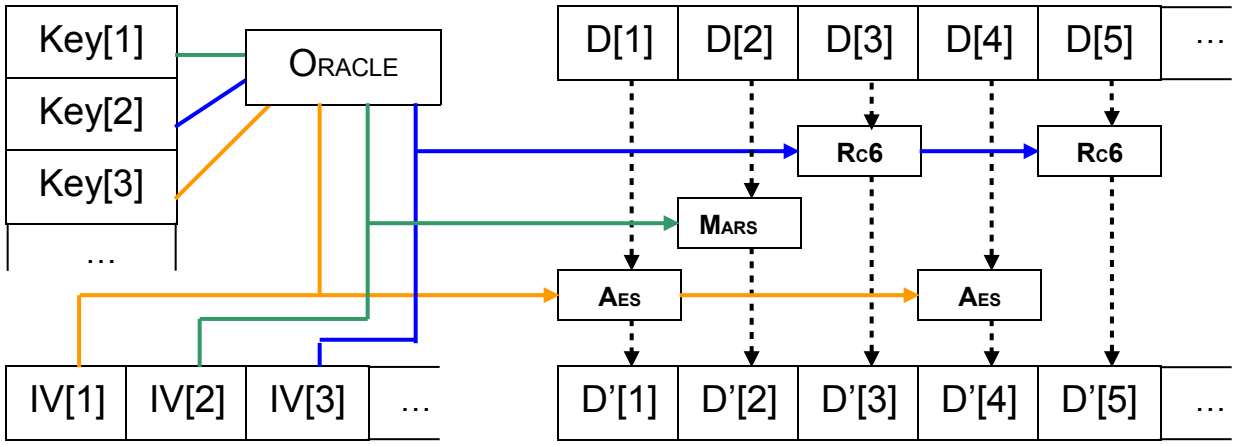
La crittografia è un processo in più passi

- i dati sono sottoposti ad un setup globale
  Setup = { { *IV* } , *CSPRNG* , { *Key* } }
- ogni algoritmo è sottoposto ad un setup indipendente
  $Cipher_j$ = { IV_j , Key_j }
- ogni blocco di dati è processato con un algoritmo diverso, scelto usando il CSPRNG
  $CryptedBlock_k = r \leftarrow Rand\text{-}i\ ()\ ;\ Cipher_r\ (\ IV_r\ ,\ Key_r\ ,\ Block_k\ )$



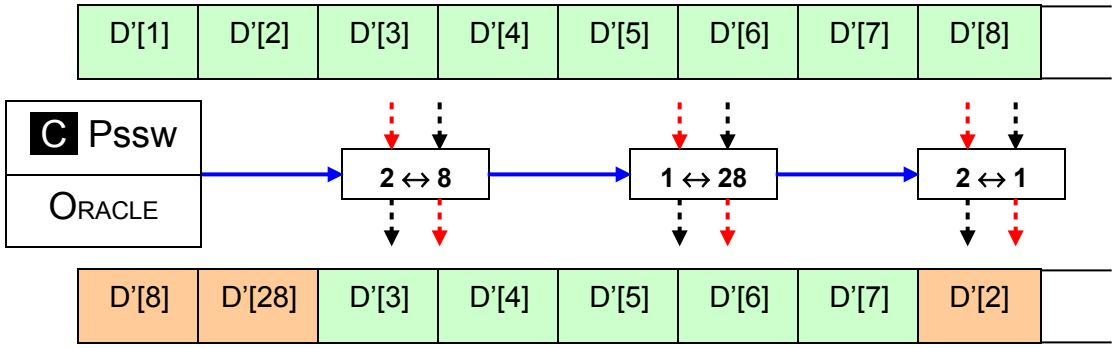
La multi crittografia è il primo livello (locale) di offuscamento

- la crittografia e il CSPRNG ricevono due password indipendenti
- ogni cifrario implementato riceve un IV e una chiave differenti
- il CSPRNG si comporta come un ORACOLO che alimenta il motore crittografico durante tutte le sue scelte (quale chiave associare a quale cifrario, quale cifrario applicare a quale blocco di dati, …)



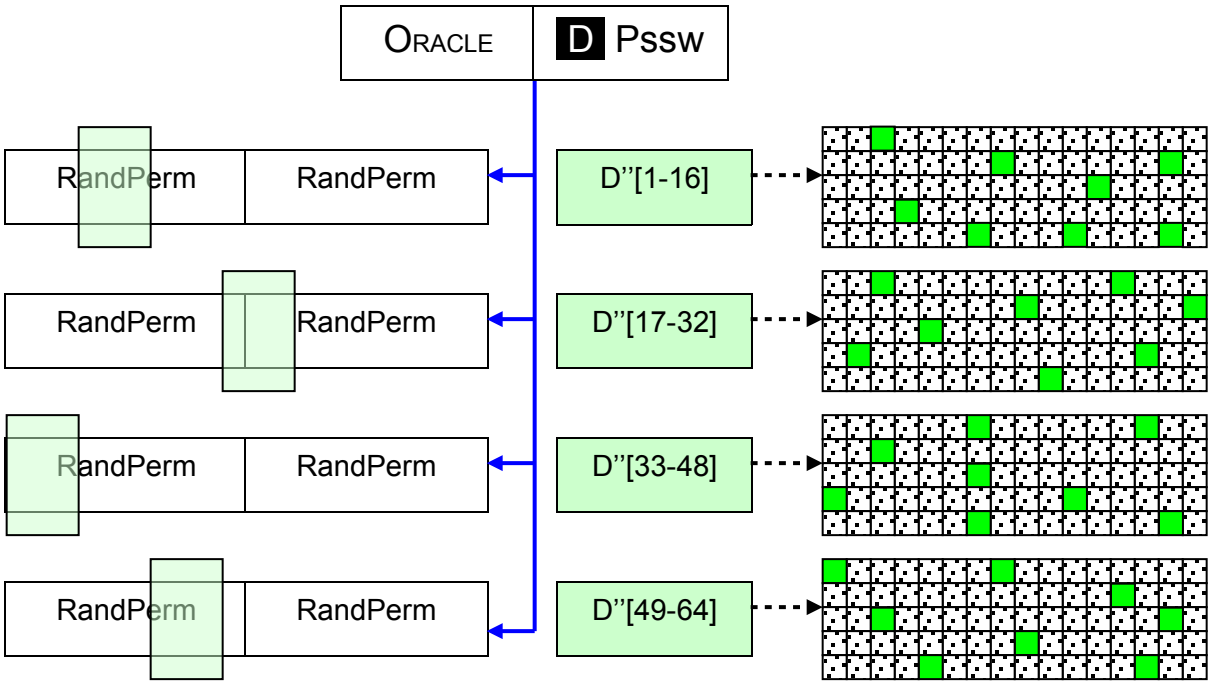
Lo scrambling è il secondo livello (globale) di offuscamento

- il CSPRNG riceve una password indipendente
- il CSPRNG si comporta come un ORACOLO che, dati **n** byte di input, effettua **n/2** shuffle random ed IN-PLACE, senza vincoli per gli indici ripetuti



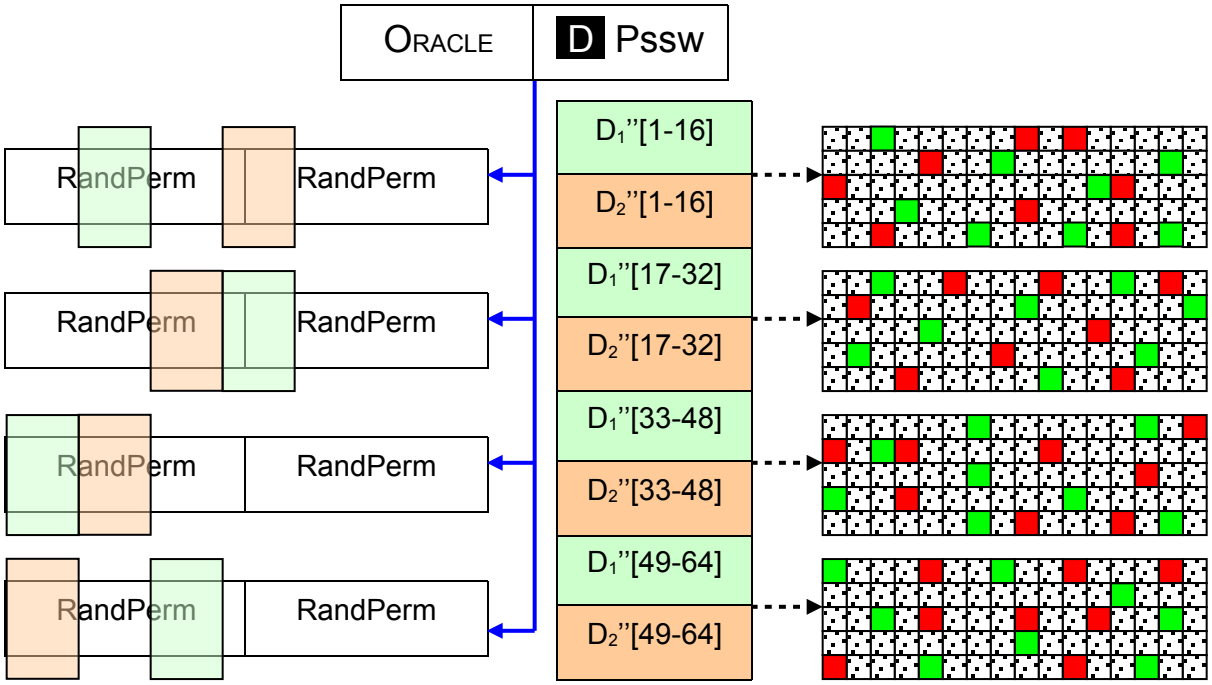
Il whitening è il terzo livello (locale) di offuscamento

- il CSPRNG riceve una password indipendente
- I dati e il rumore, a seconda del livello di rumore, sono mischiati in blocchi di dimensione costante
  minimo: 300% rumore [720 byte] / dati [240 byte]
  massimo: 5900% rumore [944 byte] / dati [16 byte]
- blocchi da 960 byte (= 3x4x5x16) forzano gli attaccanti a testare tutti i livelli di rumore disponibili (9)
- il CSPRNG si comporta come un ORACOLO che, data una P-BOX con SHUFFLE DI DURSTENFELD (una permutazione a livello di bit), alimenta il mixer con un insieme, ad offset iniziale random, di indici non sovrapposti.
  OPZIONI: LIVELLO DI RUMORE



Il whitening è anche il nucleo della Crittorgrafia negabile

- MultiObfuscator supporta dati e un'esca (un primo livello di crittografia negabile)
- libObfuscate supporta dati e diverse esche (**n** livelli di crittografia negabile, chiamati *aspetti*)
- il numero massimo di aspetti dipende, a livello del nucleo di libObfuscate, dal livello di rumore
  minimum: 300% 4x aspetti [240 byte]
  maximum: 5900% 60x aspetti [16 byte]
- l'associazione *Aspetto* ↔ *Offset* è random e indipendente dalla password
- l'associazione *Aspetto* ↔ *Offset*, dopo il whitening, è semplicemente scartata
- MultiObfuscator (e ogni sistema linkato a libObfuscate) non può, per costruzione, ricostruire l'associazione *Aspect* ↔ *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.

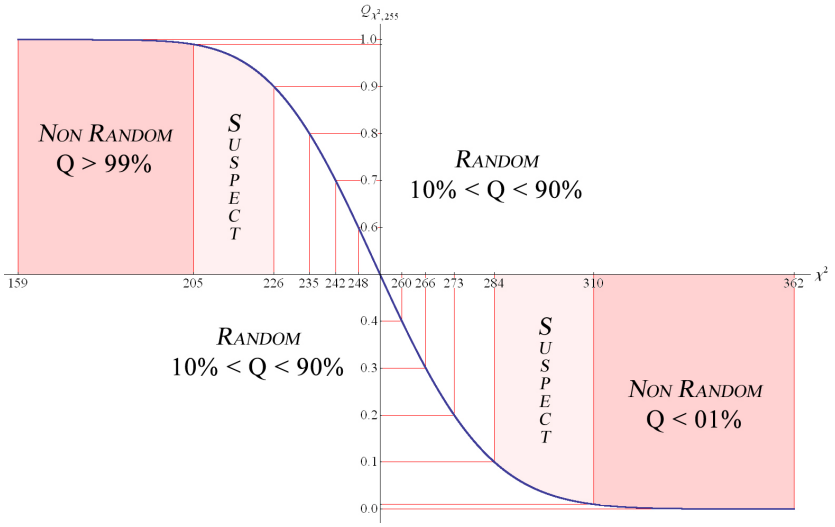
Rubberhose *è stato* (a causa dell'abbandono) un progetto avanzato che ha introdotto nuovi concetti

- 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, sfortunamente, 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.

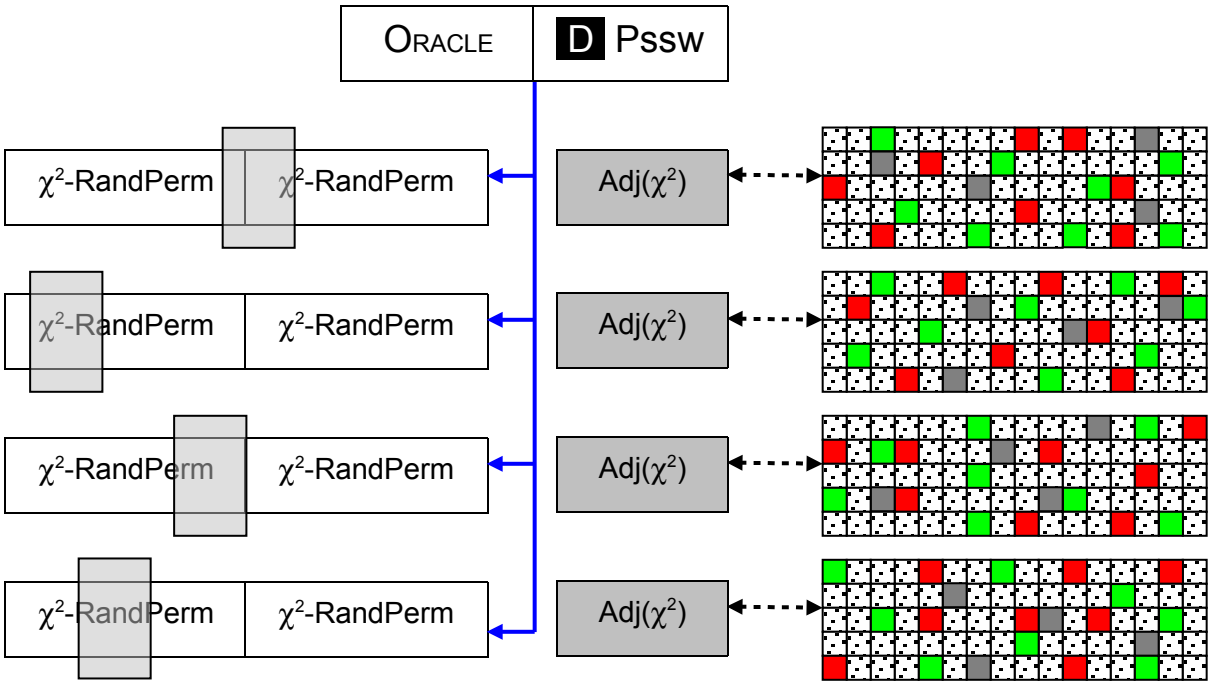
MultiObfuscator (e ogni sistema linkato a libObfuscate) implementa un auto-aggiustamento basato sulla DISTRIBUZIONE-χ^2. Alcuni byte vengono aggiunti ad ogni blocco in posizioni random, consentendo ad ogni contenitore, indipendentemente dall'uso (*vuoto* → rumore, *sparso* → singolo aspetto, *pieno* → **n** aspetti),

- di eccedere la DISTRIBUZIONE-χ^2 il 50% delle volte (Q = 0.5), come un vera sequenza random creata da EVENTI DI DECADIMENTO RADIATTIVO
- di ottenere un punteggio ≥98% nel sistema NIST di misura della randomicità



Gli utenti avanzati trarranno grande vantaggio dalla resistenza statistica dei contenitori

- aggiungendo contenitori vuoti/fasulli a quelli sensibili, per rallentare gli attaccanti
- negando in maniera sempre convincente di stare usando più di un singolo aspetto
- condividendo, all'insaputa di tutti, un contenitore con più aspetti fra persone non fidate, potenzialmente ostili



INDIETRO

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 cittografia 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 opern-source.

FAQ 4: La multi crittografia è migliore della crittografia standard?

Una *casa* è migliore di un *mattone*? No. La casa è una *superstruttura* e il mattone è un *materiale*.

La *multi crittografia* è migliore della *crittografia*? No. La multi crittografia è parte di un *processo* di offuscamento dati e la crittografia è un *componente*.

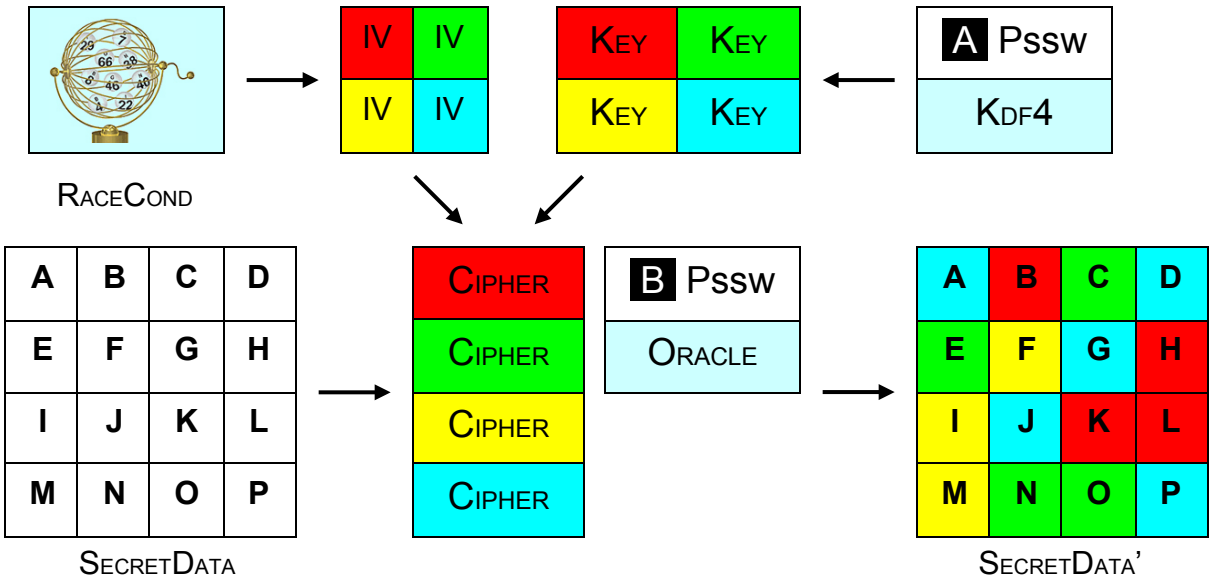
Crittografia	=	Mattone
Multi crittografia	=	Piano
Processo di offuscamento	=	Casa

FAQ 5: L'offuscamento dati è migliore della crittografia standard?

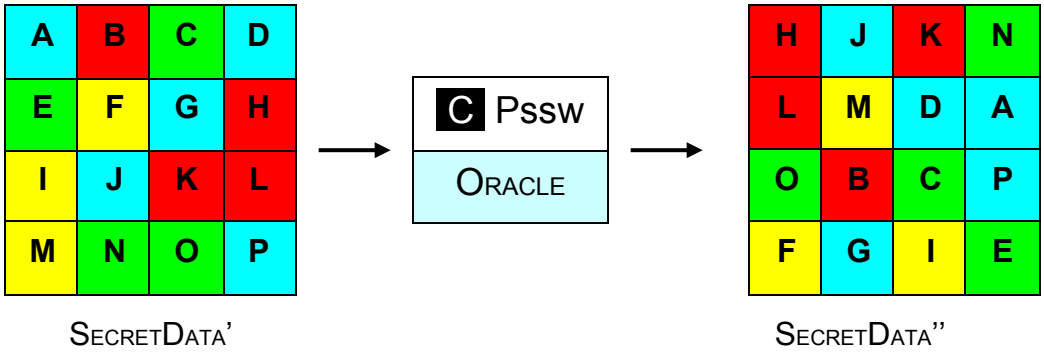
L'offuscamento dati non ha nessuna pretesa di INVIOLABILITÀ (da considerare sempre come un sintomo di inganno o CRITTOGRAFIA FRAUDOLENTA). È comunque possibile gestire il problema del bisogno *insolitamente alto* di sicurezza in modo effettivo e costruttivo (secondo il PRINCIPIO DI KERCKHOFF), come un problema (*rallentare gli attaccanti* il più possibile) da ingegnerizzare

- connettere trasformazioni di offuscamento diverse
- evitare di applicare ripetutamente la stessa trasformazione
- affidarsi unicamente a risorse open-source
- applicare qualche trasformazione globale, invertibile solo via software

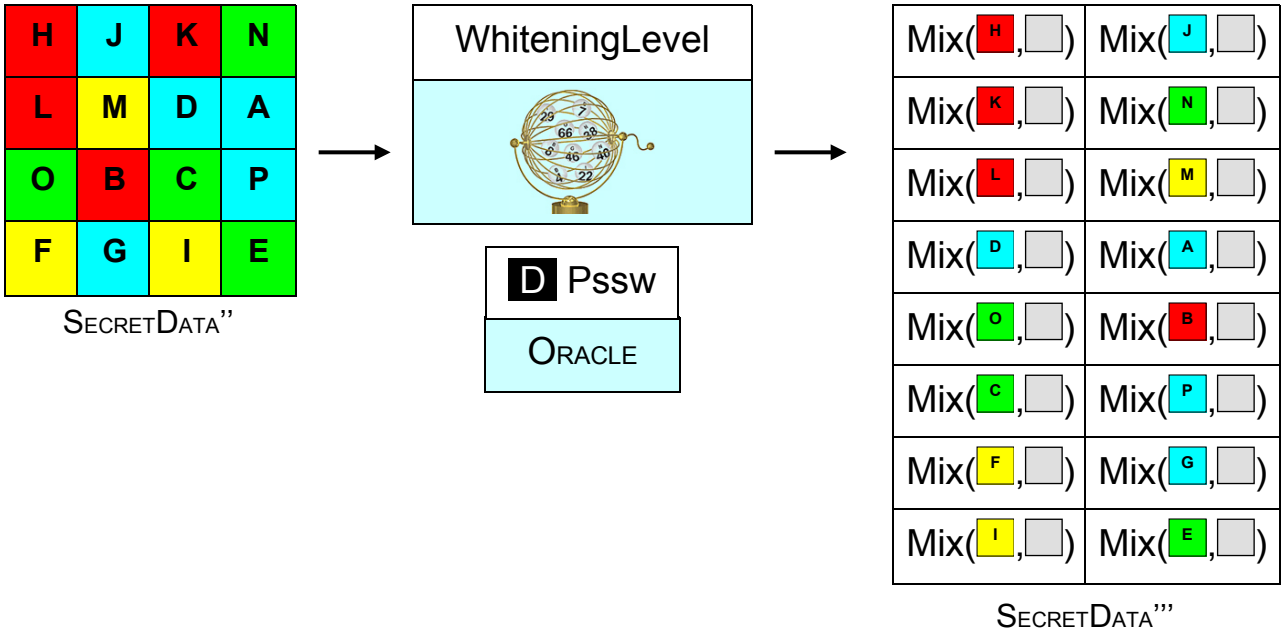
[Round 1 – MULTI CRITTOGRAFIA (TRASFORMAZIONE LOCALE)]



[Round 2 – SCRAMBLING (TRASFORMAZIONE GLOBALE)]



[Round 3 – Whitening (trasformazione locale)]

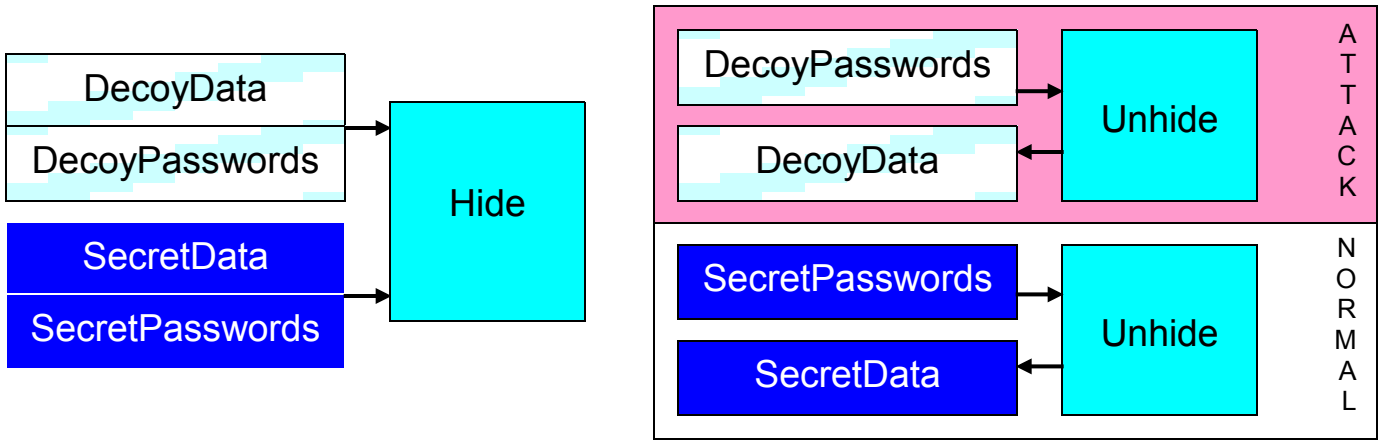


Caratteristiche: architettura del programma

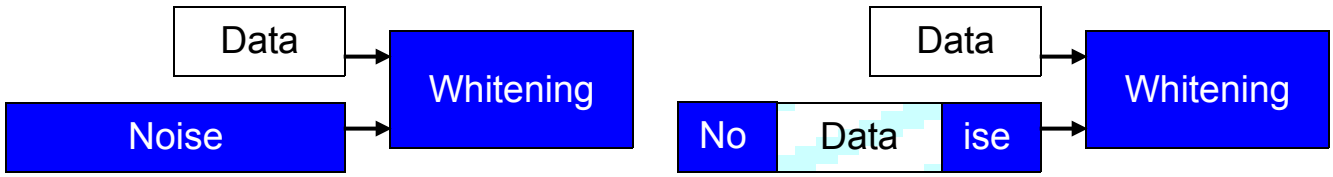
Indietro

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.



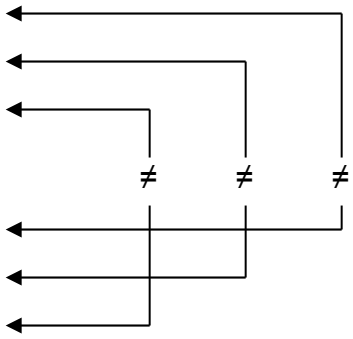
Come è possibile? I dati crittografati e sottoposti a scrambling, sono sottoposti a whitening (CARATTERISTICHE: ARCHITETTURA DEL PROGRAMMA) con una grande quantità di rumore. I dati esca possono sostituire un po' del rumore senza compromettere le proprietà finali di RESISTENZA ALLA CRITTANALISI.



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:

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**: ((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:

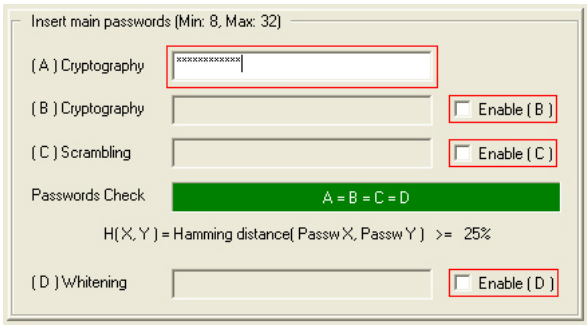
- **Formato**: testo/email
- **Blocco di dimensione costante**: Noise + Data = 960 byte → codifica a 6 bit → 1280 byte
- **Dimensione dell'output protetto**: ((size + 256) / Data) * 1280 ≤ 256 Kb

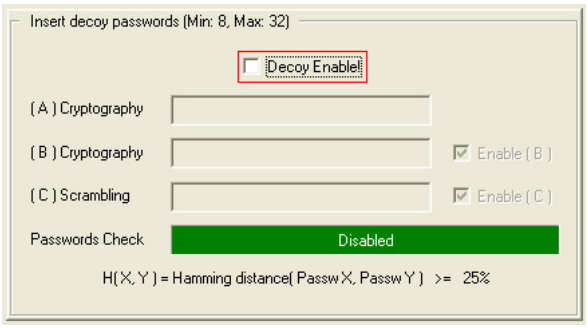
Noise Level	Noise	Data	Min. Plain → Locked Size	Max. Plain → Locked Size
300%	720	**240**	1 B → 2560 B	46 Kb → 256 Kb
	Whitening 300%: 720 noise / 240 data			
400%	768	**192**	1 B → 2560 B	36 Kb → 256 Kb
	Whitening 400%: 768 noise / 192 data			
500%	800	**160**	1 B → 2560 B	30 Kb → 256 Kb
	Whitening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

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

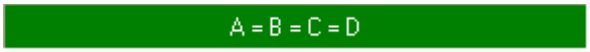
B.1) Disabilitare le password (Main_B / Main_C / Main_D)
B.2) Inserire una password (Main_A) qualsiasi

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

Vincoli:

1) Length (Main_A) ≥ 8

Esempio:



Main: ok

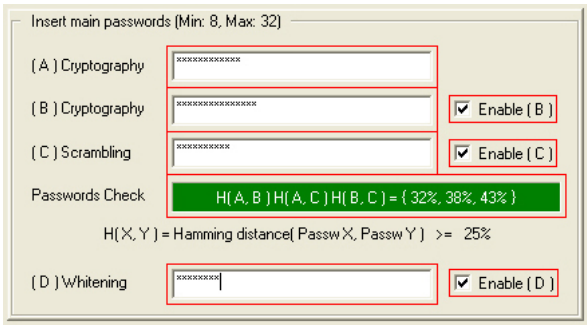
Main_A = "any password"

INDIETRO

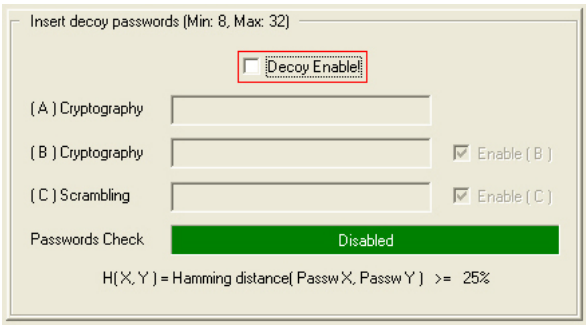
SETUP DELLE PASSWORD MEDIO

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”

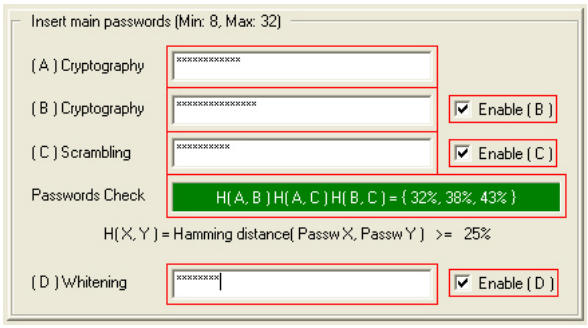
INDIETRO

SETUP DELLE PASSWORD AVANZATO – CIFRATURA

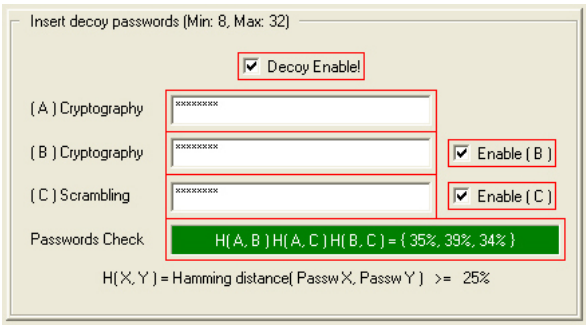
ESPERTO

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

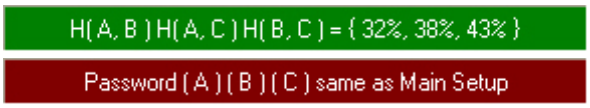
Le password (Decoy_B / Decoy_C) disabilitate diventeranno uguali alla password (Decoy_A)!

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

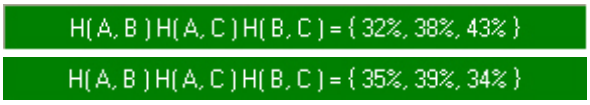
Esempio:



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, …

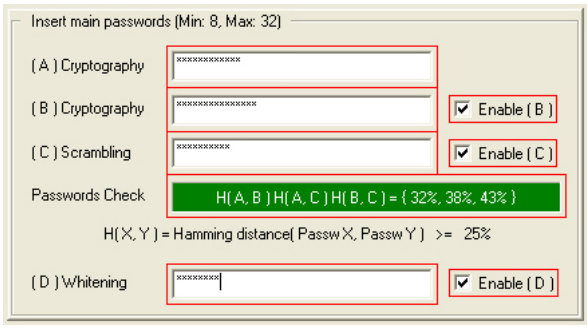
Main_A = “some_crypt_a” Decoy_A = “12345678”
Main_B = “another_crypt_b” Decoy_B = “qwertyui”
Main_C = “scramble_c” Decoy_C = “zxcvbnm,”
Main_D = “whiten_d”

SETUP DELLE PASSWORD AVANZATO – DECIFRAZIONE

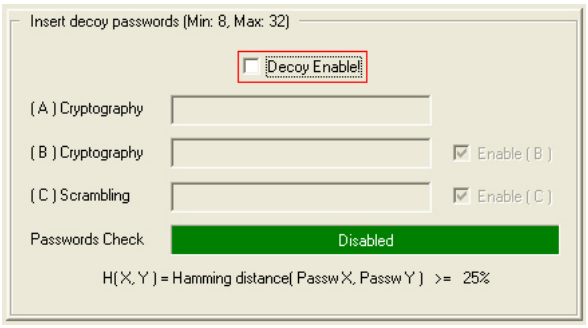
ESPERTO

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)

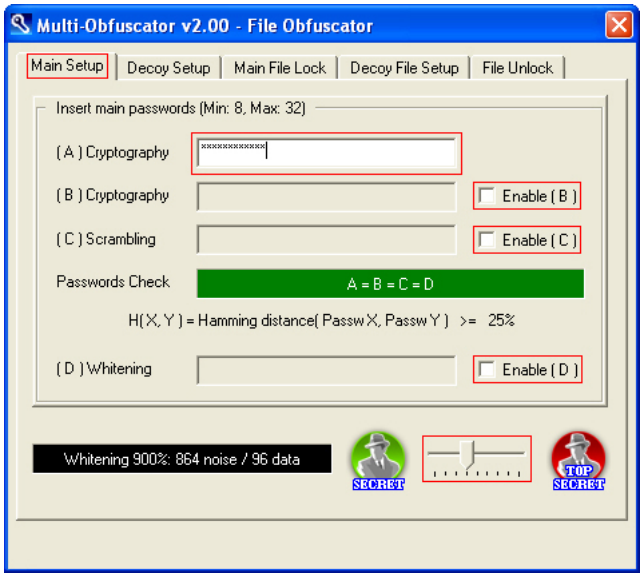
INIZIO:

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

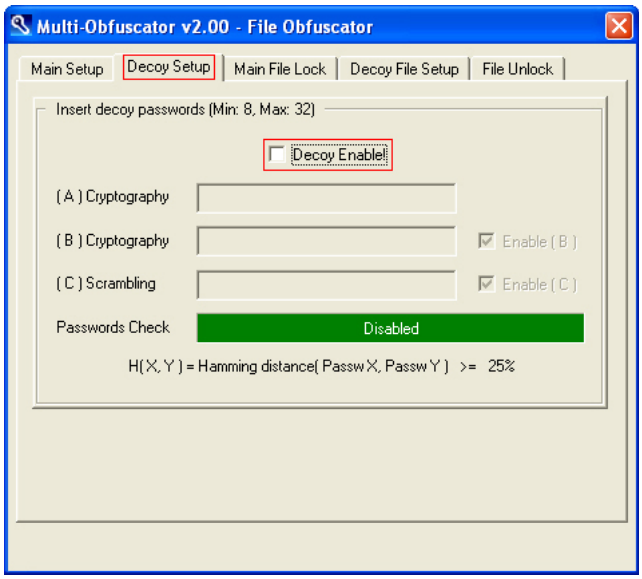
Selezionare *File Lock/Unlock*.

PASSO 1:

(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

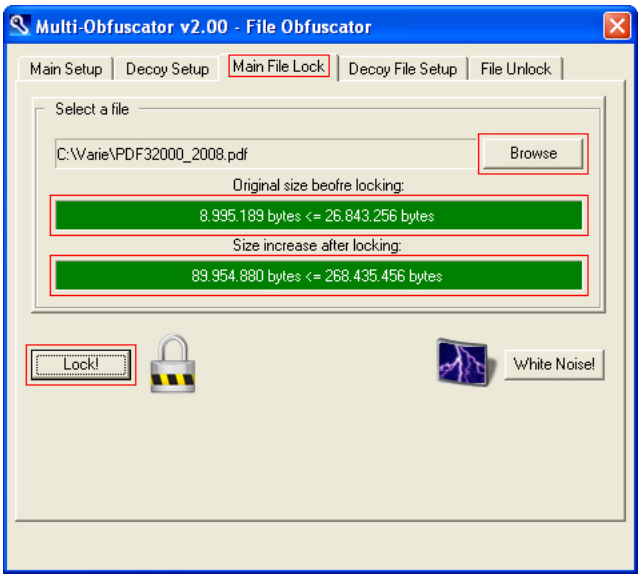
Inserire una password e selezionare un livello di rumore. I dettagli completi su password e rumore sono disponibili in speciali sezioni separate:

- 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:



(*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	**96**	1 B → 2880 B	**25 Mb → 256 Mb**

OPZIONI: LIVELLO DI RUMORE

INDIETRO

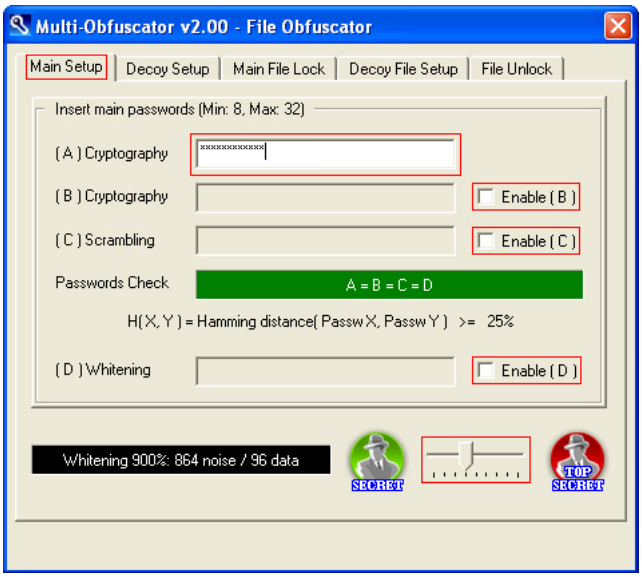
DECIFRAZIONE FILE – SETUP DI BASE (1 PASSWORD)

INIZIO:

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

Selezionare *File Lock/Unlock*.

PASSO 1:

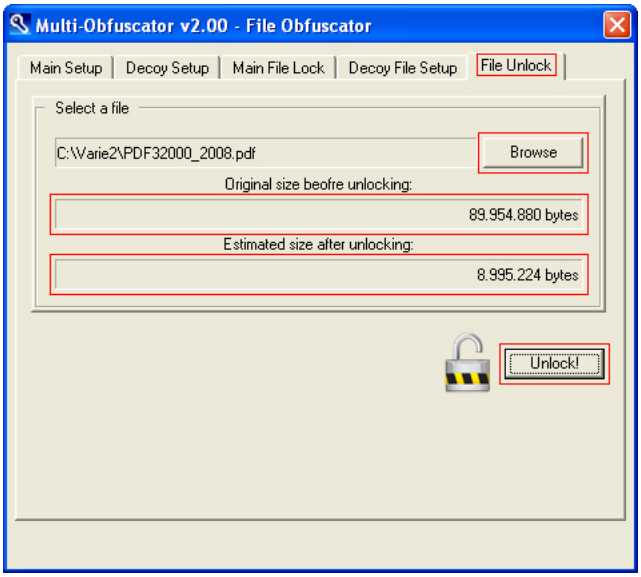


(*Cryptography A*)	La prima password
(*Enable B*)	Abilita/disabilita la seconda password
(*Enable C*)	Abilita/disabilita la terza password
(*Enable D*)	Abilita/disabilita la quarta password

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:

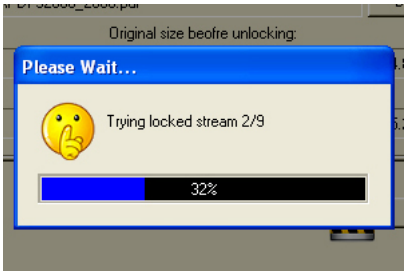
- SETUP DELLE PASSWORD SEMPLICE
- OPZIONI: LIVELLO DI RUMORE

PASSO 2:



(*Browse*)	Selezionare un file cifrato
(*Original size before unlocking*)	Esempio: 89.954.880 byte
(*Estimated size after unlocking*)	Esempio: 8.995.224 byte
(*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 MEDIO (4 PASSWORD)

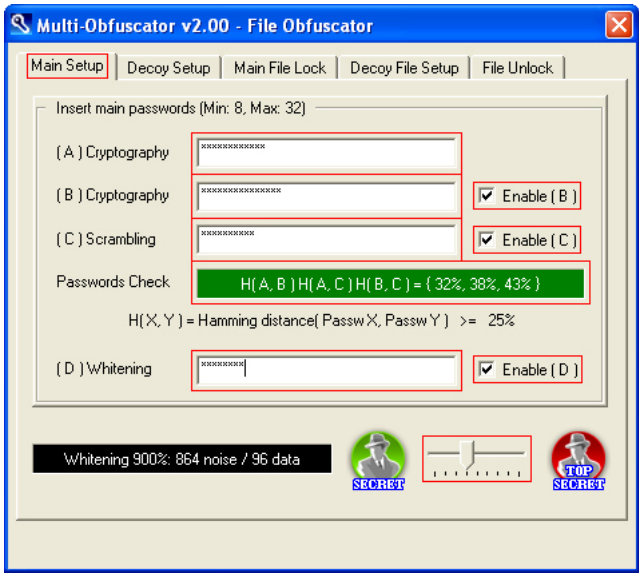
INIZIO:

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

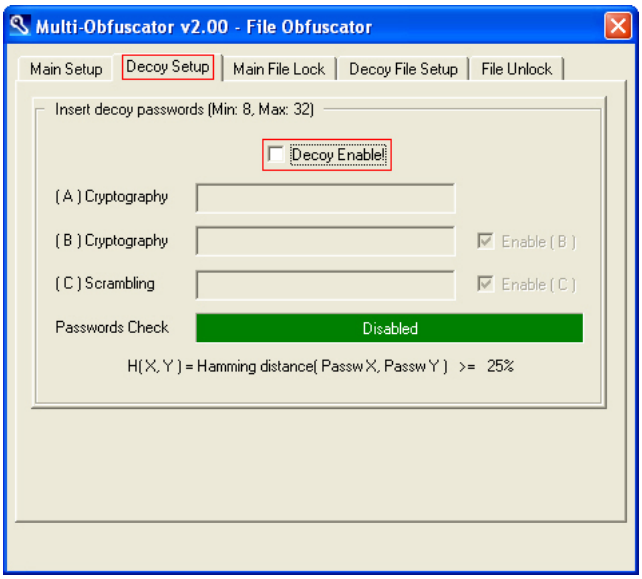
Selezionare *File Lock/Unlock*.

PASSO 1:

(I)



(II)



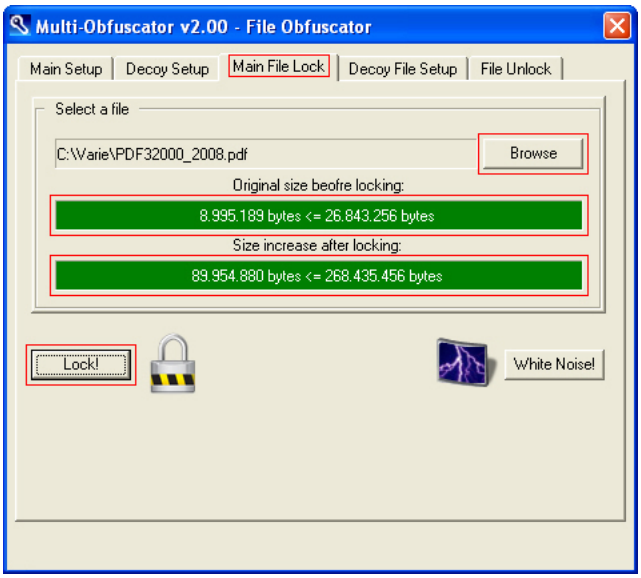
(I)	(*Cryptography A*)	La prima password (chiavi crittografiche)
	(*Cryptography B*)	La seconda password (CSPRNG crittografico)
	(*Scrambling C*)	La terza password (CSPRNG scrambling)
	(*Whitening D*)	La quarta password (CSPRNG whitening)
	(*Enable B*)	Abilita/disabilita la seconda password
	(*Enable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

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	**96**	1 B → 2880 B	**25 Mb → 256 Mb**

OPZIONI: LIVELLO DI RUMORE

INDIETRO

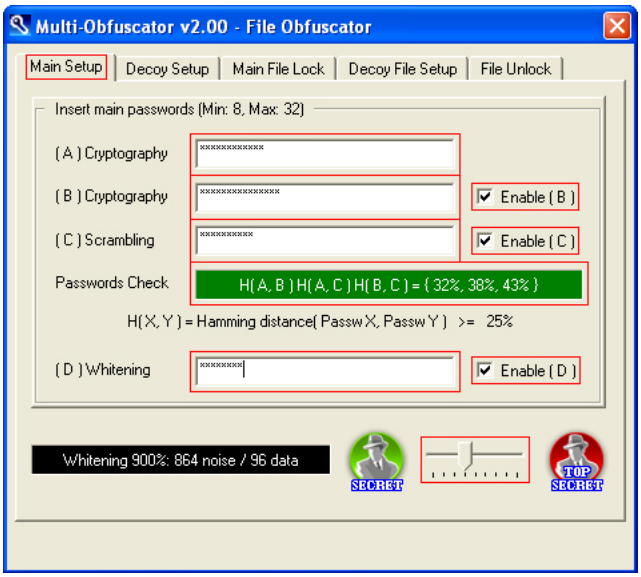
DECIFRAZIONE FILE – SETUP MEDIO (4 PASSWORD)

INIZIO:

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

Selezionare *File Lock/Unlock*.

PASSO 1:

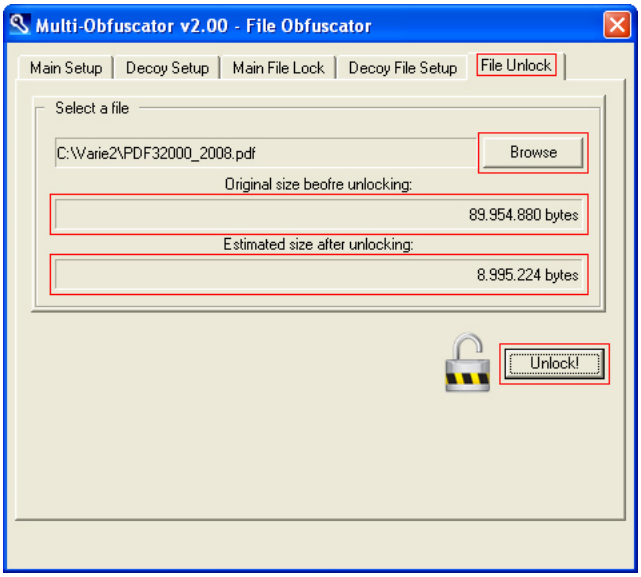


(*Cryptography A*)	La prima password (chiavi crittografiche)
(*Cryptography B*)	La seconda password (CSPRNG crittografico)
(*Scrambling C*)	La terza password (CSPRNG scrambling)
(*Whitening D*)	La quarta password (CSPRNG whitening)
(*Enable B*)	Abilita/disabilita la seconda password
(*Enable C*)	Abilita/disabilita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

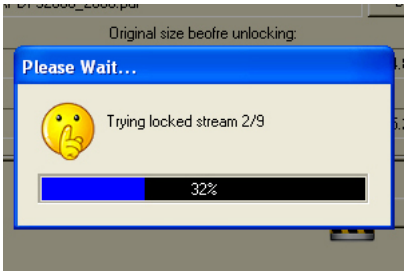
- SETUP DELLE PASSWORD MEDIO
- OPZIONI: LIVELLO DI RUMORE

PASSO 2:



(*Browse*)	Selezionare un file cifrato
(*Original size before unlocking*)	Esempio: 89.954.880 byte
(*Estimated size after unlocking*)	Esempio: 8.995.224 byte
(*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

ESPERTO

CIFRATURA FILE – SETUP AVANZATO (4 PASSWORD+ESCA)

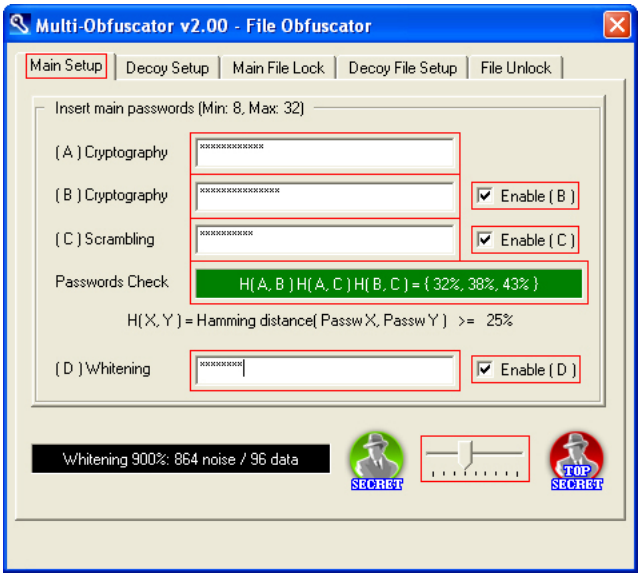
INIZIO:

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

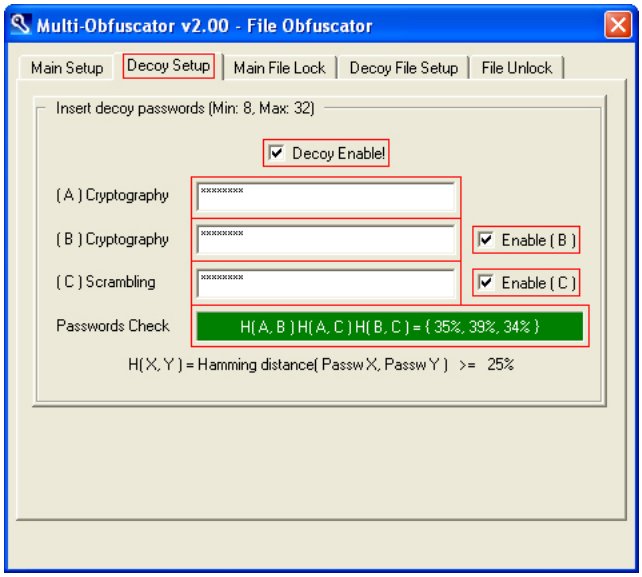
Selezionare *File Lock/Unlock*.

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

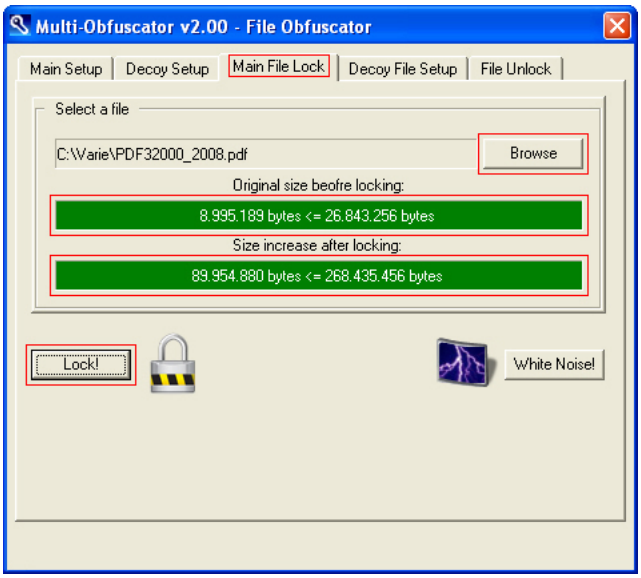
Inserire un'insieme di password, un'insieme di password esca e selezionare un livello di rumore. I dettagli completi su password e rumore sono disponibili in speciali sezioni separate:

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

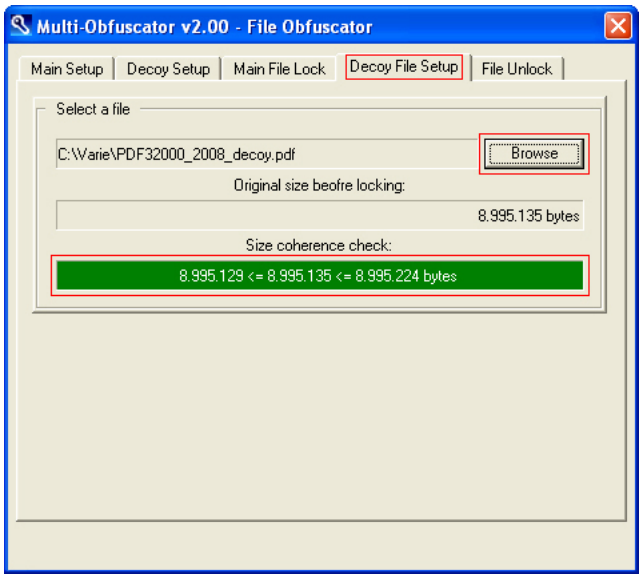
Il setup avanzato consente un uso completo dell'architettura di sicurezza multi livello e multi aspetto.
CARATTERISTICHE: ARCHITETTURA DEL PROGRAMMA

PASSO 2:

(I)



(II)



(I)	(*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
(II)	(*Browse*)	Selezionare un file esca
	(*Size coherence check*)	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 ≤ 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

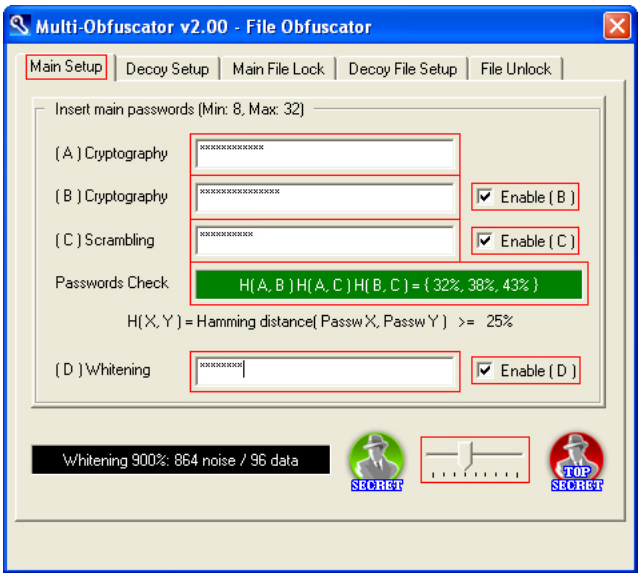
DECIFRAZIONE FILE – SETUP AVANZATO (4 PASSWORD+ESCA)

INIZIO:

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

Selezionare *File Lock/Unlock*.

PASSO 1:



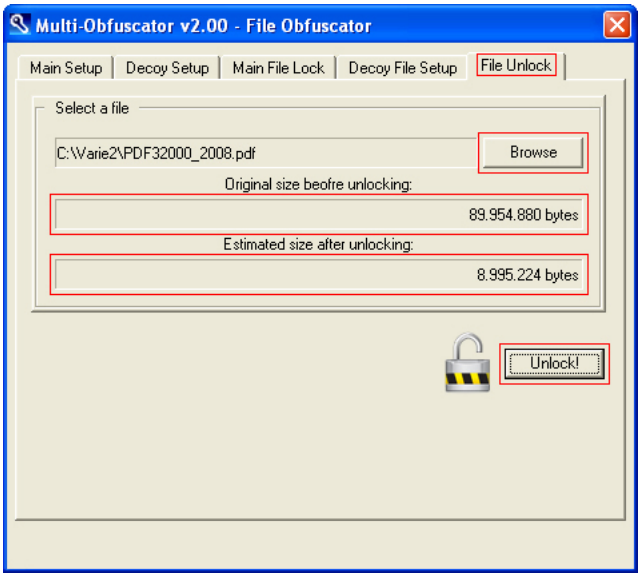
(*Cryptography A*)	La prima password (chiavi crittografiche)
(*Cryptography B*)	La seconda password (CSPRNG crittografico)
(*Scrambling C*)	La terza password (CSPRNG scrambling)
(*Whitening D*)	La quarta password (CSPRNG whitening)
(*Enable B*)	Abilita/disabilita la seconda password
(*Enable C*)	Abilita/disabilita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

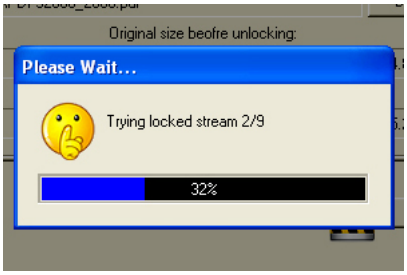
I dettagli completi sull'esca sono disponibili qui:
COSA È LA CRITTOGRAFIA NEGABILE?

PASSO 2:



(*Browse*)	Selezionare un file cifrato
(*Original size before unlocking*)	Esempio: 89.954.880 byte
(*Estimated size after unlocking*)	Esempio: 8.995.224 byte
(*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

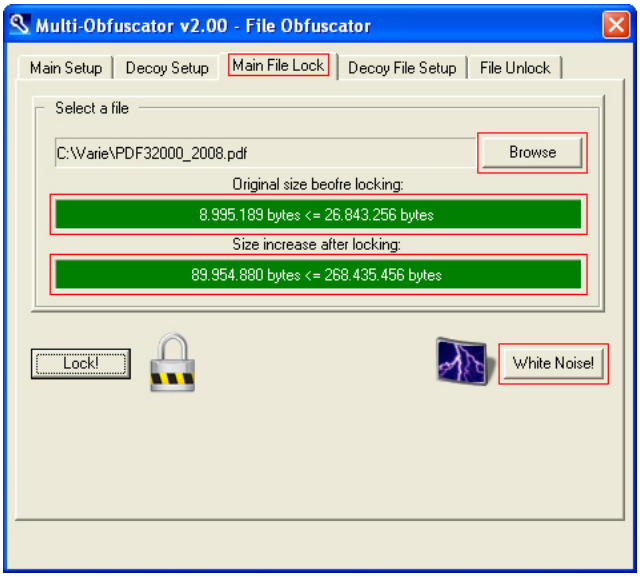
ESPERTO				RUMORE RANDOM COME ESCA (FILE)

INIZIO:

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

Selezionare *File Lock/Unlock*.

PASSO 1:



(*Browse*)	Selezionare un file
(*Original size before locking*)	Esempio: 8.995.189 byte
(*Size increase after locking*)	Esempio: 89.954.880 byte
(*White Noise!*)	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 = **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)

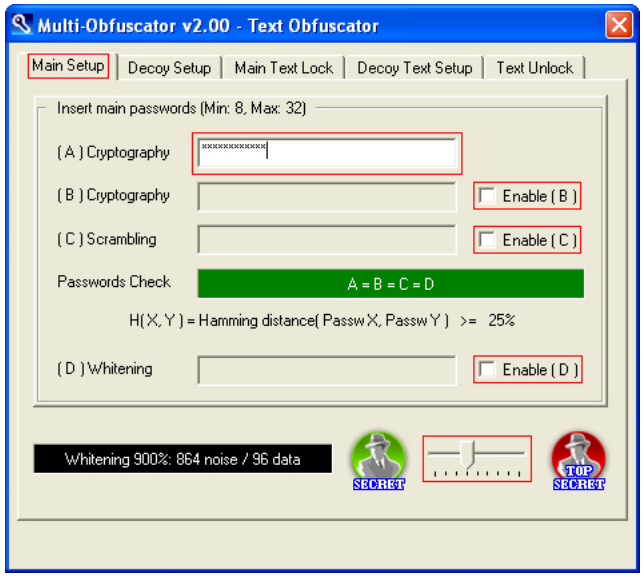
INIZIO:

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

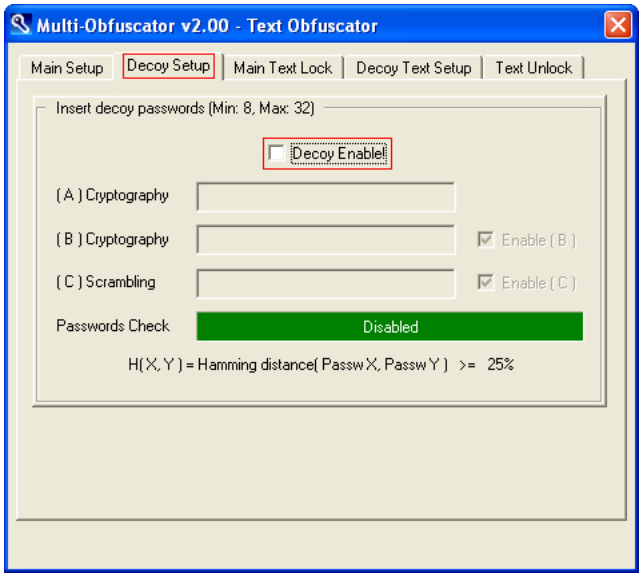
Selezionare *Text Lock/Unlock*.

PASSO 1:

(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

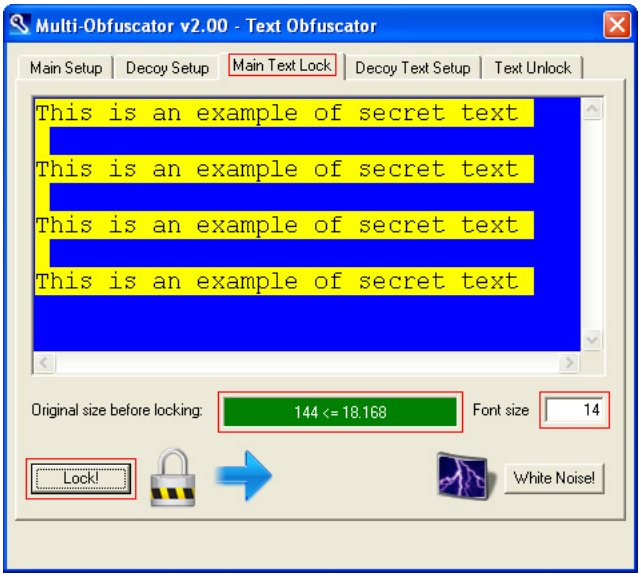
Inserire una password e selezionare un livello di rumore. I dettagli completi su password e rumore sono disponibili in speciali sezioni separate:

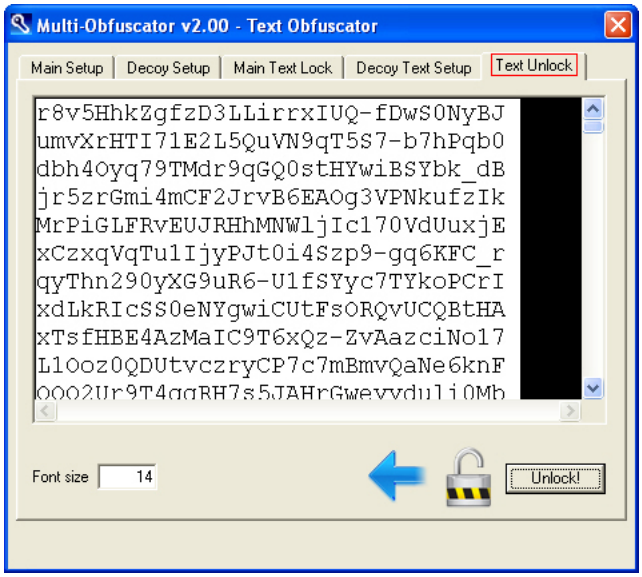
- SETUP DELLE PASSWORD SEMPLICE
- OPZIONI: LIVELLO DI RUMORE

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:

(I) 

(II) 

(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 ≤ 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

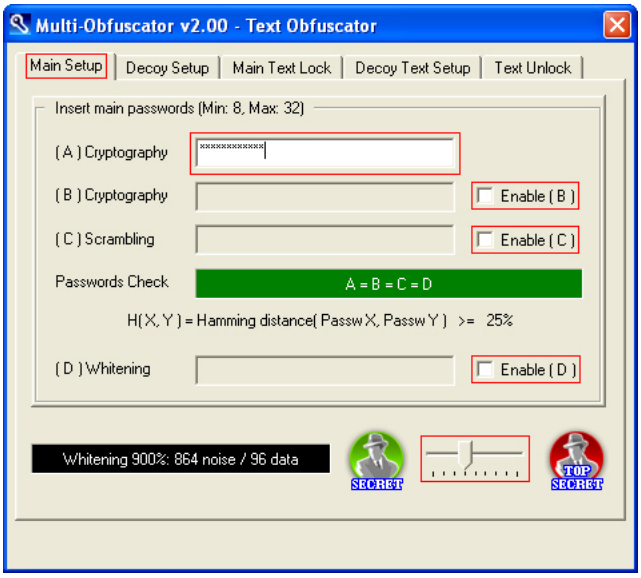
DECIFRAZIONE TESTO – SETUP DI BASE (1 PASSWORD)

INIZIO:

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

Selezionare *Text Lock/Unlock*.

PASSO 1:

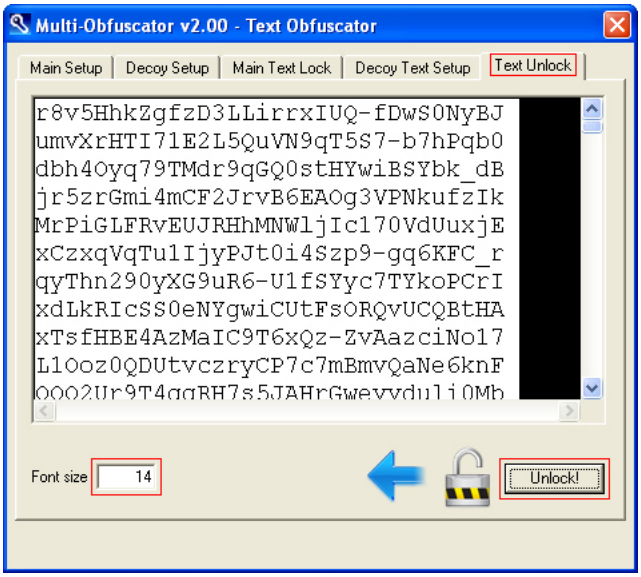


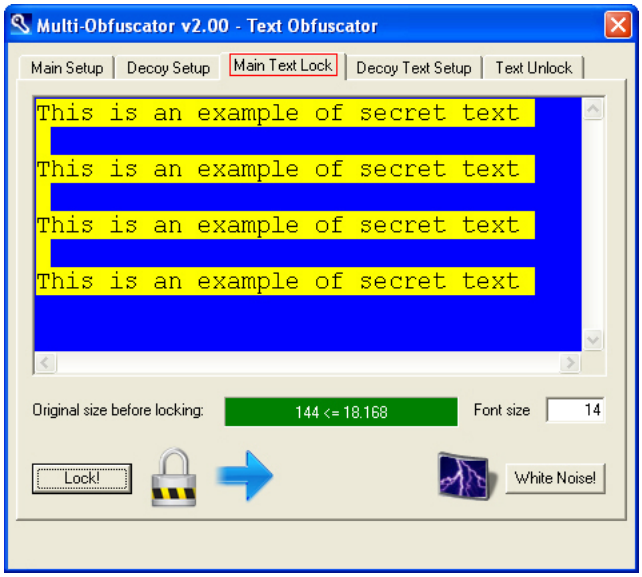
(*Cryptography A*)	La prima password
(*Enable B*)	Abilita/disabilita la seconda password
(*Enable C*)	Abilita/disabilita la terza password
(*Enable D*)	Abilita/disabilita la quarta password

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

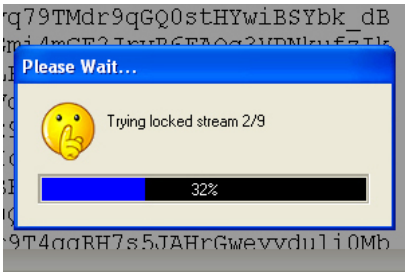
PASSO 2:

(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

MEDIO		

CIFRATURA TESTO – SETUP MEDIO (4 PASSWORD)

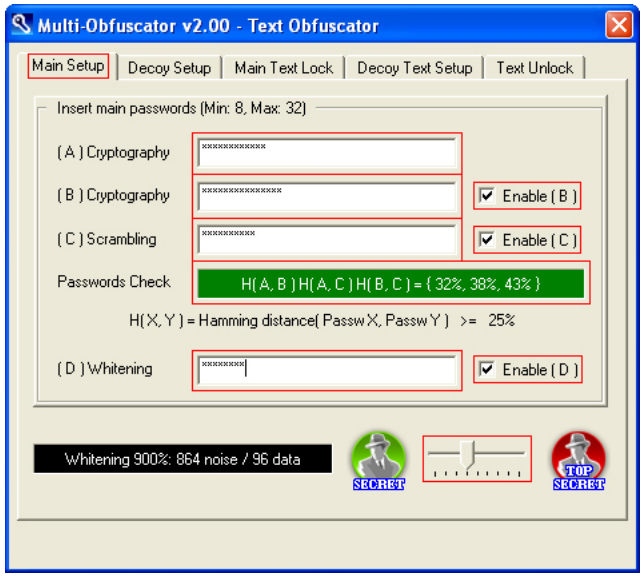
INIZIO:

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

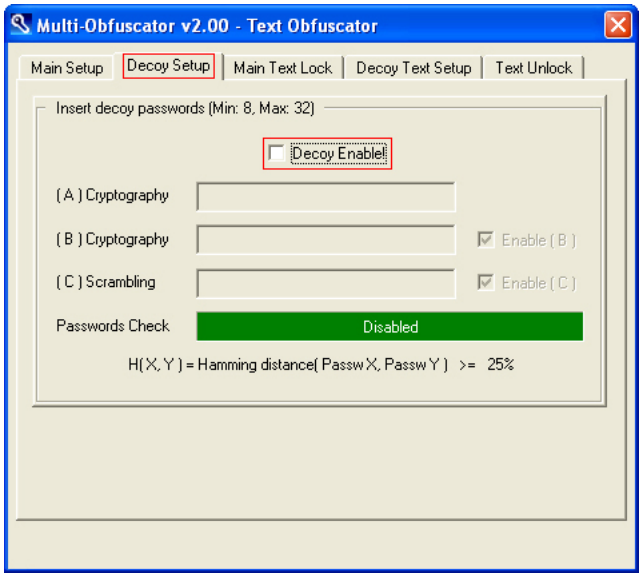
Selezionare *Text Lock/Unlock*.

PASSO 1:

(I)



(II)



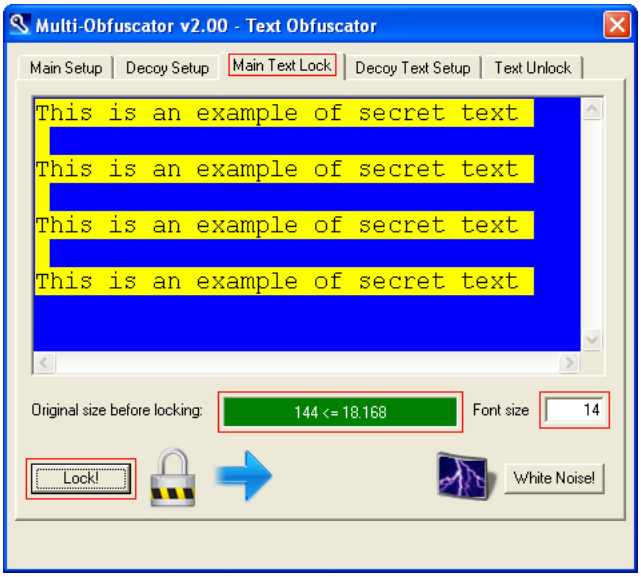
(I)	(*Cryptography A*)	La prima password (chiavi crittografiche)
	(*Cryptography B*)	La seconda password (CSPRNG crittografico)
	(*Scrambling C*)	La terza password (CSPRNG scrambling)
	(*Whitening D*)	La quarta password (CSPRNG whitening)
	(*Enable B*)	Abilita/disabilita la seconda password
	(*Enable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

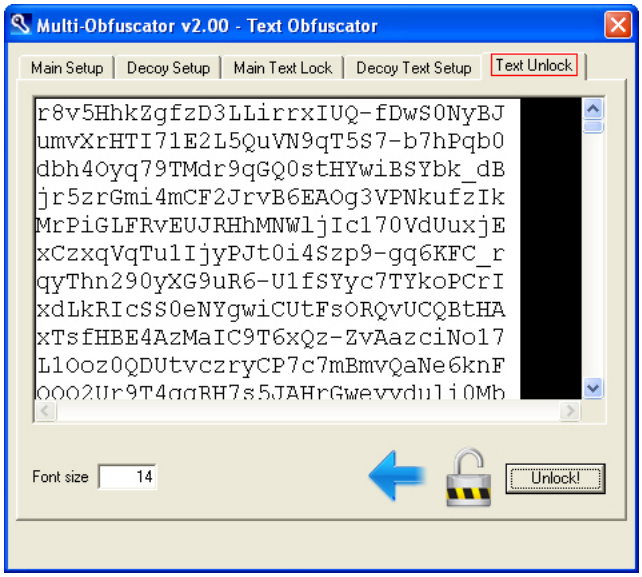
Inserire un'insieme di password e selezionare un livello di rumore. I dettagli completi su password e rumore sono disponibili in speciali sezioni separate:

- 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:

(I) 

(II) 

(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 ≤ 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

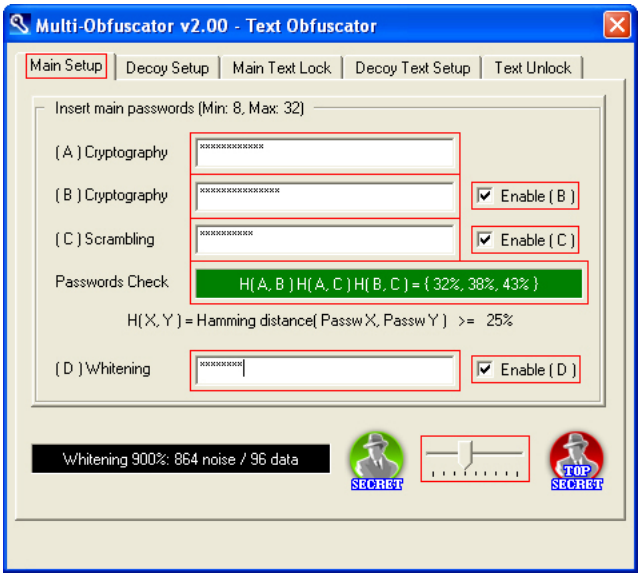
DECIFRAZIONE TESTO – SETUP MEDIO (4 PASSWORD)

INIZIO:

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

Selezionare *Text Lock/Unlock*.

PASSO 1:

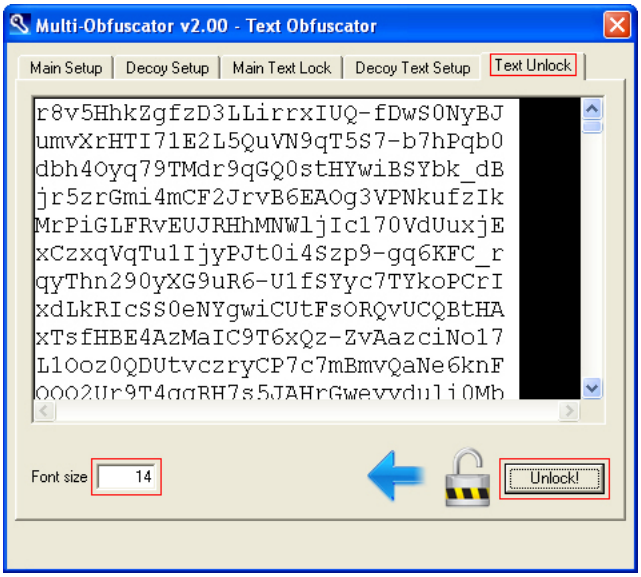


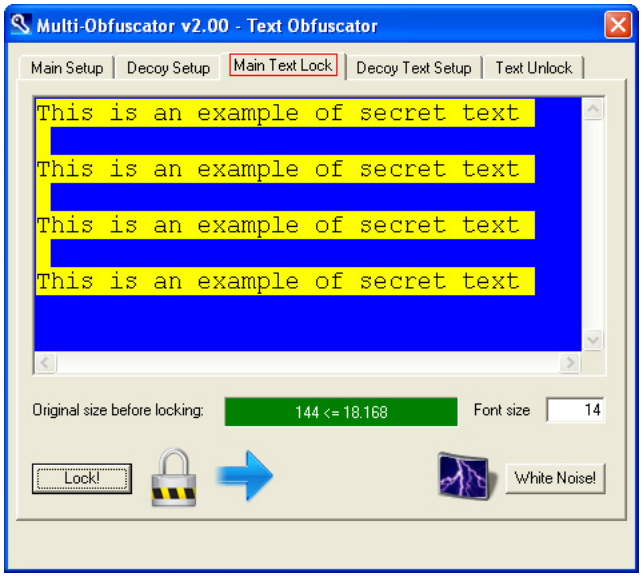
(*Cryptography A*)	La prima password (chiavi crittografiche)
(*Cryptography B*)	La seconda password (CSPRNG crittografico)
(*Scrambling C*)	La terza password (CSPRNG scrambling)
(*Whitening D*)	La quarta password (CSPRNG whitening)
(*Enable B*)	Abilita/disabilita la seconda password
(*Enable C*)	Abilita/disabilita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

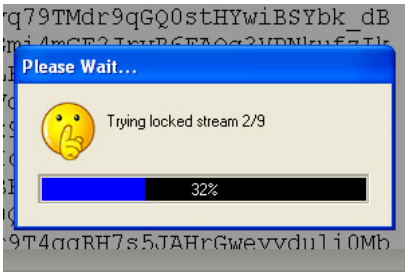
PASSO 2:

(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

CIFRATURA TESTO – SETUP AVANZATO (4 PASSWORD+ESCA)

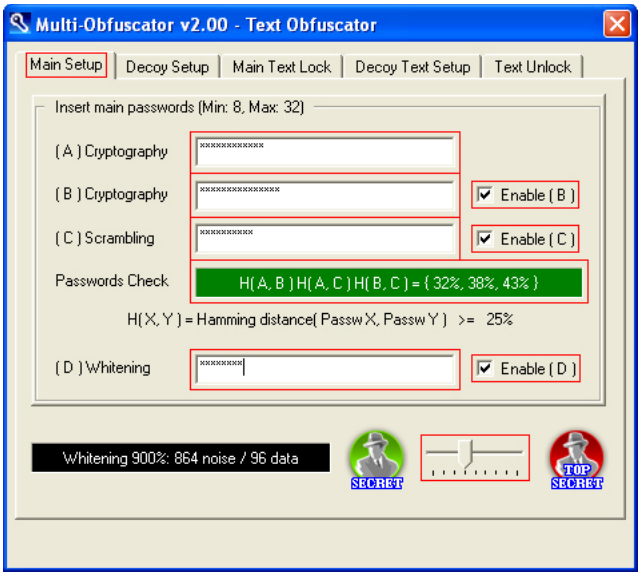
INIZIO:

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

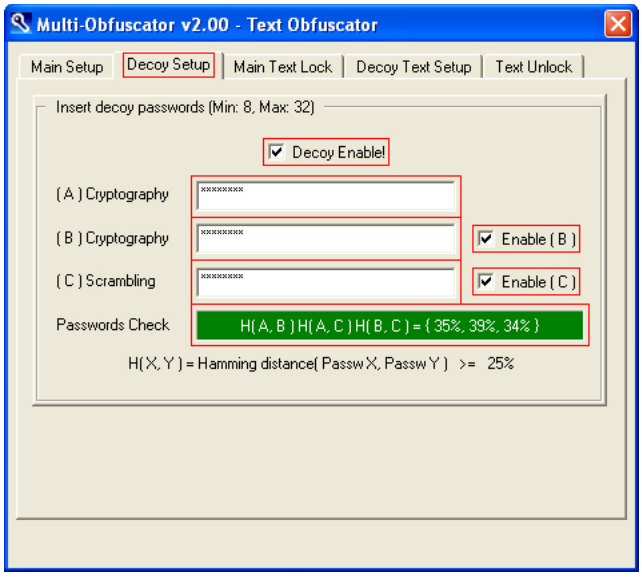
Selezionare *Text Lock/Unlock*.

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

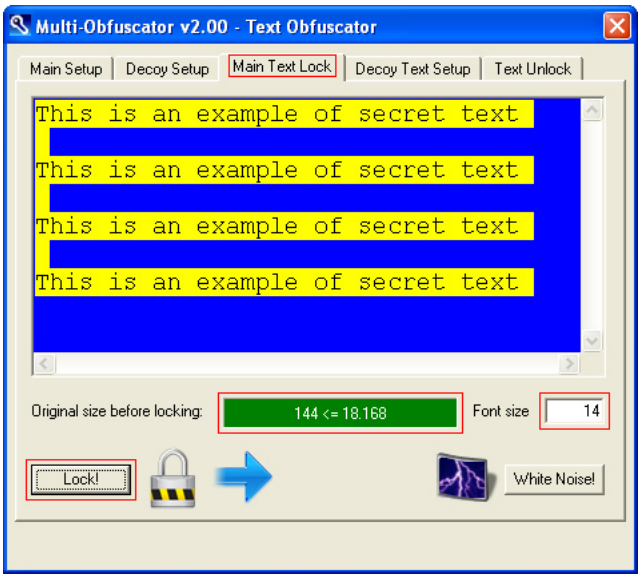
Inserire un'insieme di password, un'insieme di password esca e selezionare un livello di rumore. I dettagli completi su password e rumore sono disponibili in speciali sezioni separate:

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

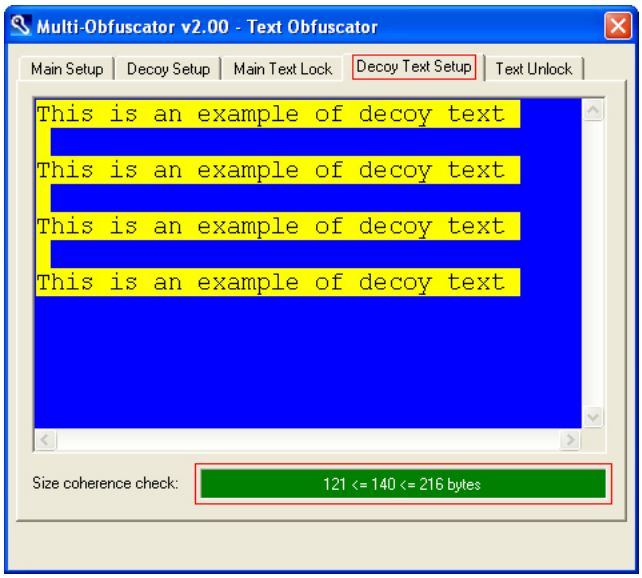
Il setup avanzato consente un uso completo dell'architettura di sicurezza multi livello e multi aspetto.
CARATTERISTICHE: ARCHITETTURA DEL PROGRAMMA

PASSO 2:

(I)



(II)



(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 ≤ 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

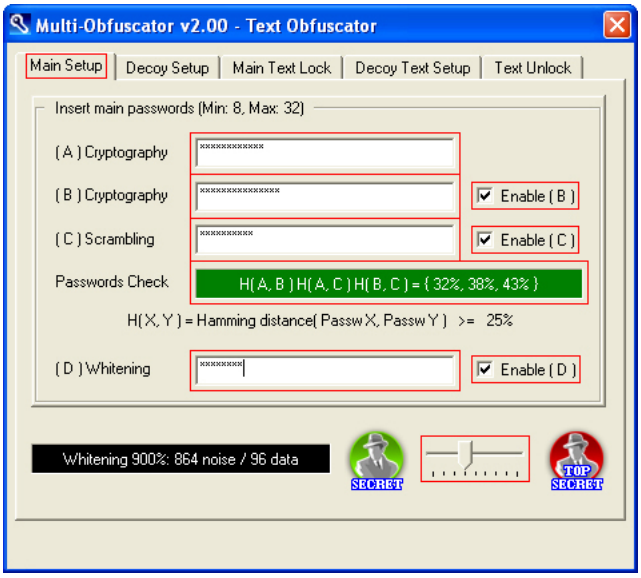
DECIFRAZIONE TESTO – SETUP AVANZATO (4 PASSWORD+ESCA)

INIZIO:

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

Selezionare *Text Lock/Unlock*.

PASSO 1:



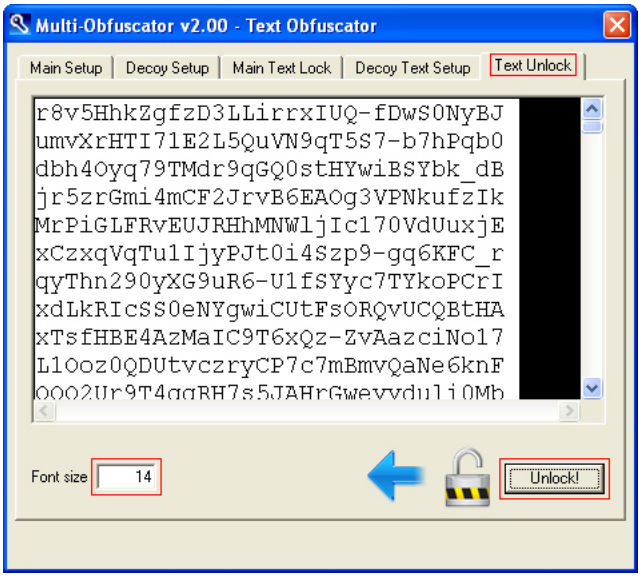
(*Cryptography A*)	La prima password (chiavi crittografiche)
(*Cryptography B*)	La seconda password (CSPRNG crittografico)
(*Scrambling C*)	La terza password (CSPRNG scrambling)
(*Whitening D*)	La quarta password (CSPRNG whitening)
(*Enable B*)	Abilita/disabilita la seconda password
(*Enable C*)	Abilita/disabilita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

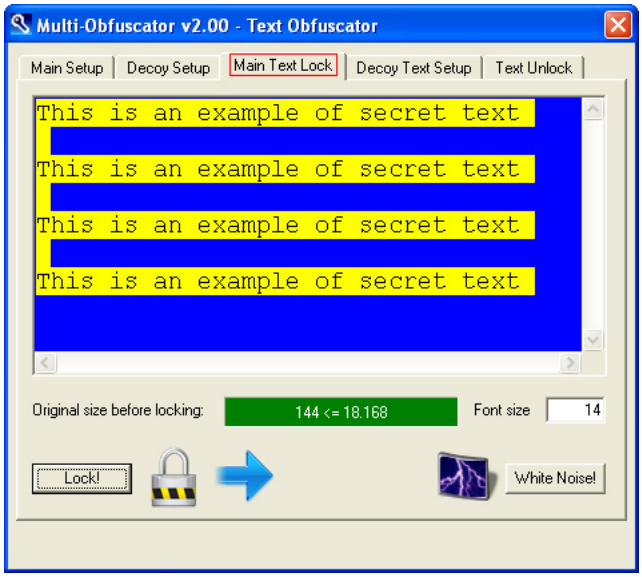
Impostare lo stesso insieme di password (segrete per estrarre i dati segreti, esca per estrarre i dati esca) e livello di rumore usati al momento dell'operazione di cifratura. I dettagli completi su password e rumore sono disponibili in speciali sezioni separate:

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

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

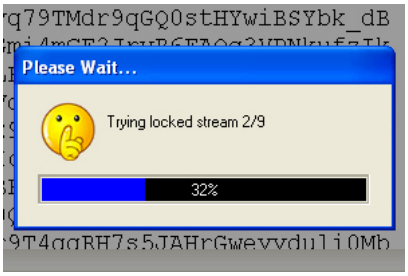
PASSO 2:

(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

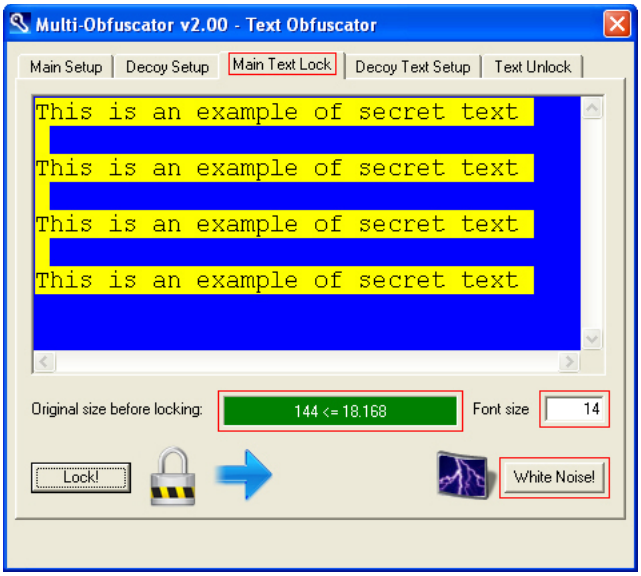
ESPERTO				**RUMORE RANDOM COME ESCA (TESTO)**

INIZIO:

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

Selezionare *Text Lock/Unlock*.

PASSO 1:



< 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 = **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