Nom: Prénom:

ISIFC3 Micro-robotique, e-santé. Cryptographie.
Décembre 2022, 1.5 heures.

J.-F. COUCHOT

On considère le code python suivant principalement inspiré de
`https://pycryptodome.readthedocs.io/en/latest/src/signature/pkcs1_v1_5.html`.

```
# coding: utf-8
#

#0
#!pip install pycryptodome
from Crypto.Hash import SHA1
from Crypto.PublicKey import RSA
from Crypto.Signature import pkcs1_15

#1
rsa_obj = RSA.generate(2048)
key_pr = rsa_obj
key_pub = rsa_obj.publickey()
message = "This is a very important message: it has to be signed."

#2
h = SHA1.new(message.encode('utf-8'))

#3
signer = pkcs1_15.new(pr_key)
signature = signer.sign(h)

#4
#message = "This is a very important message; it has to be signed."
#print(": in binary version: " + str(bin(ord(":"))))
#print("; in binary version: " + str(bin(ord(";"))))

#5
h = SHA1.new(message.encode('utf-8'))
verifier = pkcs1_15.new(pub_key)
try :
  verifier.verify(h, signature)
  print("The signature is authentic.")
except (ValueError, TypeError):
  print("The signature is not valid.")
```

Vous devez répondre aux questions suivantes pour me convaincre que vous sauriez intégrer une procédure de signature électronique dans un projet de gestion d'images numériques relatives à la santé.

1. Expliquer les quatre lignes du paragraphe identifié par `#0` (1 pt.).

2. Expliquer chaque ligne du paragraphe identifié par `#1` (2 pts.).

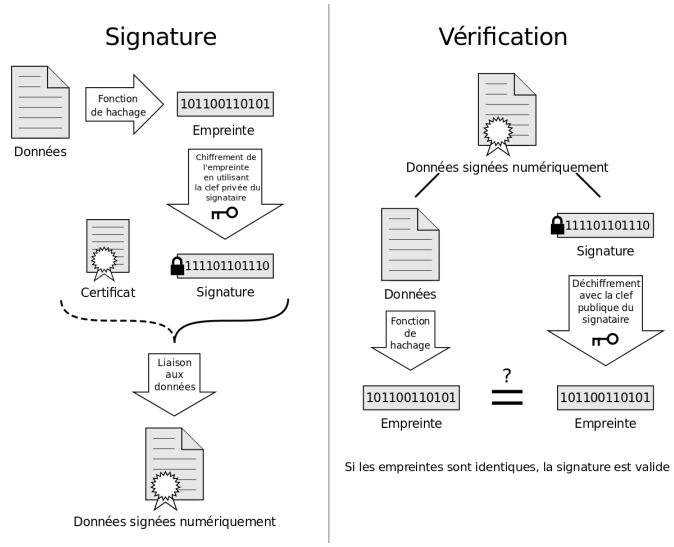
Nom: Prénom:

3. Expliquer la ligne du paragraphe identifié par `#2` (1 pt.).

4. Expliquer chaque ligne du paragraphe identifié par `#3` (1.5 pts.).

5. Expliquer chaque ligne du paragraphe identifié par `#5` (2.5 pts.).

6. Expliquer le lien entre chacune des étapes vues ci-dessus et le schéma de signature (`https://fr.wikipedia.org/wiki/Signature_num\%C3\%A9rique`) (3 pts.) rappelé ci-dessous.



7. A votre avis est-ce un bon choix d'importer le module `SHA1` de `Crypto.Hash` ? Justifier (2 pts.).

8. Appliquer un correctif correspondant à la question précédente au programme. L'exécuter. Que retourne-t-il ? Est-ce cohérent ? Expliquer (2 pts.).

9. Décommenter les trois lignes du paragraphe identifié par `#4` et exécuter le programme. Que constatez-vous en terme d'authenticité de la signature ? Expliquer (2 pts.).

10. Quels caractères diffèrent entre le message original (paragraphe `#1`) et celui dont on cherche à vérifier la signature (paragraphe `#4`). Combien de bits sont différents entre les deux messages ? Justifier. Conclure (2 pts.).

11. Modifier le code pour pouvoir signer des images et non plus du texte. Expliquer ci-dessous les lignes que vous modifieriez et comment (2 pts.).