Course Howto

Lecture Videos & Lecture Notes You can find the lecture videos and lecture notes on Zulip: `https://crypto22.zulip.aalto.fi/join/5uu25r7rbfzrkhhxtugn57hr/`.

Lecture Discussion You can ask questions on the lecture to Chris/Russell each Monday from 12:15 - 14:00 during the exercise session (in person). These slots are reserved for *technical discussions*. We do not answer questions pertaining to passing criteria in these sessions.

Exercise Sessions We have exercise sessions on Monday 12:15 - 14:00, Tuesday 14:15-16:00, and Thursday 14:15-16:00. The goal of the exercise sessions is to get started working on the exercises together with others, to discuss your understanding with others and with the TAs and generally, to be part of our crypto course community and have fun.

Companion We refer to the crypto companion for definitions and clarifications you might need: `https://github.com/cryptocompanion/cryptocompanion`.

Zulip You can ask questions on the lectures and exercises on Zulip anytime. Chris/Russell will answer questions on Mondays. During the rest of the week, other course participants or teaching assistants might also help on Zulip (no promises). Teachers are not available during the week-end. Join Zulip here:
`https://crypto22.zulip.aalto.fi/join/5uu25r7rbfzrkhhxtugn57hr/`

Submission Submit your exercise solutions to MyCourses before Monday, September 12, 11:30. Your teaching assistant will carefully study your ideas and provide helpful suggestions. We provide a nice LaTeX template in the Materials section in MyCourses:
`https://mycourses.aalto.fi/course/view.php?id=33603&section=2`
which you can use for your exercise solutions, but you can also write on paper and scan the result or take a well-lit, high-quality picture. Please return your solutions as a single pdf.

Mistakes We encourage you to choose the option of choosing many exercises and be open to the possibility of making mistakes—studies on learning[1] tend to indicate that we learn when we make mistakes and get feedback to correct and/or refine our thinking. This is a central part of learning, so we encourage you to be open to the possibility of pushing the boundaries of your understanding in a safe space which supports your learning, which is appreciative of your effort to learn and acknowledges that learning means to experiment with thinking.

Passing the course Creating a safe space for experimenting with thinking and at the same time defining "course passing criteria" is somewhat in a tension with one another. Ideally, there would be no course passing criteria, but this is not possible, so we try to make course passing criteria such that they encourage and support engaging genuinely with the material. In particular, our point system is designed to allow to obtain full points also on an exercise sheet where none of the provided answers was correct—because point-giving should encourage learning and not get in the way of it by forcing everyone to only hand-in perfectly correct exercises from the start.

There are 10 exercise sheets, each worth at most 4 points (40 points total). A mostly correct solution to one exercise yields 2 points and a good attempt yields 1 point. You can attempt as many exercises per exercise sheet as you want, but the maximum amount of points is 4 per sheet (e.g. even if you submit more than 2 correct solutions, you can only get 4 points). No points are given for late submissions, but feedback is always given.

Watching the lecture and participating in all embedded quizzes of the lecture before 11:30 on Mondays yields 1 bonus point (up to 12 bonus points for the entire course). This is another way of obtaining quick feedback on your understanding.

[1] Unsuccessful Retrieval Attempts Enhance Subsequent Learning, Nate Kornell, Matthew Jensen Hays, and Robert A. Bjork, Journal of Experimental Psychology: Learning, Memory, and Cognition, 2009, Vol. 35, No. 4, 989-998, `https://sites.williams.edu/nk2/files/2011/08/Kornell.Hays_.Bjork_.2009.pdf`

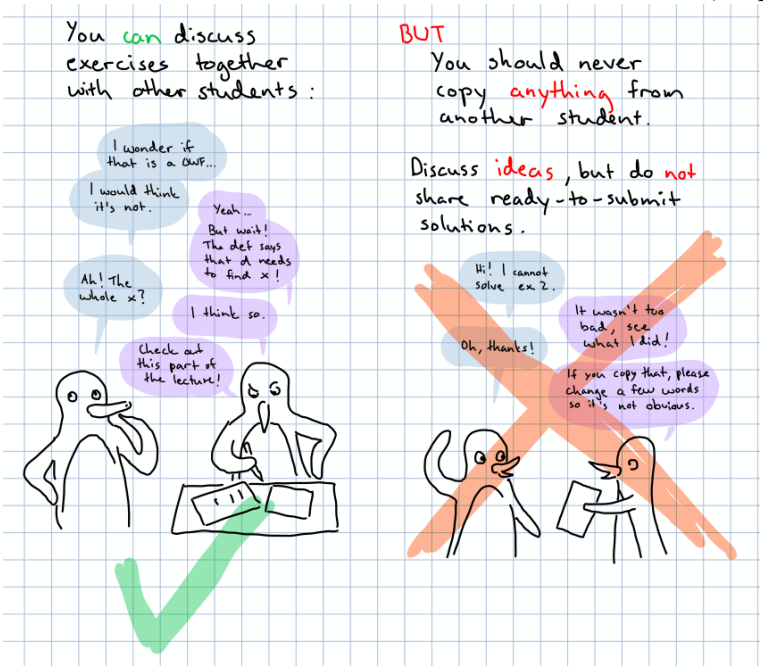
In-person sessions are reserved for discussions on cryptography. Question on system things such as passing criteria will only be answered on Zulip, not in in-person session (This preserves the informal character of in-person sessions and, additionally, is more fair, because everyone will be able to read the answers on Zulip, while in in-person sessions, only some people are present.).

Passing criteria. There are no grades, just pass or fail. Passing criteria are

- at least 30 points throughout the entire course, and
- at least 10 points in the first half of the course, and
- at least 10 points in the second half of the course

Thereby, you can choose and emphasize topics you enjoy and skip some exercises which you enjoy less. Also, if you are unable to submit one exercise sheet on time due to personal reasons or illness, it should not be too difficult to pass nonetheless. Hence, we do **not** extend the deadline even if you are unable to submit one exercise sheet for a good reason. Please take this into account when planning your studying.

Code of conduct. Remember to follow Aalto code-of-conduct[2], in particular:



[2] See in particular 'unattributed borrowing' here: `https://into.aalto.fi/display/ensaannot/Aalto+University+Code+of+Academic+Integrity+and+Handling+Violations+Thereof`

CS-E4340 Cryptography: Exercise Sheet 1

—One-Way Functions, Algorithms & Probabilities—

Submission deadline: September 12, 2022, 11:30, via MyCourses

Each exercise can give up to two participation points, 2 for a mostly correct solution and 1 point for a good attempt. Overall, the exercise sheet gives at most 4 participation points. We encourage to **choose** exercises which seem **interesting** and/or adequately challenging to you.

Exercise Sheet 1 is intended to help...

(a) ...understand the *definition* of One-Way Functions (OWFs) and gain *intuition* for OWFs.
(b) ...familiarize yourself with the idea of generic counterexamples.
(c) ...familiarize yourself with security experiments.
(d) ...practice thinking about probabilities.
(e) ...practice the use of pseudocode.

Exercise 1 aims to help understand probabilities.
Exercise 2 helps understand the notion of one-wayness and is the **most important** exercise on this sheet. We warmly encourage it.
Exercise 3 gives an opportunity to practice writing *inverters*[1] for some easy-to-invert functions, i.e. bad one-way function candidates.
Ex. 4 & Ex. 5 are advanced exercises, where you are asked to provide an attack on a generic one-way function counterexample and analyze the probability of the attack.

Exercise 1 (Probability and Pseudocode)**.** *2 points*

(a) You roll three (six-sided) dice D_1, D_2 and D_3. There are $6 \cdot 6 \cdot 6 = 216$ possible combinations of the results (D_1, D_2, D_3). For how many of the results is it true that $D_1 + D_2 + D_3 = 17$? Divide this number by 216 and determine: What is the probability that the sum $D_1 + D_2 + D_3$ is equal to 17?
(b) Define the function f and attacker $\mathcal{A}$ as

$$\begin{array}{ll} \underline{f(x)} & \underline{\mathcal{A}(y, 1^{|x|})} \\ y \leftarrow x \oplus 1^{|x|} & z \leftarrow y \oplus 1^{|x|} \\ \textbf{return } y & \textbf{return } z \end{array}$$

and show that it holds that $\Pr\left[\mathsf{Exp}^{\mathsf{OW}}_{f,\mathcal{A}}(1^\lambda) = 1\right] = 1$. The above $\oplus$ means bitwise XOR operation. For more notation, we refer to the crypto companion `https://github.com/cryptocompanion/cryptocompanion`. Recall that the experiment $\mathsf{Exp}^{\mathsf{OW}}_{f,\mathcal{A}}(1^\lambda)$ is defined as:

$\underline{\mathsf{Exp}^{\mathsf{OW}}_{f,\mathcal{A}}(1^\lambda)}$
$x \leftarrow\!\!\$\ \{0,1\}^\lambda$
$y \leftarrow f(x)$
$x' \leftarrow\!\!\$\ \mathcal{A}(y, 1^\lambda)$
if $\left|x'\right| \neq \lambda$ **then**
  return 0
if $f(x') = y$ **then**
  return 1
return 0

[1] For OWFs, the term *adversary* and *inverter* are synonymous, because an adversary against a OWF tries to invert.

Exercise 2 (One-Way Functions)**.** *2 points* Assume the existence of a length-preserving one-way function[2]. Say for each of the following statements whether you believe they are true or false and provide your intuition. You are not expected to *know* the answer to these questions, i.e., reasoning suffices (for 2 points) even if not all answers are correct. $||$ denotes concatenation of strings.

Hint. recall from the lecture that if f is one-way function, then $g^f_{leak-r}(x_l||x_r) := f(x_l)||x_r$ and $g^f_{app-zer}(x) := f(x)||0^\lambda$ are also one-way functions, where $|x_l| = |x_r|$. You can use the examples from the lecture and Section 4 of the crypto companion without justifying them.

(a) For all length-preserving one-way functions f and g, the following function h is a one-way function: $h(x) := f(x)||g(x)$.
(b) For all one-way functions f and all polynomially computable functions b with one bit output, the following function h is a one-way function: $h(x) := f(x)||b(x)$.
(c) For all length-preserving one-way functions f and g, the following function h is a one-way function: $h(x) := g(f(x))$.
(d) For all length-preserving one-way functions f, the following function h is a one-way function: $h(x) := f(x)_{1\ldots\lceil|x|/2\rceil}$. I.e., h returns all bits that f returns, except for half of the bits (rounded up).
(e) (*Advanced*) For all length-preserving one-way functions g, the following function h is a one-way function: $h(x) := g(x)_{1\ldots|x|-1}$. I.e., h returns all bits that g returns, except for the last bit.
(f) For all length-preserving one-way functions f, g, the following function h is a one-way function: $h(x) := f(x) \oplus g(x)$. I.e., h is the bitwise XOR of two OWFs.
(g) There exists a one-way function h with 1 bit output, i.e., for all $x \in \{0,1\}^*$, $|h(x)| = 1$.
(h) For all length-preserving one-way functions f, g, the following function h is a one-way function: $h(x) := f(x)||(x \oplus g(f(x)))$. I.e., h first applies f to x and then g to x, then xors the result with x, this is the second half of the function h, and the first half of the function h is just $f(x)$.
(i) For all length-preserving one-way functions f, the following function h is a one-way function: $h(x) := f(1^{|x|})$
(j) For all length-preserving one-way functions f, the following function h is a one-way function:

$$h(b||x) := \begin{cases} 0||f(x) & \text{if } b = 0 \\ 1||x & \text{if } b = 1. \end{cases}$$

where b is of length 1 (first bit of the input).

Exercise 3 (Constructing Inverter)**.** *2 points* Choose *one* out of (h), (i) from Exercise 2, give an efficient inverter and argue that the inversion probability is 1. Alternatively, you can also choose *one* out of (j) or (g) and give an inverter which inverts with probability $\frac{1}{2}$.

Exercise 4 (Attack a OWF-Candidate)**.** *2 points* Choose one of the constructions h in Exercise 2 (a)-(e) that is not one-way. Argue why it is not OWF, that is, provide an inverter and argue why the inverter is efficient (intuitive argument is enough).

Exercise 5 (Analyze the Attacker)**.** *2 points* What is the inversion probability of your inverter from the previous exercise? Justify your answer. Is the probability non-negligible? **Hint:** Since we haven't discussed the definition of *non-negligible*[3] in the lecture, you can either look it up in the crypto companion, or simply argue that your inverter inverts with constant probability, e.g., $\frac{1}{10}$.

[2] A function $f : \{0,1\}^* \to \{0,1\}^*$ is *length-preserving* if for all $x \in \{0,1\}^*$, it holds that $|f(x)| = |x|$.
[3] A negligible function is a function tends to zero faster than any inverse polynomial as λ tends to infinity. A non-negligible function is a function which is not negligible. See Definition 2.2 in the *crypto companion* `https://github.com/cryptocompanion/cryptocompanion`.