Accordo su chiavi
Esercizi con OpenSSL

Alfredo De Santis

Dipartimento di Informatica
Università di Salerno

ads@unisa.it

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

Aprile 2017

Calcolo Chiave Condivisa

Esercizio da svolgere in coppia

Ciascun elemento della coppia deve

- **Esercizio 1** Generare i parametri pubblici DH da 1024 bit e visualizzarne il contenuto
- **Esercizio 2** Generare la propria coppia di chiavi e memorizzarla, in formato PEM, nel file dhparams.pem
  - **Esercizio 2.1** Mostrarne il contenuto
- **Esercizio 3** Inviare la propria chiave pubblica all'altro elemento della coppia
- **Esercizio 4** Generare la chiave condivisa, utilizzando la chiave pubblica ricevuta dall'altro elemento della coppia
- **Esercizio 5** Cifrare un file arbitrario, mediante un cifrario simmetrico, utilizzando come chiave il segreto condiviso generato al passo precedente ed inviarlo all'altro elemento della coppia
- **Esercizio 6** Decifrare i file ricevuti

Generazione Parametri DH

- **Esercizio 7** Generare i parametri DH in accordo alla seguente tabella e valutare i relativi tempi di esecuzione, utilizzando il comando **`time`**

Bit	512	1024	2048	4096	8192
Secondi					