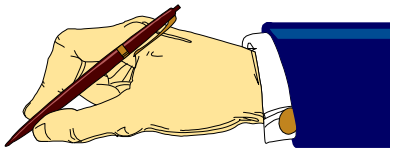
Firme digitali

Esercizi con OpenSSL



Alfredo De Santis

Dipartimento di Informatica
Università di Salerno

ads@unisa.it

http://www.dia.unisa.it/professori/ads

Aprile 2017

Esercizi

- **Esercizio 1** Per la firma digitale deve essere usata la chiave pubblica o quella privata?
- **Esercizio 2** Firmare un file mediante RSA e verificare la firma
- **Esercizio 3** Firmare un file mediante RSA con hash e verificare la firma
- **Esercizio 4** Firmare un file mediante DSA e verificare la firma
- **Esercizio 5** Firmare un file mediante ECDSA e verificare la firma
- **Esercizio 6** Creare tre file e firmare ognuno di essi mediante RSA con hash
  - Modificare leggermente un messaggio ed inviare messaggi e firme ad un compagno di corso
  - Chiedere al compagno di corso di determinare quale messaggio è stato modificato