Projects Presentation

Christophe Clavier - Florent Bruguier

University of Limoges - University of Montpellier

April, 2020

General rules

- Objective: to study and implement a particular technique (algorithms, cryptanalysis,. . .)
- Most of these techniques have been presented during the lectures
  (I will be available by email for any help request)
- Your program(s) must be written in C language
- The project work that you will send to me by email must include:
  - The source code(s) of your program(s)
  - A short technical report (pdf, 5 pages max)

General rules

- You must choose between five projects (described on next slides)
- Resources are provided when needed
- Projects must be done either individualy or by teams of two (depending on the project)
- Deadline for choosing your project: Sunday, April 14, 2019
- Deadline for sending your work: Sunday, May 5, 2019

List of Projects

List of Projects

Project A Finding collisions on (reduced) MD5 with Floyd's algorithm

Project to be done by team of two

- Implement the technique described in the lecture about hash functions
- Finding collisions between two images (meaningful data)
- Challenge: collisions for as large output size as possible

List of Projects

Project A Finding collisions on (reduced) MD5 with Floyd's algorithm

Project to be done by team of two

- Implement the technique described in the lecture about hash functions
- Finding collisions between two images (meaningful data)
- Challenge: collisions for as large output size as possible

Project B SQUARE cryptanalysis of the 4-round AES

Project to be done individualy

- Attack on 4 rounds has been explained during the lecture
- You can use any publicly available AES implementation (including mine)
- Challenge: you give me one λ-set; I encrypt it for you; you reveal the secret key to me

List of Projects

List of Projects

Project C SQUARE cryptanalysis of the 5-round AES

Project to be done by team of two

- Attack on 5 rounds has been explained during the lecture
- A bit more complex than on 4 rounds, but I can further explain either at USTH (before Saturday noon) or later by email
- You can use any publicly available AES implementation (including mine)
- Challenge: you give me several λ-sets; I encrypt them for you; you reveal the secret key to me

List of Projects

Project C SQUARE cryptanalysis of the 5-round AES

Project to be done by team of two

- Attack on 5 rounds has been explained during the lecture
- A bit more complex than on 4 rounds, but I can further explain either at USTH (before Saturday noon) or later by email
- You can use any publicly available AES implementation (including mine)
- Challenge: you give me several λ-sets; I encrypt them for you; you reveal the secret key to me

Project D Modular Exponentiation Algorithms

Project to be done individualy

- Implement in GMP all modular exponentiation methods described during the lecture
- Evaluate by simulations the average complexity of each method and compare with theoretical values

Thank you for your attention!

Questions?

Projects Presentation

Christophe Clavier - Florent Bruguier

University of Limoges - University of Montpellier

April, 2020