ECAM
BRUSSELS ENGINEERING SCHOOL

Winter 2020
Sébastien Combéfis

DB701μ Introduction to Blockchain with Python

Mission 2: Message encryption and digital signature RSA

This assessment evaluates the following competencies:

- *BC501 – Write a simple blockchain with Python from scratch* *(+1)*
- *PP501 – Understand and use basic cryptographic tools with Python* *(+2)*
- *CS103 – Write a program that encrypts data with the suitable libraries* *(+2)*

In this mission, you have to find how to encrypt a message with the RSA algorithm with the `cryptography` package [1] for Python, and also use the generated pair of keys to generate a digital signature. To succeed the mission, you have to:

1. Find how to use the `cryptography` package for Python to encrypt and decrypt a message and to sign and verify a signature with the RSA algorithm.
2. Write a program that:
   (a) asks to the user to provide a string message;
   (b) encrypt the message and then sign the encrypted message with RSA;
   (c) check the signature of the message and then decrypt it.
3. Explain to the teacher how your program is working.

[1] You can find the code and documentation of the `cryptography` package here: https://github.com/pyca/cryptography.