

PROCEDURA PER LA FORMAZIONE DI PASSWORD COMPLESSE

Gruppo Eratostene

Tutti coloro che usano un computer sanno benissimo cos'è una password; in ogni caso Wikipedia (Rif.1) la descrive molto bene, in tutti i suoi principali aspetti.

In questo lavoro seguiremo i suoi consigli per formare password molto difficili da trovare, usando l'alfabeto latino con lettere miste maiuscole e minuscole, qualche cifra, qualche carattere speciale. Facciamo un esempio pratico.

In totale, per una password di **10** simboli, avremo:

26 lettere latine maiuscole

26 lettere latine minuscole

10 cifre da 0 a 9

20 caratteri speciali tipo ; , * ,) , % , & , ecc.ecc.

82, in totale con $82^{10} = 1,374480313 \cdot 10^{19}$, cioè circa

circa 1,37... per 10 miliardi di miliardi di disposizioni

tra le quali cercare una password di questo tipo con gli

appositi algoritmi. Controllando, per esempio, una

disposizione al secondo e tenendo conto che in un anno ci

sono 31 536 000 secondi, per terminare tutte le possibilità

occorrono $1,37 \cdot 10^{19} / 31\,536\,000 \approx 4,344241502 \cdot 10^{11}$

anni; che si riducono a $4,344241502 \cdot 10^1 \approx 4,3 \cdot 10 \approx$ **43**

anni se il controllo invece ora avviene, per esempio, ad

una velocità di 10 miliardi di disposizioni al secondo

usando i moderni supercomputer (o anche **4,3** anni se la

velocità fosse invece di 100 miliardi di disposizioni al

secondo. In entrambi i casi un tempo lunghissimo,

insomma, durante il quale si può cambiare password, e ricominciare tutto daccapo..

Tipo di password di dieci simboli utilizzando tali consigli e tali caratteri alfabetici, numerici o speciali:

MaRy&39!?!+

scelti tra l'inizio, la parte centrale e finale di ogni serie per allungare i tempi di calcolo.

Il vantaggio di questo tipo di password è ovviamente l'enorme difficoltà a trovarle, e quindi il grande tempo di calcolo occorrente (Rif.2); il problema è invece che bisognerebbe ricordarle a memoria, ed è difficile; in caso contrario occorre scriverle da qualche parte, con il rischio di furto, distruzione o perdita del supporto cartaceo (il solito semplice bigliettino) oppure informatico (CD, DVD, penna USB, ecc.).

Per i nostri file, qualora occorresse in futuro, useremo

certamente password di questo tipo, a maggior protezione dei nostri lavori che eventualmente necessitassero di una certa protezione.

Caltanissetta 1.10.2010

Riferimenti

- 1) Voce “Password” di Wikipedia
- 2) Articolo di Mauro Vecchio “FBI, se la password è un rompicapo ” sul sito “ punto-informatico.it/ “