**First Project**
Cryptography
2024-1

In this programming project, you and your team will embark on an endeavor to evaluate the efficiency of various algorithms. Instead of coding these algorithms from scratch, you'll leverage pre-existing implementations within the programming language of your choice, selecting suitable libraries that offer these implementations. Your primary task is to construct a set of test vectors aligned with the input requirements of each algorithm, enabling you to gauge the execution time of each one.

| **Algorithm** | **Size** |
|---|---|
| Chacha20 | Key Size 256 bits |
| AES-EBC | Key Size 256 bits |
| AES-GCM | Key size 256 bits |
| SHA-2 | Hash size 512 bits |
| SHA-3 | Hash size 512 bits |
| Scrypt | Output size 32 bits |
| RSA-OAEP | 2048 bits |
| RSA-PSS | 2048 bits |
| ECDSA | ECDSA, 521 Bits (P-521) |
| EdDSA | ECDSA, 32 Bits (Curve25519) |

Each algorithm serves a specific purpose, and it is imperative to compare algorithms with shared objectives. For instance, when assessing hashing algorithms, your focus should be on contrasting the efficiency of SHA-2 and SHA-3 using identical input test vectors.

Following this approach, your project will involve creating a comprehensive comparison table or graph that highlights the relative efficiency of these algorithms across five distinct operations:

□ Encryption
□ Decryption
□ Hashing
□ Signing
□ Verifying

Upon running your program, you must present the results for each operation in a visually engaging manner, such as a table or graph that accurately represents the execution behavior. This is an important element of the evaluation of this project.

Finally, your project should culminate in a detailed report that addresses the following key points:

- Justify your choice of programming language and library. Explain the rationale behind your selection.
- Elaborate on the inputs required by each algorithm in your chosen library.
- Describe the process of generating your test vectors and clarify the number of vectors employed for each algorithm.
- Provide reasoning for the quantity of test vectors you selected.
- Explain the methodology used to calculate the average execution time and interpret what this time signifies for each algorithm.
- For each classification, identify the algorithm that exhibits the best performance, and substantiate why it outperforms the others.

Check the specific instructions for the report on the corresponding space on Canvas.

**References**

- NIST Official Site for testing Vectors
  http://csrc.nist.gov/groups/STM/cavp/

- IETF Data Tracker
  https://datatracker.ietf.org/

- Practical Cryptography for Developers, Svetlin Nakov, Software University, 2018, ISBN: 978-619-00-0870-5m https://cryptobook.nakov.com/