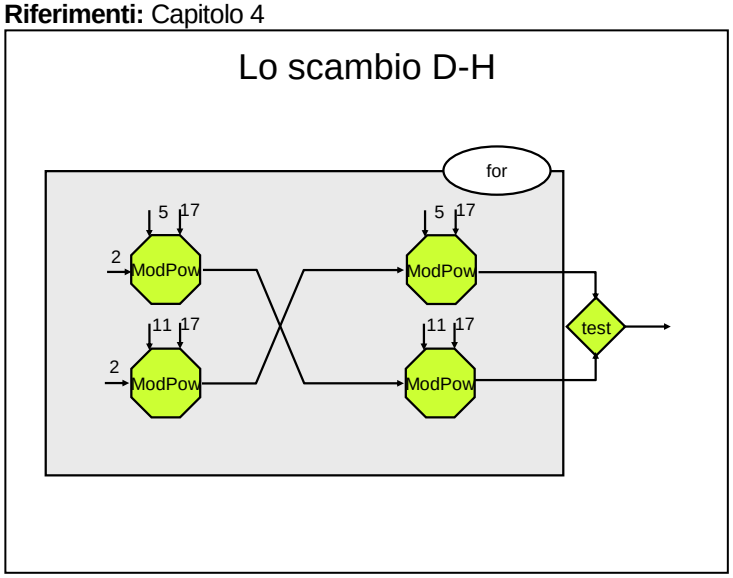
6.a Esercitazioni proposte in laboratorio

6.1 Scambio di Diffie-Hellman

Obiettivo formativo – Imparare a programmare in Java l'accordo su una chiave segreta tramite lo scambio D-H.
Riferimenti: Capitolo 4



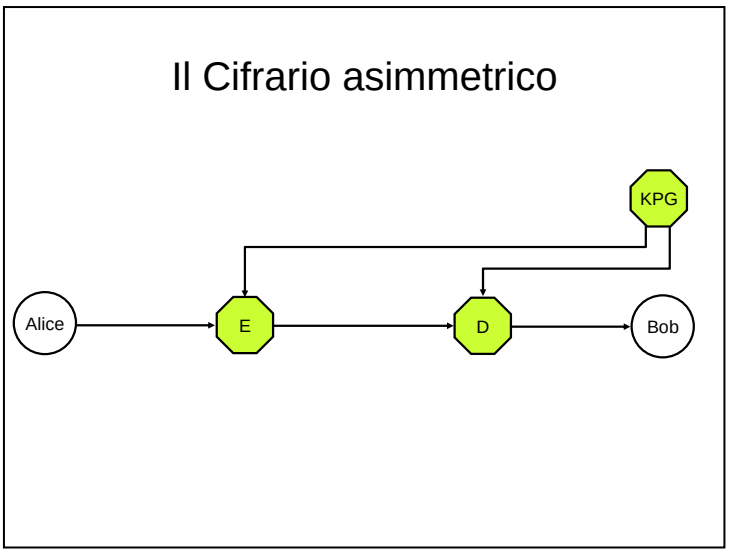
Esperimenti:

1. Istanziare una BOX-for e configurarla per l'esecuzione di un solo ciclo. Collocare all'interno della BOX quattro ModPow, connetterli in modo da realizzare uno scambio D-H e configurarli con i dati indicati in figura.
2. Introdurre un blocco test tra le due uscite, eseguire la BOX e verificare l'eguaglianza dei dati calcolati dai due corrispondenti.
3. Esaminare la scheda codice della BOX.
4. Fare click sulla BOX con il pulsante destro e selezionare il comando "Export Java Code". Prendere atto che il codice della BOX viene salvato nella cartella Java Sample Code.
5. Copiare il file e trasportarlo all'interno di un project dell'ambiente di sviluppo di Eclipse.

Modificare il codice esemplificativo, inserendolo all'interno di una definizione di classe (con lo stesso nome del file) e di un metodo *main*. Prendere atto degli errori segnalati automaticamente dall'IDE e correggerli, accettando i suggerimenti relativi all'importazione dei package necessari ed alla ridenominazione delle variabili duplicate. Aggiungere, in coda alle altre istruzioni, una stampa a video dei risultati che si vogliono confrontare e mettere in esecuzione il programma.

6.2 Il Cifrario asimmetrico

Obiettivo formativo – Analizzare il comportamento e valutare l'efficienza dei Cifrario RSA.
Riferimenti: Capitolo 5



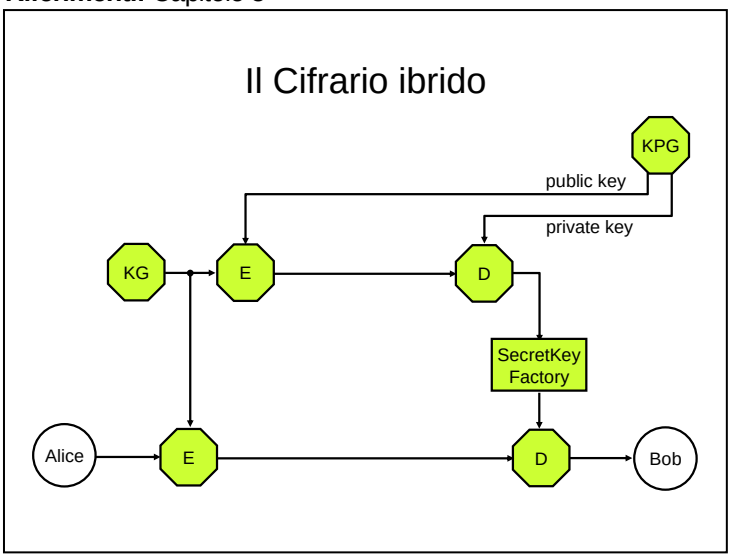
Esperimenti:

1. Generare una coppia di chiavi per il Cifrario RSA. Generare un messaggio più piccolo del modulo. Esaminare e classificare il comportamento di RSA senza padding e con padding PKCS#1.
2. Prendere atto della dimensione del testo cifrato.
3. Prendere atto dei tempi di esecuzione della cifratura e della decifrazione. Fare un confronto con i tempi di esecuzione di un Cifrario simmetrico.
4. Trasportare la coppia di chiavi all'interno di un progetto dell'IDE ed impiegare il metodo "toString()" per analizzarne le componenti.

6.b Esercitazioni aggiuntive (facoltative) da svolgere autonomamente

6.3 Il Cifrario ibrido

Obiettivo formativo – Capire come un Cifrario asimmetrico possa costituire un'alternativa allo scambio D-H ai fini di consentire la condivisione di una chiave segreta a due utenti che non hanno accordi precedenti.
Riferimenti: Capitolo 5



Esperimenti:

1. Modellare all'interno di una BOX-for il sistema indicato in figura. Configurare la BOX per una sola iterazione.
2. Scegliere e configurare un Cifrario simmetrico ed un Cifrario asimmetrico.
3. Configurare in corrispondenza i blocchi KG e KPG; metterli in esecuzione.
4. Eseguire il Cifrario asimmetrico e verificare che il componente SecretKeyFactory, suggerito quando sono in gioco provider diversi, può anche non essere presente.
5. Mettere in esecuzione il Cifrario simmetrico e verificare che Bob riceve correttamente qualsiasi testo in chiaro generato da Alice.
6. Farsi fornire da S-vLab il codice didattico delle elaborazioni eseguite all'interno della BOX.
7. Trasportare il codice didattico nell'ambiente di sviluppo Eclipse: metterlo in esecuzione dopo averlo ottimizzato e completato.