

Esercizi

Lezione 8: Crittografia

Per affrontare i seguenti esercizi potrebbero essere utili le slide ed eventuale documentazione reperita online.

Esercizio 1

creazione di hash

Creare uno script PHP che, mediante l'uso della funzione `hash()` presentata a lezione crei l'hash di una stringa a piacere.

Cosa succede cambiando la stringa? È possibile ottenere due hash uguali? Quanto è lunga la stringa ottenuta e quanti bit pesa? (Per rispondere alla prima avvalersi di uno script PHP che usa la funzione `strlen()` passando come argomento la stringa ottenuta).

Esercizio 2

criptare e decriptare stringhe

Creare uno script PHP che, mediante l'uso dello script PHP presente a questo link, cripti e decripti delle stringhe e ne stampi il risultato a schermo. Provare ora a decriptare due stringhe, cosa succede?

Che meccanismo di crittografia stiamo usando? Come potrebbe essere utile in un'applicazione web?

Esercizio 3 - svolto

gestione utenti avanzata

Data la tabella *utenti* della base di dati allegata a questo esercizio progettare uno script PHP in grado di prelevare dalla suddetta i dati degli utenti e di stamparli decriptati in forma tabellare. Una volta fatto ciò inserire un form HTML per inserire un nuovo utente che, naturalmente, dovrà essere inserito con i dati crittografati nella base di dati attuando le corrette scelte sul meccanismo di criptazione dei dati.