Project: Toy Cipher Competition

May 1, 2019

Overall structure

Two phases:

- Design phase - Everyone designs a cipher.
- Analysis phase - Everyone analyses the ciphers published.

Design phase

The design of your cipher determines the base score for the project.

- Specification of the cipher (Description, Testvectors).
- Reference implementation (Python).
- Optimized implementation.
- See project document for details.

Analysis phase

You can score bonus points during the analysis phase by:

- Partially breaking a cipher.
- Full break of a cipher.
- Providing an optimized implementation that is better than the designer's.

Note 1: If your cipher gets partially broken during the analysis phase there is no penalty, if it gets fully broken you cannot score the full 100 points for the project.
Note 2: Only the fastest optimized implementation gives bonus points.

Grading

Design:

- If you hand in a useable cipher specification you get: 60 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.

Analysis:

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

Designing a cipher

- Don't reinvent the wheel, try to look at other designs.
- Keep it simple, don't add too much clutter (no security through obscurity).
- Remember that you need to defend against: Differential/Linear cryptanalysis and MitM attacks.
- Borrowing components from proven designs is OK, stealing not (cite and give a rationale why you chose this component).

Designing a cipher (1)

- Basicly two main choices: SPN and Feistel networks.
- Then you need to choose a linear and non-linear layer.
- Create a key schedule.
- Determine how many rounds the cipher should be to provide the security required (64-bit).
- Security vs Speed

Designing a cipher (2)

Some inspiration:

- The `TC0X` series (these are deliberately weak so be careful).
- SPN: AES, Skinny, LED, Midori
- Feistel: HIGHT, Speck, Simon, LEA, RC5, DES
- Orr: KATAN, KTANTAN

Deadlines

- Design (soon): 15-05-2019
- Analysis: 30-06-2019

Please start early and as always if you have questions ask (early).