

Login “sicuro” - versione 2: cifratura delle password

Nel server si vuole implementare la memorizzazione cifrata delle password. A questo scopo occorre utilizzare un algoritmo di cifratura simmetrica, poiché il server, per costruire il *ticket* da confrontare con quello ricevuto dal client, necessita di elaborare la password in chiaro.

Note sull'implementazione

Gestione account: cifratura/decifratura password

Nel componente di gestione degli account occorre:

- Aggiungere (o modificare, se esiste già) un metodo che inserisca un nuovo account e che cifri la password prima di memorizzarla.
- Modificare il metodo che recupera la password, in modo che sia in grado di decifrarla.

Implementazione del cifrario di Vigenère

Implementare un proprio componente di cifratura, che usi il cifrario di Vigenère.