Generalitat de Catalunya
Departament d'Educació
**Institut Baix Camp**

c/Jacint Barrau,1 – 43201 Reus
Tf.977310953 / Fax.977314721
http://www.insbaixcamp.org
email: e3002594@xtec.cat

# CFGS - Desenvolupament d'aplicacions multiplataforma
# Mòdul 9 – Programació de serveis i processos
# UF1 – Seguretat i criptografia

https://github.com/marianavarrovazquez/MariaDAM2/tree/master/M9/UF1/activitat7

Per l'activitat heu de lliurar:

- el codi generat (arxiu/s *.java amb comentaris i mètodes separats i clarament diferenciats).
- un arxiu pdf que contindrà exemples de la seva execució i les explicacions que creieu necessàries.

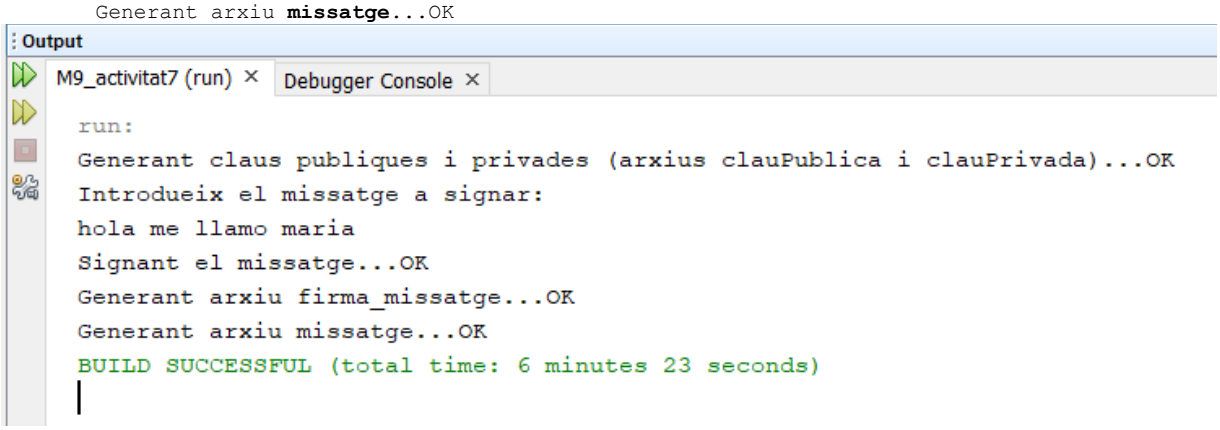
**Activitat 7**

1) Heu de codificar un algoritme (anomenat **Signatura**) que quan s'executi ha de demanar una frase (pot contenir espais) per pantalla i l'ha de signar. El missatge i la signatura s'han de guardar en fitxers. El resultat que ha de sortir per la consola ha de ser el següent:

```
Generant claus publiques i provades (arxius clauPublica i clauPrivada)...OK
Introdueix el missatge a signar:
```

I un cop introduïda la frase:

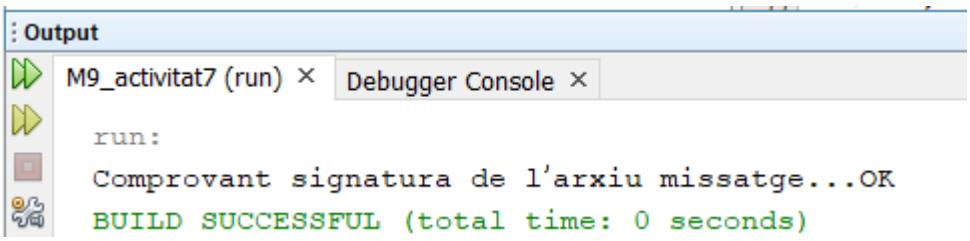
```
Signant el missatge...OK
Generant arxiu firma_missatge...OK
Generant arxiu missatge...OK
```




Els arxius que generareu s'han d'anomenar **clauPublica**, **clauPrivada**, **firma** i **missatge**.

2) Heu de codificar un segon algoritme (anomenat **Notaria**) que quan s'executi ha de comprovar si els arxius generats anteriorment estan signats correctament. El resultat que ha de sortir per la consola ha de ser el següent:

```
Comprovant signatura de l'arxiu missatge...OK
```




3) Un cop codificats els dos algoritmes, comproveu-ne el funcionament i modifiqueu l'arxiu **missatge** i comproveu que el programa **Notaria** no us valida la signatura.

c/Jacint Barrau,1 – 43201 Reus
Tf.977310953 / Fax.977314721
http://www.insbaixcamp.org
email: e3002594@xtec.cat