Esercitazione API Crittografia Java

SICUREZZA DELL'INFORMAZIONE M

AA 2017-2018

Pasquale Carlo Maiorano Picone
pasquale.maiorano4@unibo.it

Procedimento in ambiente Linux

Aprire un terminale e digitare:

```
git clone https://bitbucket.org/cmaiorano/esercitazione-sicurezza.git
```

Spostarsi nella directory:

```
cd esercitazione-sicurezza/
```

Eseguire il comando:

```
chmod +x gradlew && ./gradlew eclipse
```

Aprire Eclipse, cliccare su File -> Apri Progetto e selezionare la cartella `esercitazione-sicurezza/`

Procedimento in ambiente Windows

Scaricare da https://bitbucket.org/cmaiorano/esercitazione-sicurezza l'archivio con il progetto

Una volta scaricato estraetelo ed aprite una powershell (o anche un command prompt) e spostatevi dentro la cartella appena creata

Digitate il comando:

```
.\gradlew.bat eclipse
```

Aprite Eclipse, cliccate su File -> Apri Progetto e selezionate la cartella dell'esercitazione

Esercizio Proposto

Realizzate, utilizzando le API di JCA e/o le classi fornite, l'esempio di filesystem cifrato visto a lezione.

In particolare l'applicazione dovrà:

- Creare una coppia di chiavi asimmetrica
- Creare una chiave simmetrica, salvarla cifrata sul filesystem utilizzando la chiave pubblica
- Recuperare la chiave simmetrica decifrando il file in cui è stata salvata la chiave e cifrare in modalità cbc un file passato.

Facilities

Nel progetto sono state integrate le librerie Apache Commons io ed Apache Commons Lang3 per facilitarvi il lavoro con le operazioni di IO e lavoro su strutture dati

Apache Commons io: https://commons.apache.org/proper/commons-io/javadocs/api-release/

Apache Commons lang3: https://commons.apache.org/proper/commons-lang/apidocs/