Examen UF1: Criptografia

L'objectiu d'aquesta pràctica és simular una transmissió amb clau embolcallada (Key Encapsulation Mechanism).

- Segueix tots els passos indicats a continuació per escriure el codi.
- Pots utilitzar una única classe amb un mètode principal i dos mètodes estàtics.
- Utilitza els noms indicats per a les variables i mètodes.
- Recorda comentar breument tot el codi.

1. (3 punts) El primer pas serà crear un mètode estàtic anomenat 'emissor' que funcionarà com a emissor del missatge.
    a. Els seus paràmetres d'entrada seran: el missatge (String missatge), la contrasenya (String password) i una clau pública (PublicKey pb).
    b. (0,5 punts) El mètode haurà de generar una clau simètrica (clau) a partir de la contrasenya (password).
    c. (1 punt) Tot seguit xifrarà el missatge amb la clau simètrica acabada de generar.
    d. (1 punt) A continuació xifrarà la contrasenya amb la clau pública.
    e. (0,5 punts) Finalment tornarà com a paràmetre de sortida la contrasenya xifrada (dades[0]) i el missatge xifrat (dades[1]) en un array (byte[][] dades)
2. (3 punts) Crearem un mètode estàtic anomenat 'receptor' que funcionarà com a receptor del missatge.
    a. Els seus paràmetres d'entrada seran les dades rebudes (byte[][] dades) i la clau privada (PrivateKey pv).
    b. (1 punt) El mètode haurà d'obtenir la contrasenya xifrada de les dades (dades[0]) i desxifrar-la amb la clau privada
    c. (1 punt) Tot seguit generarà la clau simètrica amb la contrasenya desxifrada.

    d. (1 punt) Finalment desxifrarà el missatge (dades[1]) amb la clau simètrica acabada de generar i el tornarà com a paràmetre de sortida (String).

3. (2 punts) El mètode principal haurà de:
    a. (0,5 punts) Generar una parella de claus per al receptor que anomenarem 'claus' i un missatge per a l'emissor que anomenarem 'missatge`(String).
    b. (0,5 punts) Fer una crida al mètode 'emissor' passant-li la clau pública del receptor, el missatge i una contrasenya. El seu resultat es guardarà en un array (byte[][] dades)
    c. (0,5 punts) Fer una crida al mètode receptor passant-li les dades anteriors i la clau privada del receptor.
    d. (0,5 punts) Obtenir el missatge del mètode receptor i mostrar-lo per pantalla.
4. (2 punts) Test de teoria (moodle)