COMP343/ITEC643: Assignment 1

Challenges in Symmetric and Asymmetric Cryptography

Updates

Sunday March 5th, 2017: Assignment released on iLearn

Directions

This assignment has two different parts:

- **Part A – Hash Function – Due on Sunday March 19th, 2017, 11pm**
- **Part B – Elliptic Curve Cryptography – Due on Sunday April 9th, 2017, 11pm**

On March 5th, a message was sent to the official Macquarie email account of each student enrolled in COMP343/ITEC643. This email contains randomised individual data as well as a list of 8 tasks that you need to complete.

You are expected to implement some code using the language of your choice (`PARI/GP`, `Java`, `C`, `C++`, `Python`) in order to compute a solution to those tasks. You are strongly encouraged to use `PARI/GP` as it provides many existing functions that are relevant for both parts, in particular Part B. We also provide some predefined functions that are useful for Part A. Note that you will have to submit your code, which will be assessed.

You are required to submit a reasonable attempt of your work for Part A before Sunday March 19th, 11pm. A reasonable attempt means that you have at least submitted a correct answer for Task 1.

After the first submission deadline, your work will not be marked but you will receive some minimal feedback on your submission (i.e. correct or incorrect). You will then have the opportunity to resubmit your work before Sunday April 9th, 11pm. Your work for Part A and Part B will then be fully marked at this stage.

Failure to submit a resonable attempt by Sunday March 19th, 11pm means that your maximal mark for Part A will be scaled down by 40% (i.e. part A will be marked out of 30 instead of 50) and your maximal mark for this assignment will then be 80 instead of 100.

The maximum mark for this work is 100, which will then be scaled respectively to 15% and 13% towards the overall unit assessment of COMP343 and ITEC643.

Contact: christophe.doche@mq.edu.au

Background

For Part A, we introduce the Chaum-van Heijst-Pfitzmann hash. Given an integer t, a prime number p of size t bits, and two integers α, β in $[1, p-1]$, this hash function takes a positive integer $n < 2^{2t-2}$ and returns a value (called digest or hash) in the range $[1, p-1]$, according to the following principles:

1. Split n into two $(t-1)$-bit integers n_1 and n_2 such that the binary representation of n is the concatenation of the binary representations of n_1 and of n_2.

2. Return $\alpha^{n_1}\beta^{n_2} \pmod{p}$.

Ultimately, you will need to implement a function that takes a string and returns a number that is in $[1, p-1]$ expressed in hexadecimal notation. Note that, we will use the `C` notation starting with prefix `0x`.

Your Work, Hints and Marking

One of the aims of this assignment is to develop your skills and ability to think like an attacker. Thus, you are presented with a series of 8 challenges: 4 for Part A and 4 for Part B. Minimal guidance is given as an important part of your work is to determine how to tackle the problems and figure out what you have to do.

Based on the information sent to you by email, you are expected to complete the following tasks:

- **Part A – 50 marks – Hash Function**
  - **Task 1** – Compute the digest of a given string – **15 marks**
  - **Task 2** – Find a password whose hash evaluates to a given a digest – **25 marks**
  - **Task 3** – Find a collision for a hash function of small size – **5 marks**
  - **Task 4** – Find a collision for a hash function of larger size – **5 marks**
- **Part B – 50 marks – Elliptic Curve**
  - **Task 5** – Determine the coordinates of a point with given properties lying on a curve – **15 marks**
  - **Task 6** – Decrypt a message in the form of a point lying on a curve – **25 marks**
  - **Task 7** – Solve a Discrete Logarithm Problem of small size – **5 marks**
  - **Task 8** – Solve a Discrete Logarithm Problem of larger size – **5 marks**

To help you with this, we will regularly provide hints by email for each task.

Failure to submit a resonable attempt (i.e. at least a correct answer for Task 1) by Sunday March 19th, 11pm means that your maximal mark for Part A will be scaled down by 40% (i.e. part A will be marked out of 30 instead of 50) and your maximal mark for this assignment will then be 80 instead of 100.

You need to provide the code that you used in order to obtain the data that you submitted for all the tasks. Failure to do so or submission of incorrect code, which does not macth the data that you submitted will result in a zero mark recorded for that particular task.

Submission in iLearn

Your answers to the different tasks must consist of a text file **named after your student ID (e.g.** `12345678.txt`**)** and containing data formatted in **exactly** the same way as in the file `ass1_solution.txt` that is available in iLearn. Failure to follow this format will result in a penalty applied to your final mark.

Sunday March 19th, 11pm. Submit data in iLearn addressing the Tasks 1 to 4 that you received by email.

Sunday April 9th, 11pm. Submit data in iLearn addressing all the Tasks 1 to 8 that you received by email. You also need to separately submit the code in iLearn that allowed you to compute all the answers that you submitted.