ECRYP Project
Winter 2023

Project responsible persons:

- PhD Eng. Andrzej Wojeński (main contact regarding project),
  email: A.Wojenski@elka.pw.edu.pl
- Prof. Tomasz Adamski, email: chessmaster1303@gmail.com

This semester:

- **Projects are made in teams**. Each team = 2 persons
- **One person from a team submits a list of topics and a teammate full name**
- In special cases (e.g. hardware project, own topic etc.) the project can be done individually (please make note in the submission)

Marks are based on:

- Delivered documentation (MS Teams platform upload under Assignments)
- Delivered codes (MS Teams platform upload under Assignments)
- Project discussion/defense (MS Teams online discussion)

Points for the project:

- 25 points (base points for the project)
- + 5 extra points (**good code and documentation** with **earlier submission –** before the official submission date – that is up **maximum** to **10.01.2024**)

Important dates:

Projects should be delivered and discussed individually online on **MS Teams before the last ECRYP lecture**, that is due to: **17.01.2024**

Extra slot is submission up to the last meeting (**25% points less**): **24.01.2024**

Form of project development:

Implementations refer to cryptographic algorithms – based on selection.
Please send the **list of 4 projects** in following order:
first one is the one most wanted, last one (number four) the least wanted.

Please also indicate your teammate

The selection should be saved in PDF format and uploaded as result of "Assignments" called: "ECRYP Project selection" (it will be created in short time).

Project can be done in one of the following languages:

- Python (typical)
- HDL hardware project (for those who would like to choose this type of project/"volunteers"): FPGA-based, using VHDL or Verilog languages (requires proper testbench) –
  before please contact by email A.Wojeński

Requirements on project design and final results:

Any changes to the topic of the project needs to be first **discussed and approved** by Project responsible person (PhD A. Wojenski)

DOCUMENTATION:

- Description of the used algorithm (short theory)

- Functional description of the application (input data format, output text on console, format of output data etc.)
- Description of designed code structure (for example, mixing functions, shifting, main round function etc. with indication of input/output arguments, short description of each block etc.)
- **Test that were done with comments about the correctness of the results (own implementation and reference one)–** please indicate the source of **reference** values and compare them with your implementation (**important) -> MINIMUM 7 TEST cases (with different values etc.)**
- Please provide **images** (i.e. screenshots) in the documentation

CODE:

- Student's **CANNOT** use standard cryptographic libraries – the main algorithm needs to be implemented by yourself
- Comments in code are required – for example short descriptions of used functions
- The code should be divided into functional blocks representing parts of an algorithm (not everything in one function)
- Some simple user interface needs to be provided (console mode for example)

TESTS:

- Selected reference values for tests – provided externally (depends bit on a project) upon Student's selection e.g. from reference algorithms documentations, Linux embedded functions or trusted application that can provide results based on input-output scheme
- **MINIMUM 7 TEST cases (with different values etc.)**
- Procedure of tests (should be provided at least few tests):
    - Run designed ECRYP application with selected input
    - Compare the output from the designed application with corresponding trusted output value (reference value)