About the Exam

Date: **January 13th**, 2023
Time: **8:30-12:30** (GMT+1)
Style: **closed-book**

No extra material is allowed during the exam except for pens and a simple calculator (not smartphones). *No other electronic devices allowed*. Your solutions to the problems in the exam must be written in *English*. Your language skills will not be judged (but what we cannot understand or read will receive 0 points). Try to give *clear answers* and *motivations*.

See Chalmers' exam guidelines: `https://student.portal.chalmers.se/en/chalmersstudies/Examinations/Pages/default.aspx`

Exam Points

The exam is organized in 3 *parts* (following the module structure of the course). Each part gives up to 20 points, for a total of maximum 60 points that can be scored in the exam.

Grades are assigned according to the points you collect*:			
CTH Grades:	30-40 $\rightarrow$ 3,	41-50 $\rightarrow$ 4,	51 or above $\rightarrow$ 5
GU Grades:	30-50 $\rightarrow$ G,	51 or above $\rightarrow$ VG	

* You collect points by scoring points in the exam (providing correct answers with good motivations) and by passing bonus assignments during the course. Collected points are the sum of the two, provided that your exam score is at last 30 points.

Exam Problem Types

There are N types of possible problems that can appear in the exam:

- **Definitions** (e.g., syntax of a cryptographic primitive, statement of a property of a scheme)
- **Security Games** (state the game, winning conditions and the security statement)
- **Proofs** (seen during the lectures)
- **Hardness Assumptions** (e.g., discrete logarithm, factorization of large composite numbers)
- **Open Questions** (usually generic)
- **Problems** taken from the weekly exercise sheets
- **More Problems** similar to the ones in the weekly exercise sheets
- **Fantasy** (questions on topics not seen during the course or in the exercise session, but that are possible to tackle using the tools taught in the course)

Exam : What to Expect

- **Definitions**: a few [mnemonic, blue frames in slides]
- **Security Games**: one or two [mnemonic]
- **Proofs** : one or two [understanding or lots of mnemonics]
- **Hardness Assumptions**: one or two [understanding or lots of mnemonics]
- **Open Questions**: one or two [see the bigger picture]
- **Problems** several sub-exercises [understanding or lots of mnemonics]
- **More Problems** several [understanding and insight]
- **Fantasy** one or two [understanding and insight]

Exam : Examples of Definitions Questions

- Provide the definition of a one way function.
- Give a description of the syntax and correctness for a digital signature scheme.
- Describe the the adversarial models discussed in the course (type of adversary, computational power, corruption style).
- State the three properties of a secret sharing scheme.

Exam : Examples of Open Questions

- In what way will quantum computer impact the security of cryptographic constructions? [Lecture 8]
- What is the time line (or life span) of a cryptographic algorithm? [Lecture 8]
- In Sigma protocols, why removing interaction between prover and verifier makes the proof verifiabile by multiple verifiers? What technique is used to achieve this in a secure way (give name and how it works)? [Lecture 11]

Hint: in case you're tight on time, adjust the length / depth of your answer to the amount of points assigned.

Exam : Examples of More Problems and Fantasy

These are all given in the `exam-template.pdf` available on Canvas.

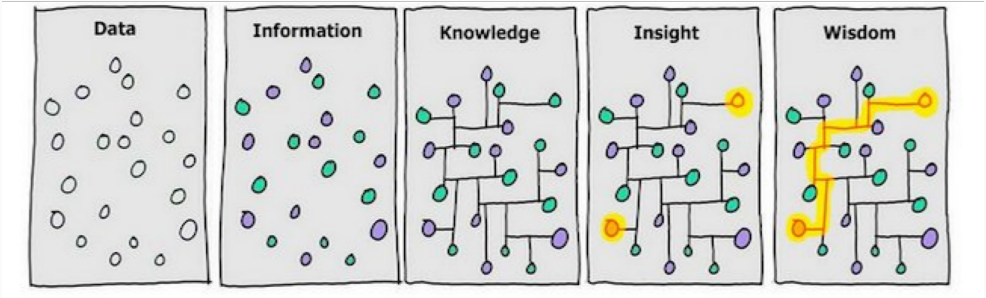
Exam : Constructions you should know by heart

Hopefully everything! If that's not possible then at least:

- OTP
- Modes of operation for block ciphers CBC, ECB.
- RSA (both encryption and signature), ElGamal
- DH key exchange.
- Shamir Secret Sharing Scheme.

Other primitives that appear in the exam will either be used in a black-box way (so, syntax, correctness and security properties are all you need to remember), or the exam question will provide a very quick description of the construction (e.g., Pedersen commitments, ECDSA, Schnorr protocol...)

About your learning



For: data, information, and knowledge use the lecture notes given as **references**.
For: knowledge, insight, and wisdom come to the **lectures**, read the **slides**.
Note: *My slides are meant as an aid your understanding, to provide intuitions that are usually hard to convey in lecture notes/books.* You are **expected** to study and use the literature given as references in the first slide of each lecture, especially the references in **boldface**.

About your workload

7.5hp = 200 hours of study

- Attending lectures + exercise sessions -> 38h (∼1 week)
- Study during the course -> 42h (∼1 week)
- 3 Home assignments -> 40h (1 week)
- Preparation for the exam -> 80h (2 full weeks)

If you miss a lecture or exercise session, it is natural that catching up with the course material may take you longer time than these estimates.