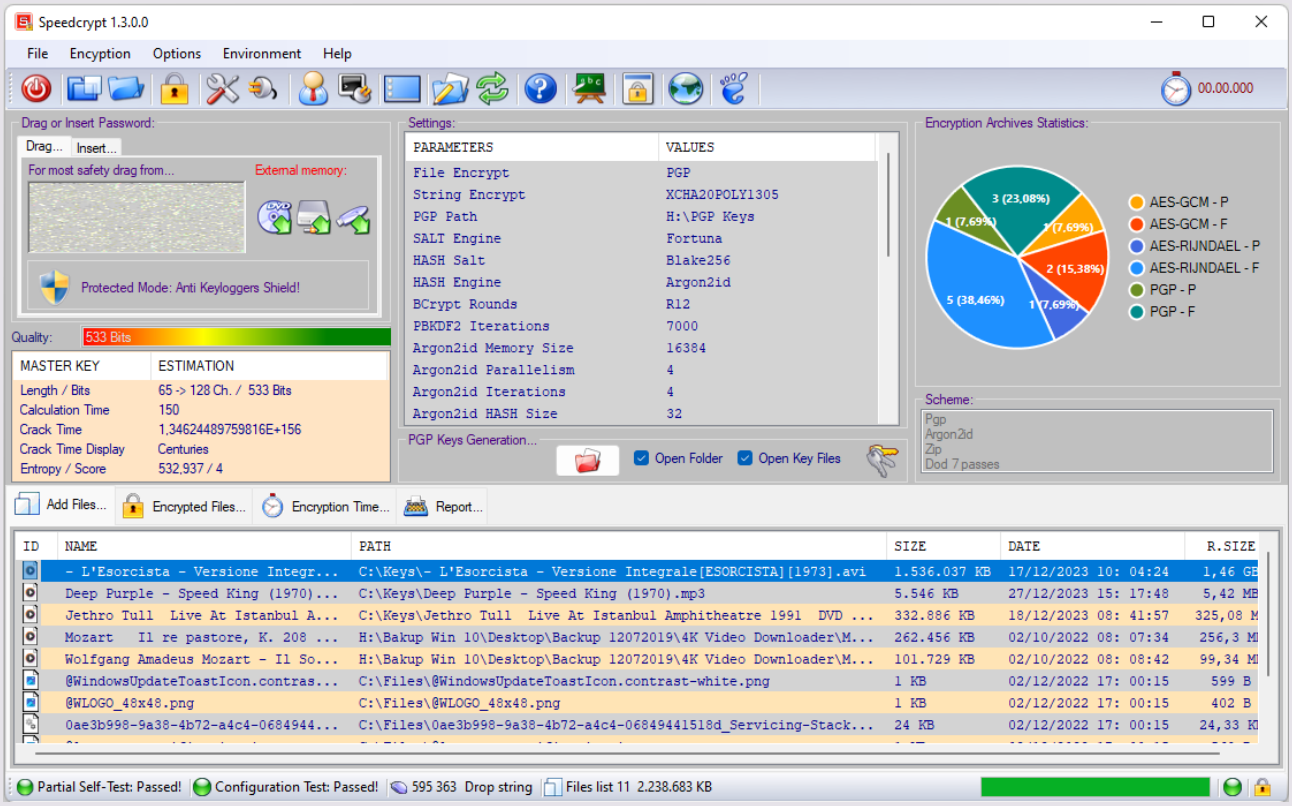
Speedcrypt Primi Passi: breve guida in lingua italiana.

OSI certified

Speedcrypt è un software concepito per cifrare file di ogni tipo e dimensione. Ideato e progettato dentro un protocollo che abbraccia in toto la filosofia *Open Source*. Il progetto viene infatti distribuito con il *Codice Sorgente*, in entrambe le versioni, *Setup Autoinstallante* e *Portabile*. Le versioni si differenziano per la gestione del file di configurazione e le operazioni dentro la *Modalità Protetta*, cioè il *Desktop Sicuro* creato da *Speedcrypt* per difendere la digitazione da tastiera contro gli attacchi dei famigerati *Keylogger*.



Speedcrypt Finestra Principale

Affinché il programma funzioni correttamente nel tuo sistema è importante che vengano rispettati i seguenti requisiti:

- *Sistema Operativo: Windows 7 o superiore. Ideale Windows 11*
- *CPU Tipo: Intel 64-Bit CPU Intel Core i7 o superiore*
- *Memoria: 4GB / 8 GB raccomandati*
- *Risoluzione Grafica: 1920 x 1980 o superiore*
- *Scheda Video: si adatta a quasi tutte le schede grafiche. Preferibili le nuove.*
- *Spazio su disco: 25 MB*
- *Mouse: Compatibile MS*
- *.NET Framework: 4.8 o superiore*
- *.NET Framework: 3.5 per entrare nella Modalità Protetta*

Nota: Il .NET Framework 3.5 è ancora utilizzato da tantissimi programmi ed averlo installato nel proprio sistema offre una buona piattaforma di lavoro.

Una volta che *Speedcrypt* è stato installato nel sistema oppure si decide di utilizzare la versione *Portabile* è bene ricorrere a determinati accorgimenti che rendono il software molto performante. Ecco quali sono i primi passi da compiere per ottenere il massimo da *Speedcrypt*:

- *Associare all'icona del programma i file cifrati*
- *Impostare uno schema di cifratura: di default Speedcrypt lo ha già composto per te.*
- *Abilitare la cancellazione automatica dei file che verranno decifrati. Da non attivare se intendi effettuare copie dei file cifrati.*
- *Eseguire il l'Autotest completo degli algoritmi contenuti nel progetto.*

Vediamo adesso in dettaglio come attuare queste operazioni preliminari che non sono obbligatorie, ma altamente consigliate.

***Associare all'icona del programma i file cifrati*:**

Enviroment/Windows Registry... [CTRL + W] ed il pulsante associato nella barra degli strumenti permettono di accedere alla finestra che consente l'associazione citata. Non ti resta altro che cliccare sul pulsante preceduto dalla dicitura *Add Key*. Per effettuare l'operazione inversa è sufficiente ricorrere al pulsante preceduto dalla dicitura *Remove Key*. Tutto estremamente semplice!

***Impostare uno schema di cifratura*:**

Speedcrypt mette a disposizione dei suoi utilizzatori diversi motori o algoritmi di cifratura da impiegare in base alle proprie esigenze, sistema, configurazione. Per quanto detto propone, quando avviato per la prima volta, uno schema di cifratura che ritiene adatto alla stragrande maggioranza degli utenti, schema che potrà chiaramente essere modificato, adattato, aggiornato come più lo si ritiene opportuno. Se abilitata l'impostazione di memorizzazione *Speedcrypt* creerà un archivio contenente i vari schemi realizzati dall'utente: questi potranno essere richiamati dopo la selezione tramite un solo click di mouse.

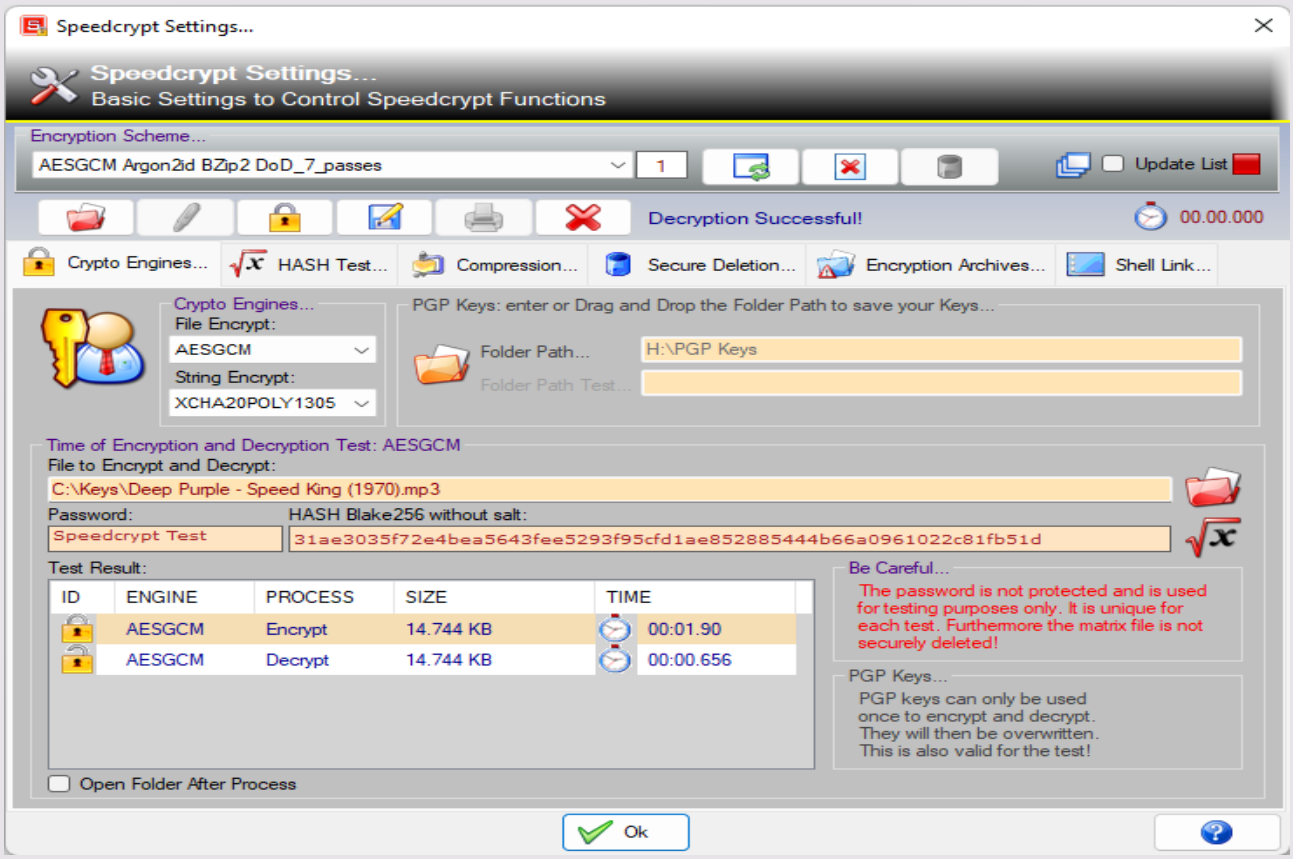
Quando si utilizza *Speedcrypt* per la prima volta, lo schema iniziale proposto nel progetto contempla le seguenti voci:

- *AES-GCM: il motore di cifratura dei file*
- *Argon2id: la funzione di HASH con la quale verrà derivata la Master Key*
- *BZip2: l'algoritmo di compressione dei file cifrati. Impostato ma non attivo.*
- *DOD 7 Passes: l'algoritmo di cancellazione dei file originali dopo un processo di cifratura.*

Questo è lo schema base, naturalmente *Speedcrypt* ha già impostato gli altri algoritmi che servono per un buon processo di cifratura dei file:

- *XCHA20POLY305: uno dei motori di cifratura per i SALT aggiuntivi.*
- *Fortuna: uno dei generatori di numeri pseudo casuali per la creazione dei SALT aggiuntivi.*
- *BLAKE 256: una delle funzioni di HASH con la quale verranno derivati i SALT aggiuntivi.*

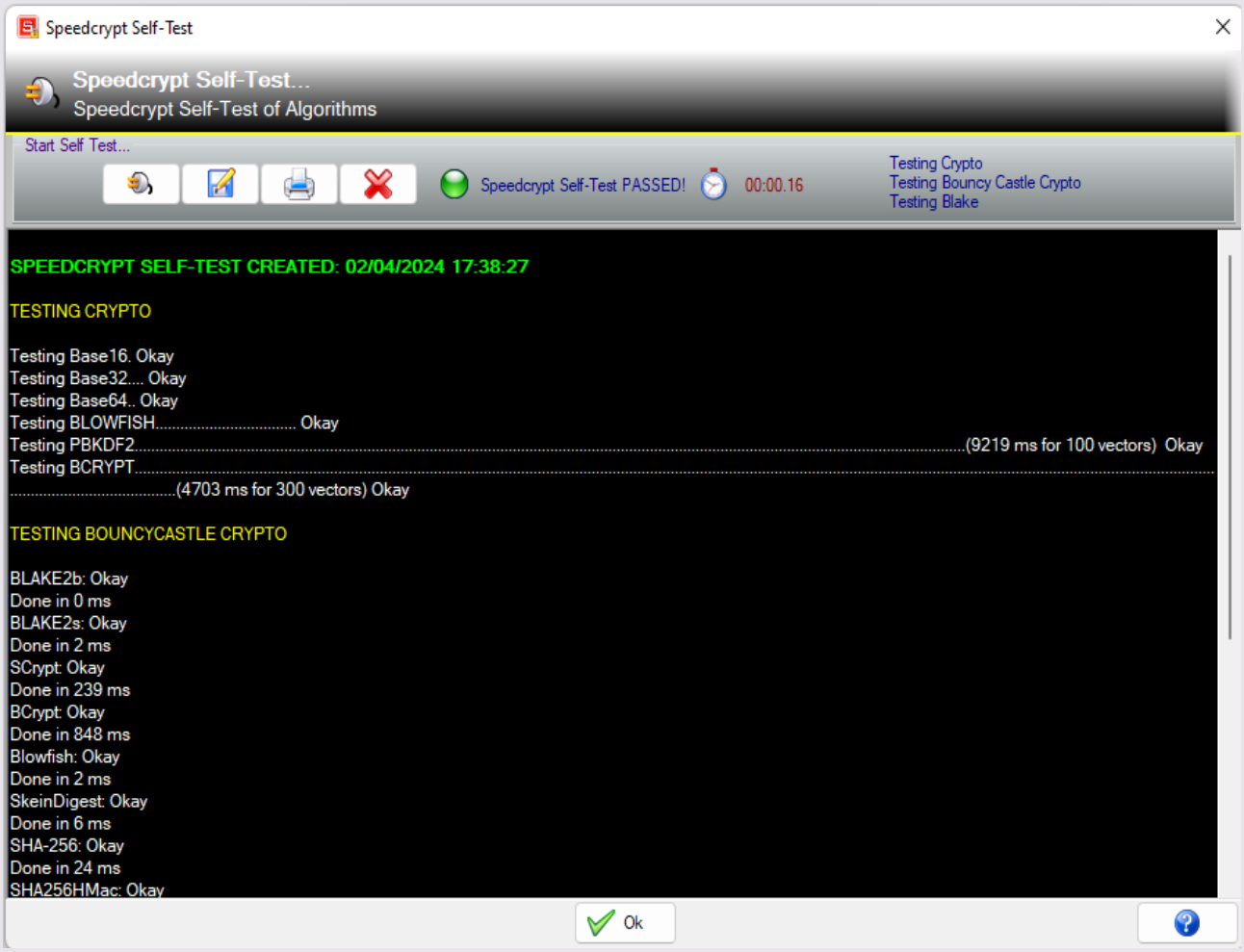
Options/Settings…[CTRL + S] ed il pulsante associato nella barra degli strumenti consentono di modificare lo schema base e tutte le altre opzioni.



Per abilitare la cancellazione automatica degli archivi è necessario accedere alla pagina denominata *Encryption Archives…* e trarre in spunta l'apposito pulsante. Nota: *quando la funzione in oggetto è attiva, dopo ogni processo di decifratura i file verranno cancellati dall'archivio*. Ciò implica che, se hai effettuato delle copie di questi file, per sottoporli ad un processo di cancellazione dovrai ricorrere al file di backup relativo alla configurazione del progetto. *Speedcrypt* aggiorna questo file ad ogni operazione relativa ai processi di cifratura e decifratura dei file.

Eseguire il l'Autotest completo degli algoritmi contenuti nel progetto:

Una buona prassi è sicuramente l'esecuzione periodica dell'Autotest tramite il quale *Speedcrypt* controlla il buon funzionamento dei propri motori. All'avvio viene eseguito un *Autotest Parziale* che restituisce all'utilizzatore una relativa tranquillità per quanto all'operatività del software. Il mio consiglio è di effettuare il *check - up* completo al primo utilizzo ed effettuare successivamente un controllo periodico. Un test viene effettuato anche sul file di configurazione per prevenire eventuali manomissioni dello stesso.



Options/Self-Test… [CTRL + T] ed il pulsante associato nella barra degli strumenti consentono di accedere alla finestra tramite la quale effettuare l'Autotest completo di tutti i motori ed algoritmi operativi all'interno del progetto. Il risultato potrà essere esportato dentro un file con estensione .txt oppure, se preferisci, stampato.

Una volta portate a termine le operazioni sopra descritte, le quali, come già accennato, *non sono obbligatorie ma vivamente consigliate*, sei pronto ad utilizzare *Speedcrypt*. Non ti resta che trascinare od importare la lista di file che intendi sottoporre ad un processo di cifratura, trascinare o digitare la tua *Master Key* ed avviare,

tramite la voce di menu *Encryption/Encrypt List…*[CTRL + Y] oppure il pulsante associato nella barra degli strumenti, la procedure che cifrerà la lista dei tuoi file.

Per ulteriori e più approfondite informazioni ti consiglio di consultare la Guida del progetto e l'Help Online che puoi trovare nelle varie pagine del mio sito. Chiedi al tuo Browser la traduzione automatica delle varie pagine, attualmente i traduttori integrati offrono prestazioni degne di nota. Per avere una reale consapevolezza delle potenzialità del progetto e come padroneggiare il software è bene soffermarsi a studiarne i meccanismi tramite le guide sopra menzionate.

Speedcrypt: il progetto in breve.

Caratteristiche principali

- *Progetto Open Source completamente libero e gratuito.*
- *Distribuzione con Setup autoinstallante e versione Portabile.*
- *Cifratura dei file di qualsivoglia tipo e dimensione.*
- *Due protocolli di inserimento della Master Key: per trascinamento o da tastiera.*
- *Valutazione e qualità della Master Key con i tempi relativi ad un eventuale crack.*
- *Creazione delle liste di file con la tecnica del Drag and Drop.*
- *Ordinamento gerarchico dei file cifrati.*
- *Generazione casuale di password robuste.*
- *Salvataggio della Master Key tramite codice PIN.*
- *Report sui tempi di cifratura e decifratura. Memorizzabile su disco.*
- *Report su eventuali eccezioni generate dal progetto. Memorizzabile su disco.*
- *Associazione dei file cifrati all'icona del progetto.*
- *Autotest parziale degli algoritmi e del file di configurazione all'avvio del programma.*
- *Autotest completo dei motori ed algoritmi operativi nel progetto.*
- *Dialogo con la Shell di Windows per inviare i file esternamente al progetto.*
- *Schema crittografico preimpostato, adattabile e memorizzabile.*
- *Test preliminari di cifratura, derivazioni HASH, compressione e cancellazione file. Memorizzabili su disco.*
- *Stampa dei test HASH e dell'autotest di motori ed algoritmi.*
- *Backup e ripristino del file di configurazione.*
- *Pulizia e ripristino degli archivi.*

Motori e algoritmi

- *Sette motori attivi per la cifratura dei file e delle stringhe associate.*
- *Sei generatori di numeri casuali.*
- *Quattordici funzioni di HASH per la derivazione delle Master Key*
- *Tre algoritmi di compressione dei file cifrati*
- *Cinque algoritmi di cancellazione dei file originali sottoposti al processo di cifratura*

Sicurezza del progetto

- *Protezione contro gli attacchi da Dizionario.*
- *Protezione dagli attacchi di ipotesi o forza bruta (Brute Force).*
- *Protezione dagli attacchi tramite Tabelle Arcobaleno.*
- *Protezione contro gli attacchi con i Memory Dump.*
- *Protezione dagli attacchi GPU/ASIC e Side-Channel*
- *Protezione dagli attacchi dei Keylogger*

Queste le caratteristiche salienti del progetto *Speedcrypt*, realizzato per poter garantire ai suoi utenti un elevato livello di praticità e sicurezza. Ad un primo approccio il programma potrebbe apparire non facile da utilizzare, ma come ben spiegato da Robert Condorache nel suo articolo di recensione '*Speedcrypt*' su Softpedia.com: "*Speedcrypt è un software utile per chiunque desideri proteggere i propri file e cartelle. Anche se all'inizio la sua interfaccia può sembrare un po' impegnativa, il programma non è difficile da manovrare dopo un po' di tempo con esso*".

Domande sulla sicurezza

Durante il periodo relativo ai test funzionali del *Progetto Speedcrypt*, mi sono state poste alcune domande da parte di utenti che non avevano alcuna dimestichezza con la *Crittografia* e la sicurezza dei dati. Di seguito alcune delle più interessanti:

- *Crittografare più volte i file già crittografati non aumenterebbe necessariamente la sicurezza e impedirebbe le modifiche da parte di un programma dannoso?*
- *La crittografia degli archivi di backup aumenterebbe la sicurezza impedendo le modifiche da parte di un programma dannoso?*
- *Crittografare il file eseguibile di Speedcrypt, il contenuto della cartella e i file di backup aumenterebbe la sicurezza impedendo le modifiche da parte di un programma dannoso?*

Alla prima domanda, risponderei che, in generale, crittografare i file più volte, noto come *Doppia Crittografia* o *Crittografia a Cascata*, non è raccomandato in quanto può portare a una diminuzione della sicurezza a causa della maggiore complessità e del potenziale di errori. *In genere è meglio utilizzare un algoritmo e una chiave di crittografia singoli e forti*.

Per quanto riguarda le altre due domande, la risposta è la stessa: NO. *Addizionare le precauzioni sopra descritte non servirebbe a nulla in termini di sicurezza*. *Speedcrypt* solleva uno scudo protettivo contro i *Keylogger*, il monitoraggio della chiave master, vari tipi di attacchi come *Dizionario*, *Dump della Memoria* e altro ancora, *ma sarebbero inefficaci se sul tuo sistema fosse presente un programma specificamente progettato per attaccare software come Speedcrypt*.

Ciò è documentato nella Law #1 delle Ten Immutable Laws of Security, come riportato nell'articolo di *Microsoft TechNet*. Ulteriori approfondimenti sono disponibili nell'articolo di *Microsoft TechNet* Revisiting the 10 Immutable Laws of Security, Part 1, in cui si afferma: "*Se un malintenzionato riesce a convincerti a eseguire il suo programma sul tuo computer, non è più il tuo computer!*".

Per evitare scenari come quello sopra descritto, è importante seguire delle regole che, se rispettate, possono rendere più sicuro il sistema su cui si opera, evitando così il furto dei propri dati:

 ***Il tuo Sistema***:

- *Se operi all'interno di un sistema Windows versione 10 e successive, affidati all'antivirus incluso nel sistema operativo chiamato Defender (il meno peggio in circolazione), assicurandoti di configurarlo con le migliori opzioni possibili. Lo stesso vale per il Firewall e tutte le altre opzioni di sicurezza offerte da questo Sistema Operativo.*
- *Non aprire mai allegati che provengono da e-mail sconosciute o che sembrano provenire da aziende di trasporto, banche, istituti di credito, etc.*
- *Naviga preferibilmente su siti Web noti, certificati e sicuri. Non scaricare e installare software da siti Web non affidabili.*

 ***Con Speedcrypt***

- *Controlla sempre tutti i dati che stai per inserire in Speedcrypt, dalle chiavi master alle liste di file da crittografare o decrittografare. L'inserimento di dati non verificati può creare problemi di sicurezza come la divulgazione di dati sensibili o l'esecuzione di codice fraudolento. Questo è un principio di base che deve essere applicato a ogni programma che usi nel tuo sistema.*
- *Inserisci sempre delle Master Key molto complicate, con Speedcrypt puoi farlo perché, una volta create dovrai solo trascinarle oppure importarle senza ricordarle carattere per carattere.*
- *Non applicare mai impostazioni di trasformazione chiave deboli soprattutto se suggerite da persone che potrebbero rivelarsi malintenzionate. Favoriresti solo un attacco ai dati crittografati.*
- *Se crei le tue Password affidandoti a un generatore suggerito da un malintenzionato, le tue Password saranno deboli di conseguenza favorirai un attacco ai dati crittografati.*
- *Se sei in contatto con altri utenti che utilizzano Speedcrypt e ti vengono affidati file da decrittografare nel tuo sistema, fai sempre attenzione. Potresti decrittografare file estremamente dannosi.*
- *Eseguire regolarmente un autotest completo degli algoritmi del progetto.*

Ricorda: se rispetti le regole di cui sopra e monitori attentamente le tue sessioni operative, nessuno degli attacchi sopra descritti avrà successo in quanto un attaccante ha sempre bisogno della tua complicità inconsapevole. Questo perché, trattandosi di operazioni di tipo manuale, un malintenzionato non può eseguirle da solo.

Per quanto riguarda la sicurezza con il progetto *Speedcrypt*, per ora è tutto. Fai buon uso di questi consigli e documentati il più possibile con testi sull'argomento e in siti seri che offrono materiale di altissimo livello. Imposta la strategia giusta per ottenere grandi risultati e proteggi i tuoi dati.
