

Sicurezza dei Sistemi Informatici

Prof. Stefano Paraboschi

Prova del 14/6/2011

- A. Progettare un protocollo crittografico che consenta ad Alice di prendere un impegno su un bit al tempo t_1 con n altri utenti. Il bit scelto può essere svelato da Alice al tempo $t_2 > t_1$ solo con la cooperazione di tutti gli n utenti.
- B. Illustrare sinteticamente i vantaggi e gli svantaggi del modello di analisi della safety di una policy *Take-Grant*.
- C. Descrivere le motivazioni che giustificano l'introduzione della poliistanziamento nelle basi di dati relazionali multilivello. Si descrivano in particolare i concetti di *poliistanziamento visibile* e di *poliistanziamento invisibile*.