CHALMERS UNIVERSITY OF TECHNOLOGY
Department of Computer Science and Engineering
Examination in Computer Security EDA263 (DIT641) for the International Master's Program in Computer Systems and Networks, Saturday 23 March 2019, 08:30—12:30

Examiner: Associate professor Magnus Almgren, Ph.031-772 1702,
email: magnus.almgren@chalmers.se

Teacher available during exam: Magnus Almgren, Ph.031-772 1702
The teacher will aim to physically come twice to the exam: about 60—90 minutes after the start of the exam, and about 60--90 minutes before the end.

Language: Answers and solutions must be given in English.

Grades: will be posted before Monday 15 April 2019. The exam review date/place will be announced on canvas when the grades have been posted.

You are **not** allowed to use any means of aid.
However, according to general rules printed English language dictionaries are allowed.

Please write the answer to each question (question 1, question 2, etc) on a separate sheet of paper.

Grade: The grade is normally determined as follows:

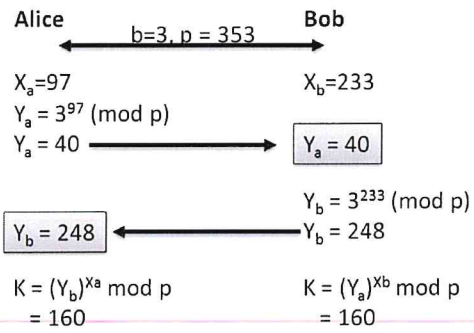
30 p $\leq$ grade 3 < 38 p $\leq$ grade 4 < 46 p $\leq$ grade 5 (EDA263)

30 p $\leq$ pass < 46 p $\leq$ pass with distinction (DIT641)

4 Cryptography (6p)

You are sitting on an airplane when you notice that the passenger next to you is correcting exams. You glance over and see the following (partial) answer from one student. You realize this is the Diffie-Hellman algorithm discussed in the lectures.

a) What is this particular algorithm mainly used for? (2p)
b) What is the underlying security assumption? (why is it considered secure?) (2p)
c) What happens if the information (marked with arrows) is sent in clear text (not protected by encryption) and the adversary Eve manages to sniff the network and extract these parameters? (2p)



5 Security Models (8p)

In the course we discussed several security models. Please describe the main objectives of the Clark-Wilson model including the additions proposed by Lee, Nash and Poland. Also give a detailed example of how it can be used. Your example should demonstrate the principal components in the model.

6 Authentication and Access Control (16p)

Give a short (i.e. less than ca. 10 lines) but exhaustive answer to each of the following questions: (The answer must include not only the function, usage, principle etc., but also the (security) context into which the object of the question would be applicable.)

a) Biometric authentication systems are becoming more prevalent (e.g. fingerprint sensors on phone). Explain why there might still be misclassifications even though fingerprints are believed to be unique. (4p)
b) Many times a *slow hash function* is used when authenticating users with passwords. Why is a hash function used? Why is it slow? Explain two (2) reasons why a *salt* is used in combination with the password. (4p)
c) What is the difference between a password and a passphrase? What is the preferred method for modern authentication according to NIST guidelines? Why? (4p)
d) Describe the reference monitor and what it is for? Draw a figure demonstrating its function and the in/out data necessary. (4p)