TECNICHE DI CIFRATURA DEI FILES

Scritto da Giardino Matteo

Molte persone sono convinte del fatto che la sola password del proprio account utente di Windows costituisca una barriera impenetrabile anche da parte dei più esperti. In realtà non è così: sfruttando una tecnica di cracking come la tecnica delle "**Rainbow Tables**" (tabelle arcobaleno, in italiano) è possibile scoprire la password di un account di Windows in una manciata di secondi e accedere a tutti i dati memorizzati sul proprio hard disk.
L' unico modo per essere sicuri che nessuno possa accedere ai nostri dati più riservati è utilizzare un' apposito software e costruire un **disco virtuale cifrato**.
Un disco virtuale è un disco rigido che non è fisicamente presente sul computer ma è emulato da un apposito software.
Se il disco viene cifrato, ovvero tutto il suo contenuto viene protetto mediante un **algoritmo di cifratura** è veramente difficile, se non impossibile, riuscirvi ad accedere.

- CIFRATURA SIMMETRICA

Gli algoritmi di cifratura possono essere di tipo **"simmetrico"** se la chiave di cifratura è identica a quella di decifratura o "**asimmetrico**" se le due chiavi sono diverse.
I sistemi simmetrici sono generalmente a **blocchi** o a **flusso**. Gli algoritmi a blocchi operano su blocchi di dimensione fissa (solitamente di **64** o **128 bit**). Lo stesso blocco di testo in chiaro verrà cifrato sempre nella stessa maniera se la chiave rimane identica. Esempi di cifrari a blocchi sono l' **AES**, il **DES**, il **TDES** e il **Blowfish**.
Gli algoritmi a flusso generano un flusso di bit pseudocasuali, detto **keystream**, sul quale si esegue uno **XOR** (disgiunzione esclusiva) con il testo in chiaro. Questi algoritmi sono utili quando si devono generare flussi continui di dati. Esempi di cifrari a flusso sono l' **RC4** e l' **LSFR**.

- DES, TDES e AES

Il **Data Encryption Standard** (**DES**) è un algoritmo di cifratura a blocchi che fu scelto nel 1976 dal Dipartimento della difesa degli Stati Uniti come standard ma venne abbandonato nel 2001, quando venne giudicato insicuro per la maggior parte delle sue applicazioni. Molti suppongono che la segretezza di alcune caratteristiche del DES fu voluta dal-

la NSA (National Security Agency); altri sostengono che nel DES sia stata inserita una **backdoor**. Uno dei problemi principali del DES fu la lunghezza della chiave troppo limitata (solo ***56 bit***) che rendeva l' algoritmo vulnerabile ad attacchi di tipo forza bruta.

Per sostituire il DES, venne allora ideato il **Triple DES** (**TDES**), basato sulla ripetizione del DES per tre volte consecutive. La lunghezza delle chiavi utilizzate dal TDES è quindi ***56 · 3=168 bit***.

L '**Advanced Encryption Standard** (**AES**), denominato anche **Rijndael**, è l' algoritmo attualmente utilizzato come standard dal governo degli Stati Uniti d'America. La chiave utilizzata può avere dimensione ***128, 192 o 256 bit***.

Data la sua sicurezza e le sue specifiche pubbliche si presume che in un prossimo futuro venga utilizzato in tutto il mondo come è successo al suo predecessore, il DES. L' AES è stato adottato ufficialmente dalla **National Institute of Standards and Technology** (NIST) nel novembre del 2001.

– *BLOWFISH E TWOFISH*

Il **Blowfish,** fu ideato da Bruce Schneier nel 1993 ed è uno dei più diffusi algoritmi di cifratura. L' algoritmo Blowfish venne ideato come possibile sostituto dell' allora decadente DES. La dimensione della chiave può variare da **32 a 448 bit**, anche se generalmente si utilizza una chiave a **128 bit**.

Il **Twofish** fu uno dei cinque algoritmi finalisti nel concorso per la scelta dell' Advanced Encryption Standard, che fu poi vinto dal Rijndael. Fu inventato nel 1997 da Bruce Schneier. Il Twofish utilizza chiavi di ***128, 192 o 256 bit***.

Il Twofish e il Blowfish non sono stati brevettati ma rilasciati come dominio pubblico e per questo sono implementati in moltissimi software opensource.

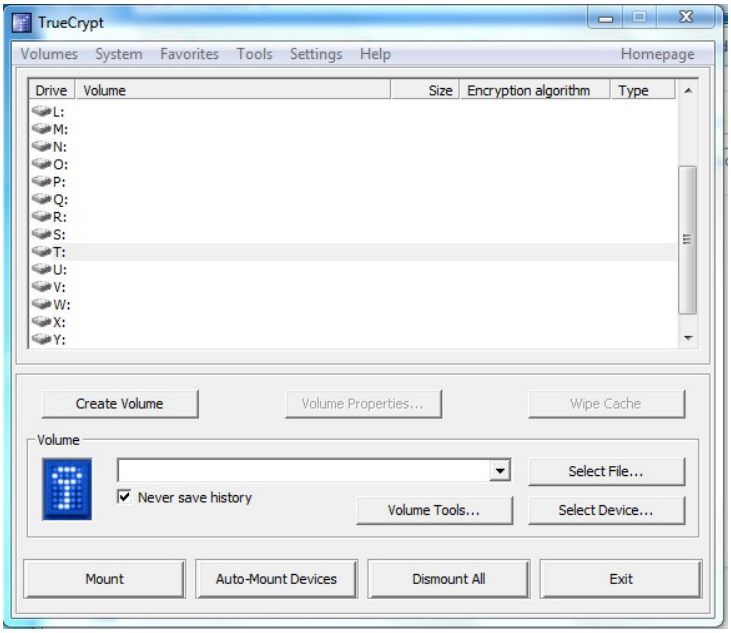
– *CIFRATURA ASIMMETRICA*

Gli algoritmi di tipo asimmetrico usano due chiavi: una pubblica e una privata. La **chiave pubblica** (che è resa pubblica) viene utilizzata per cifrare il messaggio, la cui decifratura può avvenire solamente con la **chiave privata**. I sistemi asimmetrici sono però molto più lenti di quelli simmetrici ma eliminano il problema dovuto alla scarsa sicurezza dei canali di comunicazione mediante il quale si comunica la chiave segreta.

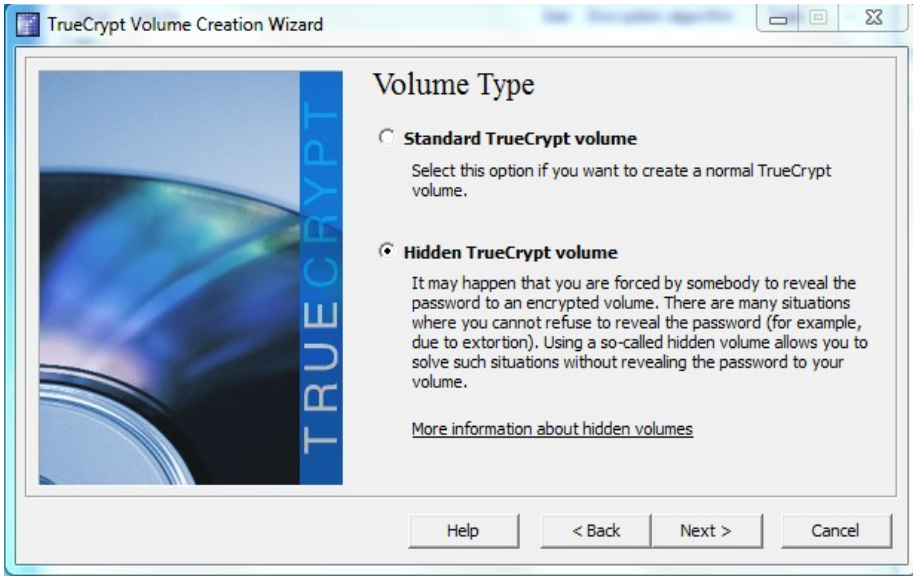
Esempi di sistemi di cifratura asimmetrica sono il **DSS** e il **Rabin**.

– *CREAZIONE DISCO VIRTUALE CON TRUECRYPT*

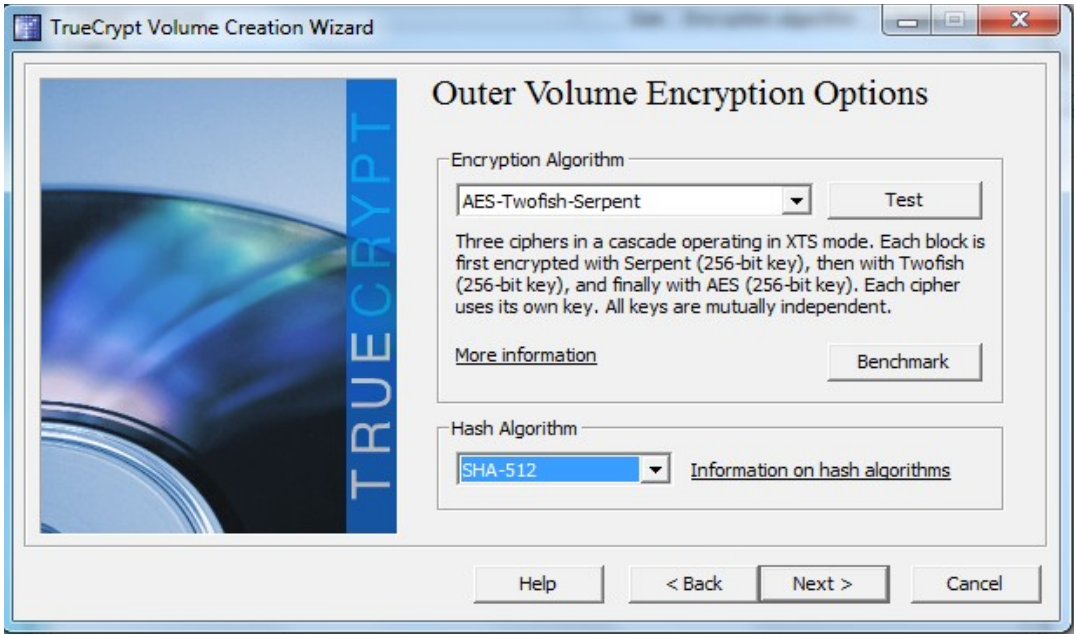
Una volta scaricata e installata l' ultima versione di Truecrypt dal sito ufficiale (www.truecrypt.org), avviare il programma. Nella schermata che appare seleziona la lettera da assegnare all'unità da creare e fare click su **Create Volume** per avviare il wizard di creazione.



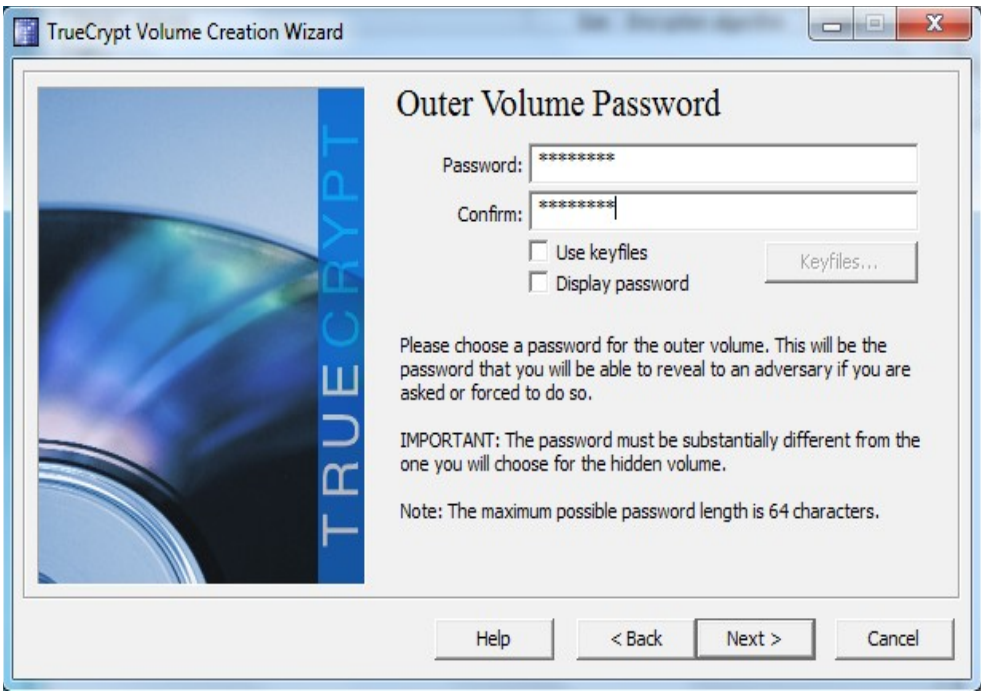
Nella schermata successiva selezionare la voce **Create an encrypted file container** e fare click su **Next** per procedere.
Verrà chiesto se la partizione da creare deve essere nascosta o no. Selezionando l' opzione **Hidden TrueCrypt Volume** (partizione nascosta) si potrà creare una partizione nascosta la cui esistenza non può nemmeno essere dimostrata.



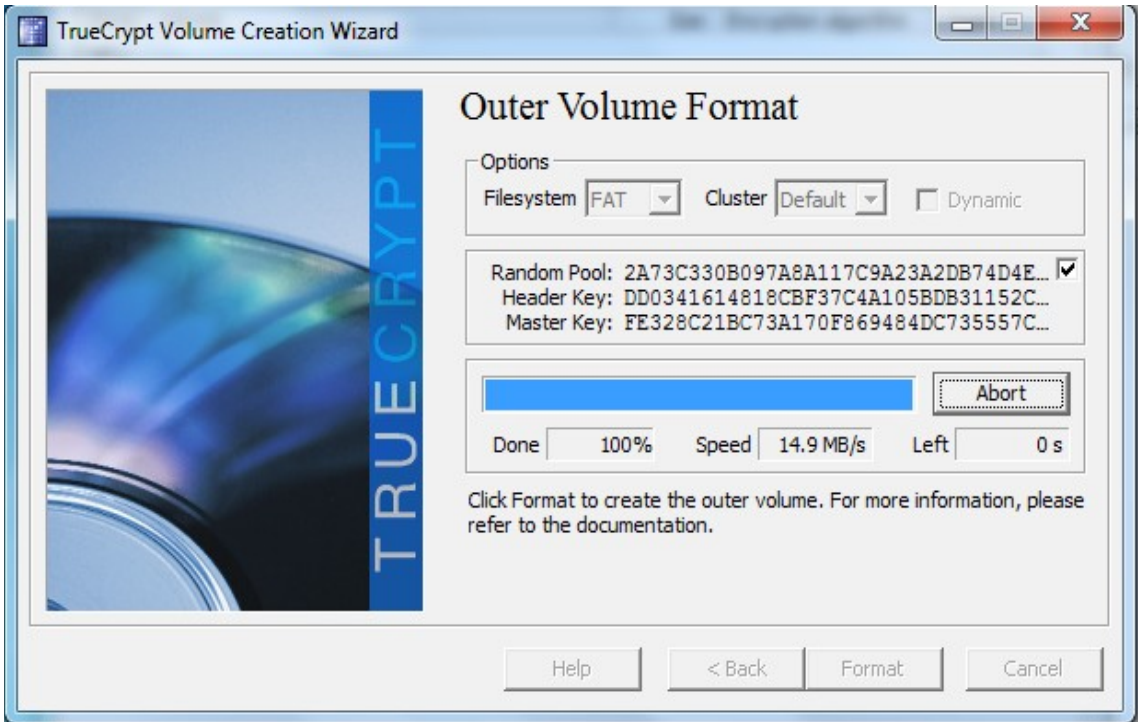
Scegliere l' opzione desiderata e premere su **Next** per procedere. Nella finestra che appare selezionare **Normal Mode** e premere **Next**. Nelle schermata successiva indicare il nome e il percorso in cui creare il file da utilizzare come contenitore della partizione e premere su **Next**.
A questo punto verrà chiesto di selezionare l' algoritmo da utilizzare per cifrare la partizione.



Si consiglia di selezionare l' algoritmo di cifratura **AES+Twofish+Serpent** e l' algoritmo di hash **SHA512**. Una volta effettuata la scelta premere **Next**. Indicare la dimensione del disco virtuale e premere nuovamente **Next**. Inserire la password di accesso al disco.



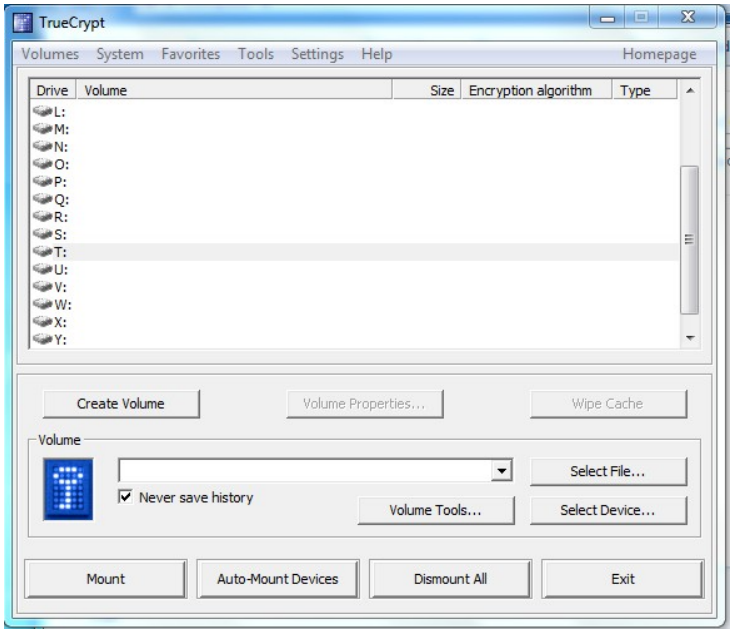
Come password è consigliato utilizzare sequenze casuali (almeno 8 caratteri) di lettere (maiuscole e minuscole), numeri e caratteri speciali (?,/, !, £, &, $, (,), ecc..). La lunghezza e la casualità della password hanno lo scopo di rendere più difficili gli attacchi a **forza bruta** e rendere addirittura impossibili quelli **basati su dizionario**.
Una volta inserita la password premere su **Next**. Selezionare il tipo di file system (consigliato **NTFS**) e premere **Format**. Attendere il completamento della procedura di creazione del disco.



A questo punto, a meno che abbiate selezionato la voce **Hidden TrueCrypt Volume**, la procedura è terminata e potete montare il vostro hard disk virtuale cifrato.
Se avete selezionato la creazione di un disco nascosto sarà necessario seguire una procedura identica a quella appena mostrata visto che si deve solamente creare un partizione all' interno di quella appena creata.

– *MONTARE/SMONTARE UN DISCO DI TRUECRYPT*

Per utilizzare un disco virtuale creato con TrueCrypt è necessario **montarlo**. Per fare ciò è sufficiente cliccare su **Select File** nella schermata principale, selezionare il file usato come contenitore per il disco che si desidera montare e fare click su **Mount**.
Verrà chiesta la password di accesso impostata durante il wizard di creazione. Inserire la password e fare click su **OK**.



Da questo momento è possibile accedere liberamente al disco virtuale cifrato la cui icona sarà visibile nelle **Risorse del Computer**. Per evitare che qualcuno possa accedere abusivamente al nostro hard disk virtuale, è opportuno, prima di chiudere TrueCrypt, fare click su **Dismount All** nella schermata principale.

– *BIBLIOGRAFIA DELLE FONTI*

John Erickson, *"L' arte dell' Hacking"*, Apogeo Editore, Milano 2008, p.441, € 45,00

AA.VV., *"Computer Forensics"*, Apogeo Editore, Milano 2007, p. 366, € 35,00

AA.VV., *"File blindati a prova d' intruso"*, da Win Magazine (giugno 2010 – anno XIII – n. 6), Edizioni Master

http://www.truecrypt.org/docs/?s=version-history

Contributori di Wikipedia, "TrueCrypt", *Wikipedia, L'enciclopedia libera*, http://it.wikipedia.org/w/index.php?title=TrueCrypt&oldid=36675298 (in data 3 dicembre 2010).

Contributori di Wikipedia, "Advanced Encryption Standard", *Wikipedia, L'enciclopedia libera*, http://it.wikipedia.org/w/index.php?title=Advanced_Encryption_Standard&oldid=35263163 (in data 3 dicembre 2010).

Contributori di Wikipedia, "Data Encryption Standard", *Wikipedia, L'enciclopedia libera*, http://it.wikipedia.org/w/index.php?title=Data_Encryption_Standard&oldid=36745784 (in data 3 dicembre 2010).

Contributori di Wikipedia, "Twofish", *Wikipedia, L'enciclopedia libera*, http://it.wikipedia.org/w/index.php?title=Twofish&oldid=34252312 (in data 3 dicembre 2010).