— PL 4: Performance Measures for Message Digests, Symmetric and Asymmetric Cryptography

---

ASSIGNMENT #1: Performance Benchmarking of Cryptographic Mechanisms

Due date: **April 8, 23:59**

Grading: Assignment #1 is worth **2 points**

TO BE DONE IN **GROUPS OF TWO (MANDATORY)**

[Cryptography hazmat python manual: https://cryptography.io/en/latest/hazmat/primitives/]

In this exercise you should measure the time AES, RSA and SHA take to process files of different sizes, using a python implementation of the encryption/description and hash mechanisms.

a. Generate random text files with the following sizes:

- For AES (in bytes): 8, 64, 512, 4096, 32768, 262144, 2047152
- For SHA (in bytes): 8, 64, 512, 4096, 32768, 262144, 2047152
- For RSA (in bytes): 2, 4, 8, 16, 32, 64, 128

b. Encrypt and decrypt all these files using the AES function that you wrote previously. Employ a key of 256 bytes. Measure the time it takes to encrypt and decrypt each of the files. To do this, you might want to use the python module timeit.

   Make sure to produce statistically significant results. Do results change if you run a fixed algorithm over the same file multiple times? And what if you run an algorithm over multiple randomly generated files of fixed size?

c. Implement RSA encryption and decryption; measure the time of RSA encryption and decryption for the file sizes listed in part a, with a key of size 256 bytes.

d. Measure the time for SHA-256 hash generation for the file sizes listed in part a.

e. Prepare a report of your observations, including the following information:

- Code implemented for points b., c., and d. above
- Explain how you obtained the results – must be *statistically significant*
- Plots showing: (i) AES encryption/decryption times; (ii) RSA encryption times; (iii) RSA decryption times; and (iv) SHA digests generation times (plots can be combined for easier comparison). In these graphs, the X axis should plot the file sizes in units of bytes, and the Y axis should plot time measurements in units of microseconds (us).
- The report should also analyze and explain the performance results of:
  - Comparison between AES encryption and RSA encryption.
  - Comparison between AES encryption and SHA digest generation.
  - Comparison between RSA encryption and decryption times.

Submit your report in moodle.