Il codice MD5

Cos'è
E' una stringa a 128 bit, quindi 32 caratteri, risultato di un'operazione di hashing. Per semplicità si dice semplicemente MD5, ma il nome completo è MD5 checksum o MD5 hash. Calcolare l'hash MD5 di un file significa applicare una tecnica di hashing (un algoritmo) che estrae dal file una stringa che lo identifica univocamente.

A cosa serve
Gli hash MD5 dei file vengono utilizzati in almeno due circostanze.

1- **Download e copia dei file**

Ogni volta che si sposta, copia, muove o scarica un file, l'hash MD5 dice se il file è corrotto o meno. Se per esempio si è a conoscenza del valore di MD5 di un file possiamo verificare che sia integro ed esattamente uguale all'originale attraverso il calcolo dell'MD5 e confrontare la stringa con quella segnalata sul sito. Se il valore è identico, allora il file è identico a quello che c'è sul sito.

2- **Memorizzazione sicura delle password**

Un portale o un sito web che deve memorizzare le password degli utenti trova nei checksum MD5 un ottimo alleato. Infatti è sufficiente che il sito salvi nel proprio database non le password vere e proprie, ma il valore hash MD5 delle password.
Se anche un hacker si impossessasse di un MD5, non potrebbe risalire alla password che l'ha generato. Quando gli utenti accedono al sito e inseriscono la password, il portale calcola l'MD5 e lo confronta con quello memorizzato nel database. Se coincidono allora la password specificata dall'utente è corretta.

Si può decifrare? Diciamo subito che MD5 è una tecnica di hashing e non di crittografia. E la differenza non è di poco conto. La crittografia infatti è una funzione reversibile, ossia una volta cifrato qualcosa, se si possiede la chiave si può tornare indietro all'originale. L'hashing invece è un processo monodirezionale ossia una volta trovato un hash MD5 non è possibile tornare indietro. Da un hash non si può quindi risalire a ciò che l'ha originato, se non per (infiniti) tentativi.