Laboratorio di sistemi– classe 5ª – data 30/1/2020

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.

Nota bene: in tutto questo, dove siano memorizzate le password cifrate è irrilevante. (È possibile gestire tutto in memoria, memorizzando le password in una lista statica.)

Implementazione del cifrario di Vigenère

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

Astrarre il componente di cifratura

Creare un tipo astratto che fornisca la cifratura / decifratura delle password e che sarà utilizzato nel codice applicativo del server.

Questo tipo sarà implementato da due componenti concreti:

1. Un componente che farà da “adattatore” dell’oggetto di cifratura simmetrica definito dal .NET Framework.
2. Un componente che implementa il cifrario di Vigenère.