

Blowfish Advanced CS

Blowfish Advanced CS, noto anche con l'abbreviativo BFacs, è un programma distribuito in modo completamente gratuito che permette di crittografare file e intere cartelle su disco fisso e rappresenta la soluzione ideale per la protezione dei dati a livello locale (sul proprio personal computer o in rete aziendale LAN).

Le informazioni trasmesse via Internet non sono sempre sicure: una e-mail, per esempio, prima di arrivare a destinazione passa attraverso una "catena" di computer collegati in Rete e, durante questo passaggio, può essere intercettata da qualche malintenzionato per leggerne il contenuto. Quando si inviano via Internet documenti importanti, la soluzione migliore è quella di affidarsi ad appositi programmi che permettano di crittografare i propri dati.

La crittografia è una tecnica che permette di codificare le informazioni, di qualunque tipo esse siano, affinché solo le persone autorizzate possano entrarne in possesso.

Il sistema utilizzato da BFacs è quello a chiave simmetrica: esso implica la conoscenza della password impostata sia per l'operazione di codifica che per quella di decodifica. BFacs permette di crittografare file e cartelle utilizzando un congruo numero di algoritmi: Blowfish (algoritmo open source), Twofish, Rijndael, Cobra128, CAST, Idea, Mars, PC1, triple-DES ed altri ancora.

BFacs, contrariamente a quanto si possa pensare, è estremamente semplice da utilizzare e non necessita di installazione: può essere avviato facendo doppio clic sul suo file eseguibile (exe) e può essere addirittura lanciato da floppy disk (decompresso occupa solo 1,3 MB). Grazie a questa possibilità, BFacs può essere quindi utilizzato per crittografare dati personali sul personal computer di casa, al lavoro o su qualunque altro computer. Per aprire il software è sufficiente cliccare sulla simpatica icona a forma di pesce.



Avviato il software, apparirà la schermata principale di BFacs.

File Browser Tools Favorites Help Image: Section 1 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2	🕮 Blowfish Advanced C	s 🗐 🗍 🙋
Solution	File Browser Tools Favor	rites Help
Image: Content of the second set of the second set of the set of the second set of the set of the second set of the second set of the set of th	🗟 🌡 🌢	🖻 · 👔 且 🧼 🤣
	🖻 🖌 🔂 🗮 🖉 🗣	😳 🔠 🇰 🛛 🔹 💽 C:\Documents and Settings\Administrator\Desktop\blowfish

Tramite la barra contenente i pulsanti standard è possibile accedere a tutte le funzioni del software.



Per criptare un file o una cartella, sarà sufficiente selezionarlo dalla finestra principale e cliccare sull'icona raffigurante il lucchetto chiuso.



Nella schermata Encrypt si inserisce poi la password di codifica del file o della cartella scelti. Tramite tale finestra è possibile inoltre selezionare una serie di opzioni fra le quali: la visualizzazione della password durante la scrittura (Show Password), la compressione dei dati durante il criptaggio (Compress Data), la possibilità di rinominare il file criptato (Rename Files) o di scegliere la directory dove salvare il file criptato (Use Destination Path). Una volta inserita la password scelta, è necessario cliccare sul pulsante OK.

Encrypt			
🔽 🛛 se Cached Key			
Password:			
1			
☐ <u>S</u> how Password	Auto Confirmation		
∣ Cach <u>e</u> Key ∏ Use <u>K</u> ey Disk	Multi Key Input		
Compress Data	Store Original Pathnames		
Re <u>n</u> ame Files	Relative to Current Path		
	🔽 Keep Directories		
Use <u>D</u> estination Path:	Remo <u>v</u> e Source Files		
	<u>B</u> rowse		
	el <u>Apply</u> <u>H</u> elp		

Il programma chiederà una conferma della password scelta. Digitate di nuovo la password e cliccate sul pulsante OK.

Confirm		
Reenter the password:	ord:	
<u> </u>	<u>C</u> ancel	

Alla schermata che richiede la conferma di avvio della crittografia dei dati cliccate sul pulsante Sì.

Blowfish Advanced CS 🛛 🛛 🔀				
?	Found 1 file Start the e	e (1,655,695 by ncryption now?	/tes).	
	Sì	No		

Ultimato il criptaggio dei dati, il software vi presenterà una schermata di report dell'operazione o delle operazioni eseguite. E' possibile salvare tale report in formato txt o creare un file di lavoro con estensione bfj (blowfish job).

🐡 Job Report 📃 🗖 🔀				
Encryption Job				
Original File	Size	Encrypted To		
C:\Documents and Settings\Ad	1,655,695			
1 file (1,655,695 bytes) 00:00:01	Operation compl	iete.		
Save <u>C</u> reate Job File		<u>0</u> K	<u>H</u> elp	

Per decriptare una file sarà sufficiente selezionare il file criptato e cliccare sull'icona raffigurante il lucchetto aperto. La procedura di decriptaggio è identica a quella effettuata in precedenza per criptare il file.



Sarebbe cosa inutile crittografare file su disco se un malintenzionato, interessato a visionare i nostri documenti personali, avesse comunque la possibilità di recuperare gli originali facendo uso di particolari utilità undelete. BFacs include, allo scopo, un'interessante funzionalità (wiping) utilizzabile selezionando il file scelto e cliccando sull'icona contraddistinta dal disegno di una bomba con la miccia accesa (in figura) che permette di distruggere in modo permanente i dati cancellati.



Per accedere al setup del programma, cliccate sull'icona che raffigura il cacciavite ed il martello.



La schermata delle opzioni permette di scegliere il tipo di algoritmo di crittografia che si intende utilizzare, oltre ad un'altra serie di funzioni avanzate per il cui utilizzo si consiglia uno studio approfondito dei metodi di crittografia.

Options 🛛
Security Configuration File Handling Miscellaneous
Encryption Algorithm:
Bandom Number Generator: Yarrow
Wipe Method: Simple (1x)
Key Cache
Expiration Time (in secs) : 60
Cache <u>d</u> key never expires
<u>D</u> K <u>C</u> ancel <u>Apply</u> <u>H</u> elp

BFacs è un programma di semplice da utilizzare e rappresenta la soluzione ideale per la protezione dei file sul proprio personal computer. Attualmente non è stata ancora rilasciata una versione in italiano di BFacs, ma il programma mette a disposizione un file esterno che ne facilita, da parte di chiunque, la traduzione e la personalizzazione di menu e comandi.