

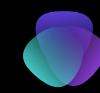


EPICODE: ATTACHI AI SISTEMI



S6/L3

Cracking passwords



Pratica di oggi

- Lo scopo di oggi è quello di provare a craccare le seguenti password:
-
- 5f4dcc3b5aa765d61d8327deb882cf99
- e99a18c428cb38d5f260853678922e03
- 8d3533d75ae2c3966d7e0d4fcc69216b
- 0d107d09f5bbe40cade3de5c71e9e9b7





Introduzione all'azienda

Le password mostrate precedentemente sono password hash, di tipo MD5.

Una password hash è una stringa di caratteri ottenuta tramite un algoritmo di hash, che è una funzione crittografica che trasforma i dati in ingresso in una stringa di lunghezza fissa.

Questo processo è unidirezionale, il che significa che è facile ottenere il valore hash a partire dai dati in ingresso, ma estremamente difficile ottenere i dati in ingresso a partire dal valore hash, soprattutto se si utilizzano algoritmi di hash crittograficamente sicuri.

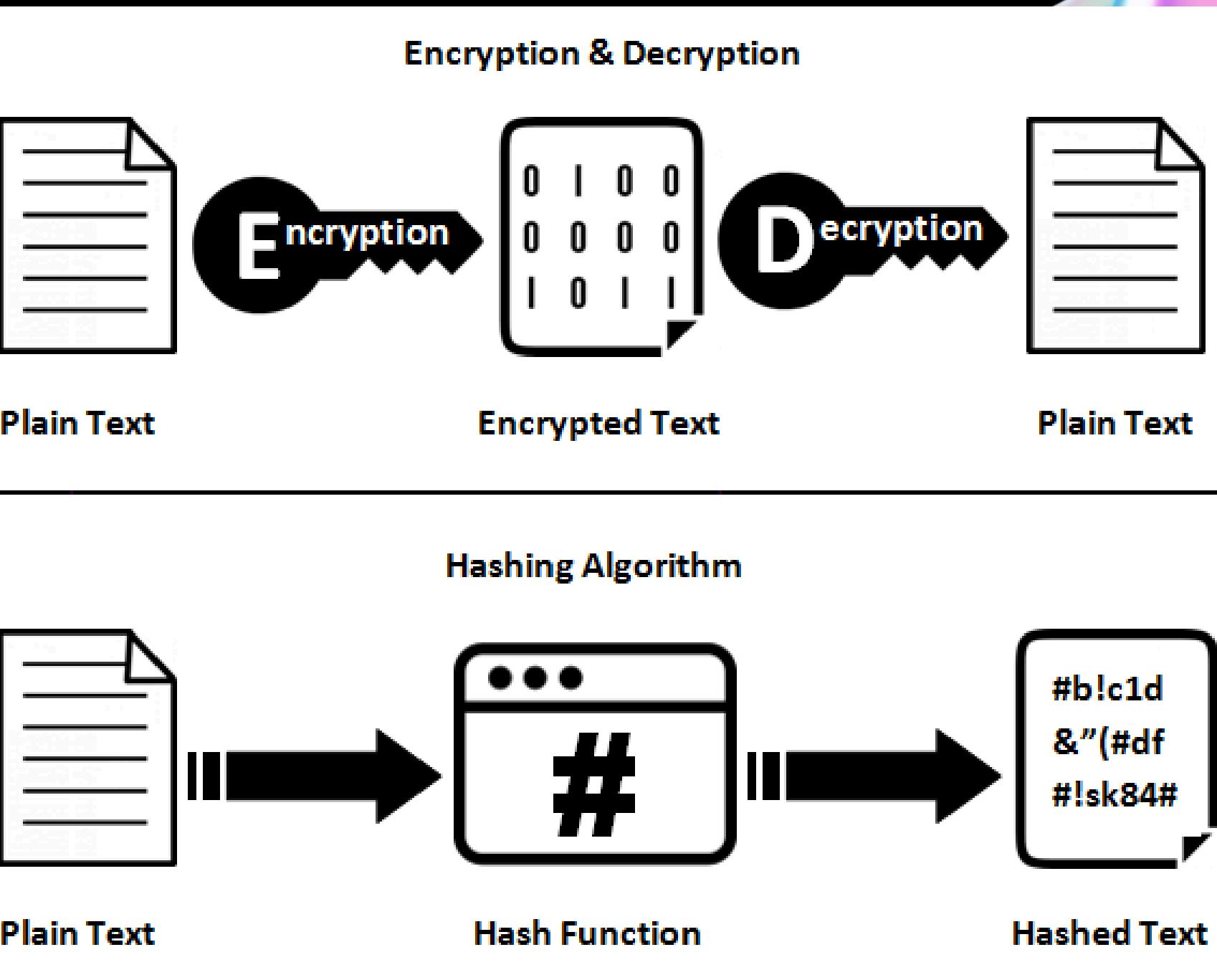
Le password vengono spesso hashate prima di essere memorizzate nei database per proteggerle in caso di compromissione del database stesso.

In questo modo, se un malintenzionato riesce ad accedere al database, non riesce a vedere le password in chiaro, ma solo i loro hash.

Quando un utente inserisce la password per il login, viene hashata nuovamente e confrontata con quella memorizzata nel database.

Se i due hash corrispondono, l'utente viene autenticato. Gli MD5 (Message Digest Algorithm 5) sono un algoritmo di hash crittografico progettato per produrre un hash di 128 bit a partire da dati di input di lunghezza variabile.

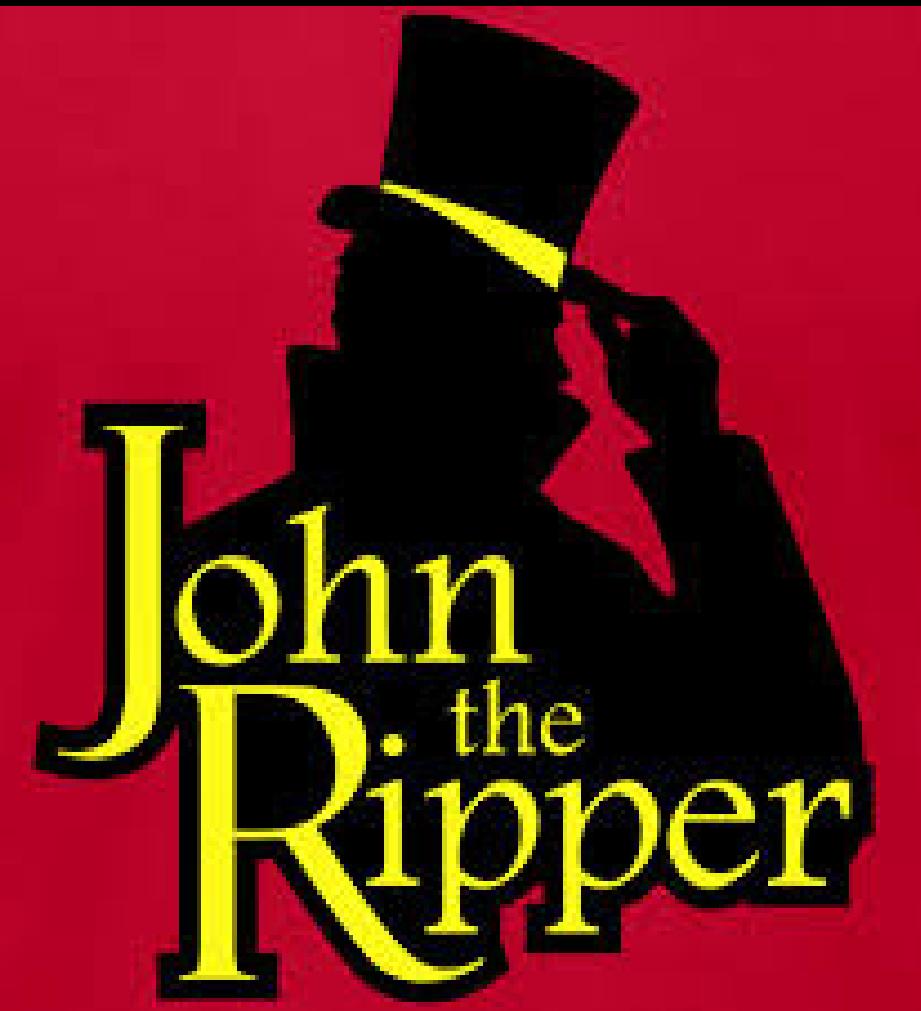
La caratteristica principale di MD5 è che produce un hash relativamente corto rispetto ad algoritmi più recenti, con l'avvento di tecniche come il "rainbow table", che consiste in una tabella pre-calcolata di hash di parole comuni, l'efficacia di MD5 è notevolmente diminuita per la crittografia delle password e di conseguenza il suo utilizzo è stato notevolmente ridotto.





Tool: John the ripper

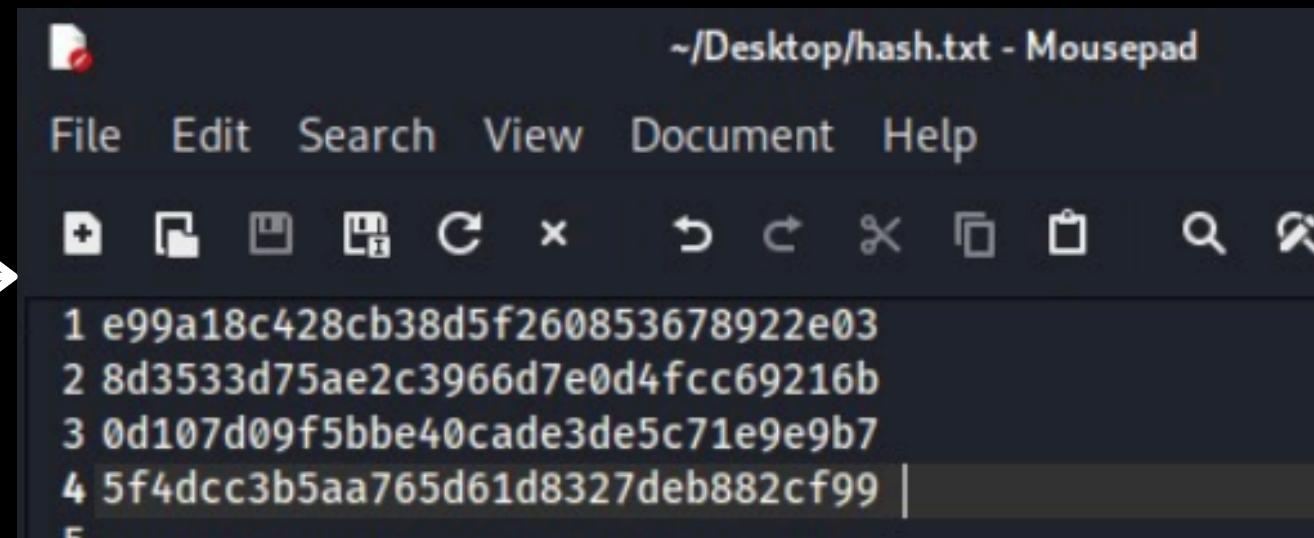
Per craccare le password esistono un sacco di tool, uno di questi è JONH THE RIPPER, John è uno dei tool più noti nel campo della sicurezza informatica. È un potente strumento utilizzato per il cracking delle password, progettato per recuperare le password dimenticate o per testare la robustezza della sicurezza delle password. JTR supporta varie modalità di cracking, tra cui il cracking basato su dizionario, l'attacco a forza bruta e l'attacco basato su pattern.





Tool: John the ripper

Per prima cosa apriamo un qualsiasi documento di testo e andiamo ad inserire le password da craccare.



Salveremo il file(hash.txt) su “Desktop” Successivamente lancieremo il tool JOHN, ci muoveremo nella directory Desktop, dove abbiamo precedentemente salvato il file con la password, e con il comando “`john --format=raw-md5 --incremental <nome del testo>`” il tool procedera con il cracking delle password.

```
(kali㉿kali)-[~/Desktop]$ john --format=raw-md5 --incremental hash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128]
Warning: no OpenMP support for this hash type, consider --fork=3
Press 'q' or Ctrl-C to abort, almost any other key for status
abc123      (?)
charley     (?)
password    (?)
letmein    (?)
```



Resultato

il risultato sarà invidenziato in arancione
nel terminal.

```
(kali㉿kali)-[~/Desktop]
$ john --format=raw-md5 --incremental hash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts!
Warning: no OpenMP support for this hash type,
Press 'q' or Ctrl-C to abort, almost any other
abc123          (?)
charley         (?)
password        (?)
letmein         (?)
```