Communication and Information Engineering Program

Cryptography (CIE 582)

Spring 2023

Project Guidelines

I. Introduction

In this project, you will work in groups of 2 to 5 students. You will be required to turn in both your code and a detailed report describing the work done and results of your project, and to make a presentation about your work.

II. Project Definition

In this project you will implement in detail and evaluate the performance of modern cryptographic algorithms and cryptanalysis techniques. You may use (Java, Python) programming language. The result of this project should at least meet the main objectives below. Additional bonus objectives will count as bonus coursework marks.

For all the objectives below, you are required to follow the RFC4880 standard for implementing the PGP CFB mode of operation.

Main objectives:

1. Develop an integrated **PGP-CFB**-mode for encryption and decryption using AES as the mode's block cipher and PKCS for padding.
2. Evaluate the performance of the implemented tool with respect to encryption and decryption time, in comparison with the **Standard CFB** mode (using existing programming tools). The comparison should include encryption/decryption of message sizes {1 KB, 5 KB, 10 KB, 100 KB}. Messages to be encrypted are text files and files are provided.
3. Also, compare the performance of the RSA encryption scheme with your PGP-CFB encryption **only**, using {1 KB, 5 KB} files and 256-bit security level.

Bonus:

In 2005, Serge Mister & Robert Zuccherato published a paper [link] that proved an attack on the PGP-CFB mode. Develop a tool that demonstrates this attack on your PGP-CFB implementation. Provide a full documentation and comments of your results.

III. Deliverables

There are **three** steps to the final project, as follows:

1. Declaration of team members

Firstly, decide and declare your team members.

2. Files: Presentation, Report and Code **(see phases in section IV below)**

Prepare a presentation about the work that you have done for your final project. In addition, write a document describing the design and implementation of your project, and submit it with the project's code by the deadline which is announced via e-learning. The report should help understand what you have done, how, what difficulties did you face and how did you overcome it. In addition, the outputs and screenshots of your work must be documented in the report. The evaluation of the report and presentation will consider your technical writing and presentation skills, in addition to your understanding.

3. Discussion

Each team must give a presentation and discussion. All the team members must participate. The following points should be considered: 1) The implementation can be shown to work correctly (also documented in the report). 2) The code can be read easily. 3) The work done, and all the results are documented/presented properly.

IV. Project Breakdown

The Project will be divided into two main phases and a Bonus phase as follows:

1. Phase 1: This phase includes Objective 1 (Overall Grade of Phase 1: 50%).

   Objective 1 – (50%):

   - PGP-CFB Encryption using AES (20%)
   - PGP-CFB Decryption using AES (20%)
   - PKCS Padding (10%)

2. Phase 2: This phase includes Objective 2 (Overall Grade of Phase 2: 30%).

   Objective 2 – (20%):

   - Evaluate the performance of the PGP-CFB mode for Encryption and Decryption (15%)
   - Evaluate the performance of the standard CFB mode for Encryption and Decryption (15%)

   Objective 3 – (10%):

   - Comparison with RSA using {1 KB, 5 KB} file and 256-bit security level – (10%).

3. Bonus Phase – (3 points on the scale of 15):

   a. Success attack – (2 point).

   b. Well-documented code – (1 point).

The rest of the project mark is divided as follows:

- Report, Presentation and Discussion – (20%).

V. **General Remarks**

- Readily available implementations shared by others are not allowed.
- You may suggest a new or modified project idea.
- In case you would like to propose a new project idea, generally, your project proposal should be related to Information security and Encryption. Replicating an interesting recently published research work may also form a project idea. As a general advice, try to propose an ambitious project that you might want to continue working on afterwards. The expected work in the student-proposed project should be comparable to the amount of work involved in the predefined project.
- No project proposals are accepted after 7 days from the date of this announcement.
- All tasks should be verified with test cases that will be provided to you.
- The grade of each task depends on the correctness of its implementation and the correct verification using the test cases.
- Your code should include comments and the used variables should be meaningful.
- Part of your grades will be dedicated to comments in each phase.
- In case, Phase 1 is submitted along with phase 2, 50 % of your phase 1 grade will be deducted.
- Skipping the discussion is not allowed.