**Project - ENEB 451 Network Security**

Each student group (2 members in a group) will implement the following algorithms using a programming language of their choice.

1. **SHA256**
2. **AES 128**

* Both students must participate in the implementation of both **SHA256** and **AES**.
* Write enough comments in your program so that the readers can understand your code.
* Mention the sections each student within the group worked on, in your program file (In the beginning comment section)
* The projects must be tested for the correctness of the functionality.
* Use the inputs from the following files (available on ELMS Course page)
  + - **SHA256-example** (The message with two blocks – Page 3)
    - **AES nist.fips.197** (Appendix B)

Report requirements

1. **Front page** showing the Course name, Project titles, student names/ID numbers, the semester and date of submission
2. **Abstract** (maximum 1/2 page)
3. **Introduction** (1 page, maximum)
4. **Algorithm** description (SHA256 and AES as two sub sections – in brief)
5. **Implementation** (Programming language, organization of your program, different functions)
6. **Verification** (Did you test the individual functions separately, and then the overall algorithm? Did you test the algorithm section by section before the final test?)
7. **Results** (Show the input message, key etc. and your output & expected output. If they do not match, mention the debugging you did and anticipated issues in your program. Also show a **screenshot** of your **results** getting displayed)
8. **Challenges** faced and how did you solve them (in brief)
9. **Conclusion**/**Summary**
10. **Reference**
11. Your **Full program for SHA256** (Provide in appendix section)
12. Your **Full program for AES** (Provide in appendix section)