Project: Block Cipher Competition

April 28, 2021

1 Goal

The goal of this project is to use the knowledge you gained during the semester to design and attack a (Toy) block cipher. The project consists of two phases: in the first phase you design a cipher and in the second phase you attack one or multiple of the other designs made by your colleagues.

2 Designing a cipher

You need to design a cipher with a block size of 64-bit and a key size of 64-bit. The cipher should be simple (as in easy to understand and analyse), fast (in software), and secure (providing 64-bit security). You can reuse the design techniques that we saw in the `TC0X` series of ciphers, but your work should be your own (no copying, although reuse of components is OK, as long as you cite the source).

The deliverables for this part are:

- Specification of the cipher at least including:
  - Description of the cipher (round function, key schedule and number of rounds)
  - Test vectors
  - Design rationale (optional)
  - Performance figures (optional)
- Reference implementation (Python).
- Optimized implementation.

The reference implementation should be clear, understandable and concise. The optimized implementation is used to asses the speed of the cipher.

3 Cipher analysis

In this phase you choose one or more ciphers to analyse. For each design there will be a set of exercises on the exercise website (with a varying number of rounds). You can attack any cipher (also your own). For each cipher that you break you need to create a short report on how you

did it (these will be shared with your peers).

The deliverables for this part are:

- For every attack a short report on how the attack works, the handle of the exercise website, and the code.
- For every improved implementation a short report on the improvements, the optimized implementation and an accurate (reproducible) performance comparison between your and the designers optimized implementation.

4 Grading

The grade for the design phase is calculated as follows:

- If you hand in a useable cipher specification you get: 50 points.
- Clear, concise and technically accurate specification: +/- 20 points.
- Cipher design: +/- 20 points.
- Clear reference implementation: +/- 10 points
- Not meeting the security requirements: - 20 points.

Note: The last point (not meeting the security requirement) is decided before the analysis phase starts and is there to prevent ciphers with trivial flaws in the competition. If you put effort into designing the cipher this should not be something you should worry about.

With the analysis phase you can get bonus points as follows:

- No analysis done: -20 points.
- Full break: +15 points.
- Partial break: +10 points.
- Optimized implementation (fastest implementation, per cipher): +10 points.

Note: No points are deduced if your design gets partially broken, with full break of your cipher you cannot score the full 100 points.
Note 2: The optimized implementation points are given to the fastest implementation per cipher.

The project is individual. During the analysis phase you can work in teams, but the points will be distributed equally among the team members (so if you fully broke a cipher in a team of 2 both will get 7.5 points).

5 Deadlines

- Deadline for **Design** phase: 26-05-2020
- Deadline **Analysis** phase: 01-07-2020