Selected Topics in Cryptography: project guidelines

Piotr Chołda and Andrzej Kamisiński

September 30, 2017

It is recommended that you read the **entire** document before attending the first class.

Revision history

- September 30, 2017 — The first version of the document.

Basic rules and schedule

- The primary goal of the project is to design, implement, and evaluate either a random sequence generator producing high-quality sequences with respect to their entropy, or a new high-quality hash function.
- Students will work in teams (3, preferably 4 people in each team).
- To receive credit, each team is required to:
  - prepare a short written report documenting the proposed design and the evaluation results;
  - present the project in front of the other students in the group.
- According to the AGH UST rules (§11.3), presence at the project meetings is obligatory. Students who missed a meeting should present their contribution to the teacher until the end of the week of the meeting. If the contribution is not presented, the final grade will be decreased by 0.5.
- Project meetings are scheduled on **Tuesdays, 2.40-4.10$^{\mathbf{PM}}$** and **Wednesdays, 4.15-5.45, 5.50-7.20$^{\mathbf{PM}}$** — see Tab. 1 (appointment by e-mail, **at least three days** prior to the meeting).

Contact via e-mail

- Teacher: Andrzej Kamisiński (andrzejk@agh.edu.pl)
- The subject of an e-mail should be created according to the following template:
  `[STiC-project] <Team member(s)>: <subject of the e-mail>`, e.g.,
  `[STiC-project] John Doe: meeting no. 2` or
  `[STiC-project] John Doe and John Smith: corrections to the report.`
- Please include your full name in the message.

Table 1: Meeting schedule

Date	Scope
Oct 17-18, 2017	Project meeting 1 (duration: approximately 15 minutes for each team)
Oct 24-25, 2017	Project meeting 2 (duration: approximately 15 minutes for each team)
Nov 14-15, 2017	Project meeting 3 (duration: approximately 15 minutes for each team)
Nov 28-29, 2017	Project meeting 4 (duration: approximately 15 minutes for each team)
Dec 12-13, 2017	Presentation of projects

General hints and requirements

1. The proposed design of a random sequence generator must use an alphabet consisting of 256 8-bit symbols, so that it can be compared with the solutions of other teams. The same note applies to the selected existing reference implementations.
2. The proposed design of a hash function must accept any sequence of 8-bit symbols on input, returning a hexadecimal output sequence of length 64, 96, or 128 bytes.
3. Recommended programming languages: C, C++, Python.
4. The use of third-party components must be explicitly indicated in the final report.
5. It is expected that all members of a team will be familiar with every part of the project.

Final project report

1. A successful delivery of the project report involves:
   - submission of the **final pdf version** of the report by e-mail, together with all files related to the project, such as the source code of the proposed algorithms, applications, scripts, and concise instructions presenting how to build and use the included tools;
   - delivery of the **printed version** of the report (you can leave the report at the security office in D5 — in this case, please notify the teacher via e-mail).
2. The main components of the report:
   - a short presentation of the topic (the objective, the selected parameters, assumptions);
   - description of the implementation (you may consider to use block diagrams or pseudocode);
   - characterization of the obtained results (comparison with the selected reference solutions);
   - conclusions, your own opinions, recommendations.
3. Formal requirements:
   - standard typescript: margins no smaller than 1.5 cm, font size no smaller than 12 pt, standard line spacing;
   - up to **FIVE** pages (A4);
   - it is necessary to specify the contribution of each team member;
   - reports failing to meet the formal requirements will not be accepted.

Typical errors in writing

You are expected to avoid the following typical errors in your report. Some of them, although acceptable in the colloquial language, are not recommended in formal reports.

- Confusing ‘amount’ and ‘number’ (uncountable/countable).
- Confusing *hyphen* (e.g., ‘branch-and-bound’), minus sign (the so called *en dash*, e.g., ‘$-\pi$’) and *em dash* (e.g., ‘λ_d — dual variable’).
- Confusing algorithms (i.e., a sequence of operations to do something) and mathematical formulations.
- Confusing numerical calculations, emulation results and simulation results.
- Diminishing significance of your own work by writing that you ‘tried’, ‘attempted’, etc. to describe your efforts.
- Ending report, chapter or section title with a dot or colon.
- Giving captions of tables beneath them.
- Lack of commas/semicolons/dots in bullets.
- Lack of adjustment (alignment) of the paragraph text.

- Lack of description of the used abbreviations.
- Lack of full bibliographic data of the paper/book/text you reference.
- Lack of indentation at the beginning of a paragraph.
- Lack of italics while giving mathematical variables (or constants, sets).
- Lost references to figures or tables in the text (you should refer as “in Fig. 7” or “in Tab. III”).
- Putting figures/tables without captions.
- Putting figures/tables without numbers.
- Usage of Polish quotation marks („”).
- Writing comma instead of decimal dot.
- Writing digits, numbers, brackets and indicators of standard mathematical operations (e.g., the maximum function) or operators (e.g., the addition operator) with italics.

Significant failure to meet the recommendations above may result in the reduction of the final grade by 0.5.

Correction

After reading your report, the teacher may send you the scan of your text with some remarks. You should send the electronic version with the improvements taking into account the suggestions (unless you are satisfied with the proposed grade). The following symbols might be used:

- Change of order: *change order*.
- Removal of unnecessary blank space: *(word*.
- Removal of a text fragment: *unnecessary* ~~*pleple*~~ *word*.
- Character/word insertion: *lac*^{k}*ing*.
- Insertion of a lacking blank space: *spacenecessary*.
- Change of the font type to italics (or the other way round): *plain*.

Presentation of the results

- Each project team is granted 15 minutes to present its project in front of the other teams.
- Presentation of a project should involve all team members.
- Presentations are graded based on their quality, content, and the ability of the presenters to manage time appropriately.
- Grades will be assigned by the teacher, taking into account the results of a survey among the audience.

Grading

- Projects are graded based on their scientific value, novelty of ideas, quality of the implementation, the obtained results, the overall quality of the report, and presentation of the results by the team.
- All projects presenting new concepts (i.e., concepts designed and proposed by the respective project teams) will be considered in the internal competition and may receive the highest grade (5.0).
- Alternatively, it is also possible to implement and evaluate an existing solution — in this case, the project report cannot receive a higher grade than 4.0.
- The final grade is determined based on the average value of two grades: one corresponding to the report, and the other one corresponding to the presentation.