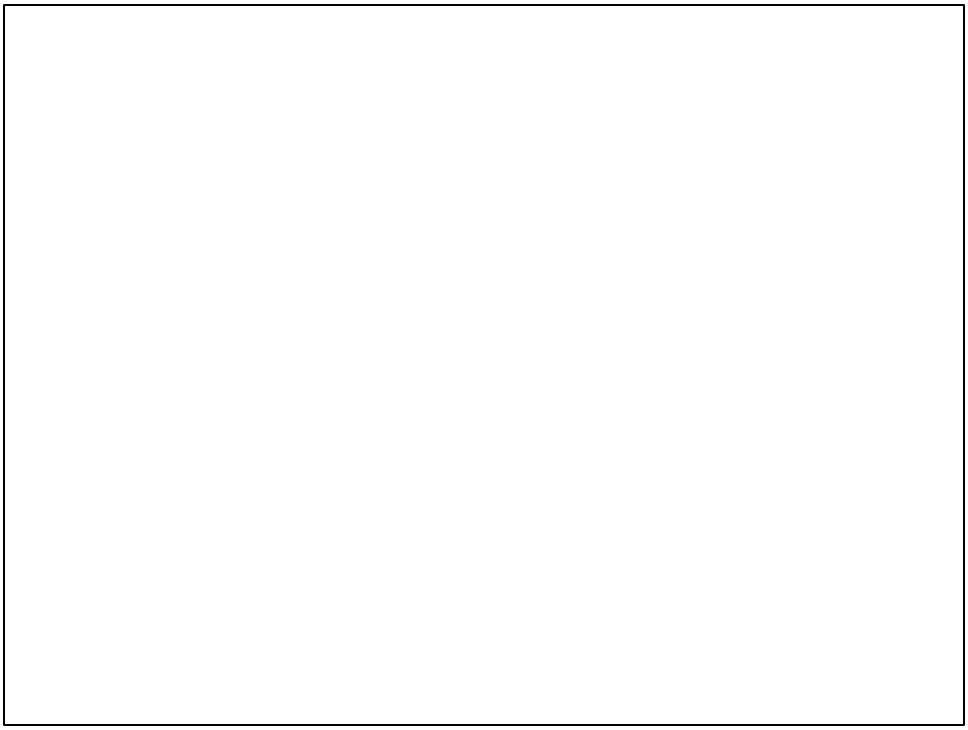
esercizi su pianificazione, progetto e leggi



entità in gioco:

utente

autorità

metti timestamp(m: documento)

utente: h=hash(m)

utente: invia h all'autorità

autorità: t è un timestamp, $tf=[h|t]_{autorità}$

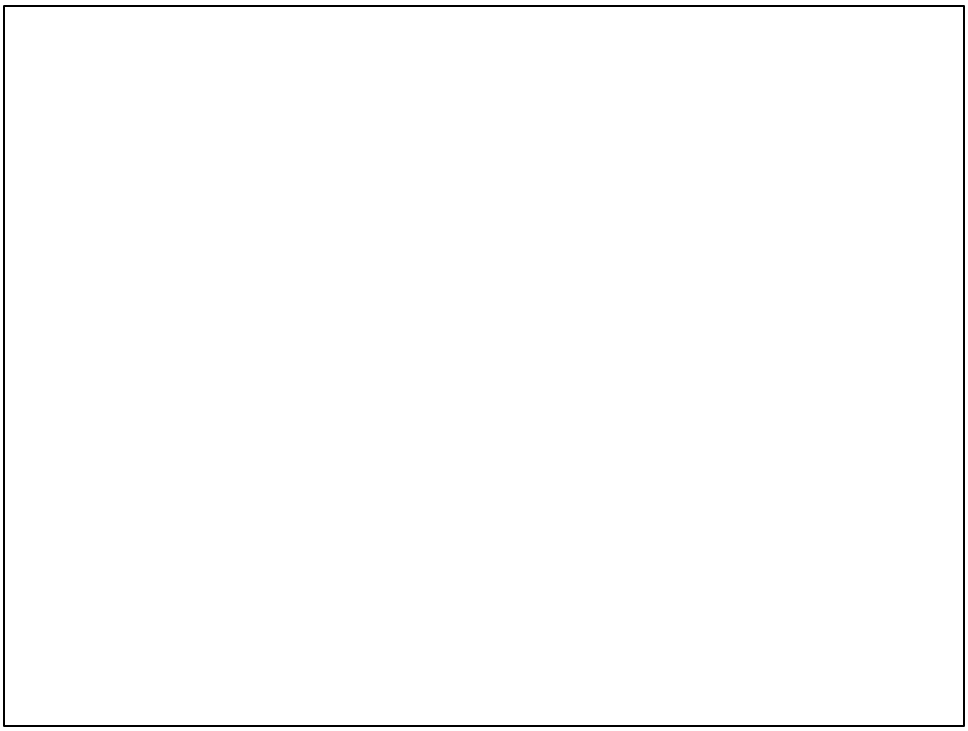
utente: associa tf a m

verifica timestamp(m,tf): t

utente: decritpa tf con chiave publica dell'autorità e ottiene h|t

utente: verifica che h=hash(m)

utente: return t



entità in gioco:

utente

autorità

metti firma con timestamp(m: documento, chiave privata di utente)

utente: h=hash(m)

utente: $hf=[h]_{utente}$

utente: mf= m|hf

utente: mettitimestamp(mf)

verifica timestamp(mf,tf): t

utente: decripta tf con chiave publica dell'autorità e ottiene hf|t

utente: decripta hf con la chiave pubblica dell'utente ottenendo h

utente: verifica che h=hash(m)

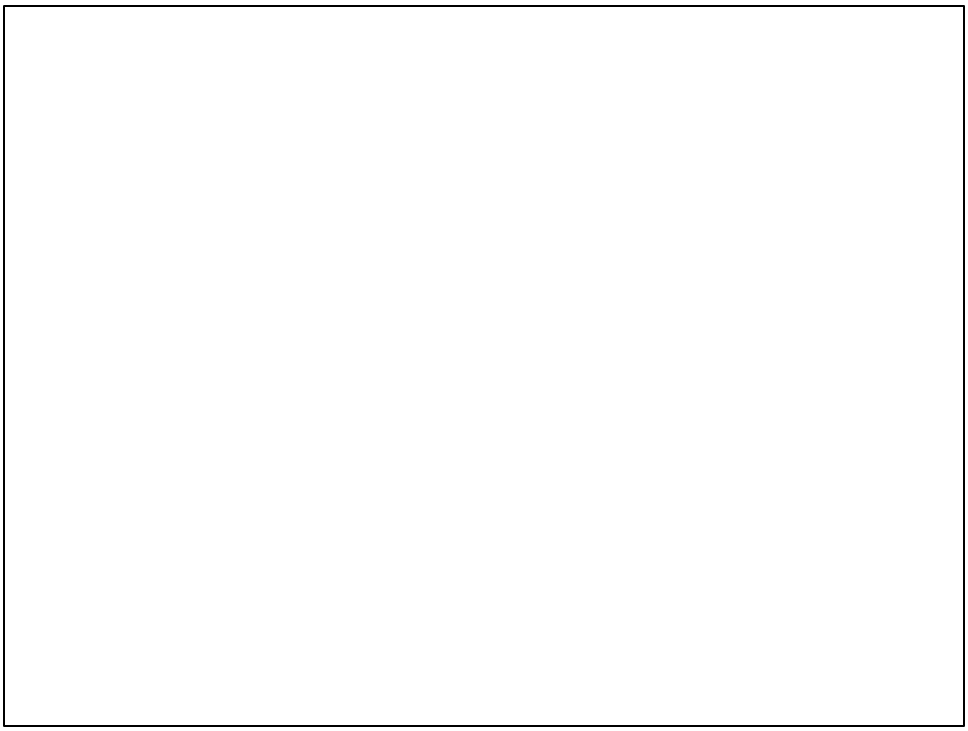
utente: return t

lancio missili

- il servizio “lancio missili” può essere utilizzato da un colonnello solo per un tempo limitato (ore o minuti) e solo se autorizzato da un generale.
- supponi che il servizio lancio missili abbia una interfaccia accessibile tramite https
- progetta un sistema informatico che automatizzi la procedura di controllo mediante l’uso di una PKI

ateneo

- un ateneo tratta tra gli altri i seguenti dati
  - generalità dei dipendenti
  - generalità degli studenti
  - esami sostenuti
  - informazioni sui progetti di ricerca
  - finanziamenti dati ai dipartimenti
- nel dps dell'ateneo quali dati figureranno tra i "trattamenti"



tls, dbms con cryptazione

polizia

- caratteristiche devono avere i sistemi che mantengono i dati relativi alle indagini?
- quali procedure si devono adottare per adempiere alla normativa?

azienda e protocolli

- struttura aziendale
  - sede centrale Bologna
    - server
    - amministrazione
    - accesso a internet
  - 2 sedi sede Roma e Milano
    - amministrazione
    - sala ospiti wifi
    - accesso a internet
  - agenti di commercio
- sviluppa una politica aziendale per il piano di sicurezza che...
  - protegga i dati dell'azienda
  - sia conforme alla legge 196/2003
- progetta una rete che implementi la politica

esempio

i segreti industriali devono essere protetti da tutti coloro che non fanno parte del personale dell'azienda

i dati sensibili devono essere cifrati

il server C tratta dati personali **sensibili**

le comunicazioni delle sale ospiti devono essere separate da quelle della azienda

ecc.