*

2MMC10_Cryptology_Q2_20/retake

Cryptology

Course Name:	Cryptology	Course Code	2MMC10
Date:	19 January 2021		
Start Time	13:30	End Time:	16:30
Number of questions	5		
Maximum number of points/distribution of points over questions:	100		
Method of determining final grade:	Points/10 rounded to 1 decimal		
Answering style: formulation, order, foundation of arguments, multiple choice:	Free-form text ansers and numerical answers		

Permitted items:

- The following items are permitted
  - Books (phyisical or pdf), printouts, digital documents on the computer or online, handwritten notes
  - Your homeworks and the corrections you received
  - Blank paper for taking notes (no upload of pictures)
  - Pens, pencils, etc
  - Calculators
  - You may run comuter algebra systems as well as your own code on the computer and in online calculators
  - You may use spell-checking tools and pepare text in other editors.
- You may not communicate with any other person regarding the exercises by any means during the exam. As an exeption you may contact Tanja Lange if you encounter any problems.
- Looking up existing webpages is permitted; posting the questions or answers counts as communication and is not permitted.
- You may visit the bathroom during the exam time and you may have food and drink on your desk.

Instructions for answering questions:
All answers should be entered into the answer fields in Ans; do not write on paper and upload photos of your answers.

The exam has numerical questions, i.e. questions you answer with a single number, and open questions, i.e. questions where you get a text field and can type arbitrary text. For the latter type of questions, make sure to justify your answers in detail and to give clear arguments. Document all steps, in particular of algorithms. It is not sufficient to state the correct result without explanation.

You may copy instructions and outputs from your computer algebra system into the answers but need to explain what they do and why you invoke them.

If an exercise requires usage of a particular algorithm, other approaches will not be accepted even if they give the correct result.

Video upload:
After this first part finishes you should record a video of you explaning your solution. Choose 3 exercise parts which are not numerical questions and aim for 5 min of recordinng (no longer than 10 min). Show your student ID and state your name at the beginning of the video.
Please use https://surfdrive.surf.nl/files/index.php/s/uWvzGC0mGsnfNsc
for uploading your video. Name the file as
ID_{student ID}_[Last name].[file format]
filling in your TU/e student ID, your last name, and the file format (mp4, webm) instead of the brackets.
If your connection is too weak, store the video on your computer and compute the SHA-256 checksum of it and mail that to Tanja Lange at t.lange@tue.nl.

Support:
If you want to indicate that any unwanted disturbances occurred that might be registered as an irregularity, or if your exam does not go as expected due to technical problems that indered your exam (for example power or Internet failure in the region), you can report this within 24 hours to the Examination Committee via the Webform Online Exam at https://educationguide.tue.nl/studying/corona/webform-online-exams/.

You can start the exam now, good luck!

START