Fall 2019
Sébastien Combéfis

I5020 Computer Security

Mission 2: Python cryptographic tools

This assessment evaluates the following competencies:

- *CS102 – Make connections between cryptographic tools and the CIA triad*
- *CS104 – Write a program that encrypts data with the suitable libraries*
- *CS107 – Identify the suitable cryptographic tool for a given security issue*
- *CS202 – Understand software protections that can be installed on a computer system*
- *CS006 – Identify residual risks that come from a countermeasurecurity issue*

In this mission, you will have to find how the main cryptographic tools are implemented in Python libraries. You have to find, in the standard library if possible, how to perform encryption/decryption (symmetric/asymmetric), hashing (message digest/authentication tag) and signature. To succeed the mission, you have to:

1. Find Python modules and functions related to cryptographic tools.
2. Write a program that use these modules and functions (simple examples are enough).
3. Explain to the teacher your findings and relate them to the CIA triad, and think about residual risks of using them.