Final Exam
Cryptology (1DT075)

Teacher: Tjark Weber

Home Exam
2020-06-09, 08:00–13:00*

Instructions

Read and follow these instructions carefully to increase your chance of getting good marks.

- Please submit **a single PDF file** on the Student Portal, preferably created using a word processor. (The file may include photos or scans of handwritten answers. However, illegible answers give no points.)
- Please **sort** the answers in your submission by question number. For each answer, clearly indicate to which question the answer belongs.
- The exam will be **open book**: you are allowed to use course materials, textbooks, your own notes, and any other material that was written before the start of the exam. Remember to give credit (i.e., to provide references) when you use third-party sources. You are also allowed to use technical aids, such as a calculator.
- The exam will be **individual**: you are NOT allowed to get help from other people to answer the questions. Do NOT share or discuss the questions with other people (online or otherwise). Do NOT share or discuss solution approaches with other people. Do NOT submit other people's answers as your own.

The course teacher will be available by email during the exam: tjark.weber@it.uu.se. Important announcements or clarifications will be posted on the Student Portal.

Grading scale: 0–49 pts. (U) / 50–69 pts. (3) / 70–84 pts. (4) / 85–100 pts. (5)

*Answers must be submitted on the Student Portal before 13:30. This includes additional time for submission in case of technical difficulties. Submission before 13:00 is strongly encouraged.

Problem 0

What is your exam registration code (e.g., AB-1234-XYZ)?

(0 points, but your exam answers will not be graded unless you are registered)

Problem 1

Suppose the Swedish Ministry for Foreign Affairs wants to develop a proprietary software to allow the approximately 80 Swedish embassies around the world to exchange confidential messages with each other over the Internet (e.g., via encrypted email attachments). You are the cryptography expert on the development team.

What knowledge from the course could you apply to this task, and how? Discuss the cryptographic aspects of the system design. What design choices would you make, and why? What are the main issues, and how would you address them? Provide a detailed technical discussion; explain and motivate your choices.

(30 points)

Problem 2

1. Does the system that you described in your answer to Problem 1 provide perfect secrecy? Justify your answer.

   (5 points)

2. What does this mean for the security of the system in practice? Discuss.

   (5 points)

Problem 3

You are informed that the system from Problem 1, in addition to confidentiality, should ensure message integrity and non-repudiation.

How would you modify your system design to achieve this? Discuss the cryptographic aspects of your solution. Provide a detailed technical discussion; explain and motivate your choices.

(15 points)

Problem 4

Considering again the system from Problem 1, you are informed that no embassy employee alone should be able to learn the contents of a confidential message, but that this should require the collaboration of *any two* of the embassy's diplomatic staff. (The number of diplomatic staff at each embassy varies, but is usually between 5 to 10.)

How would you modify your system design to achieve this? Discuss the cryptographic aspects of your solution. Provide a detailed technical discussion; explain and motivate your choices.

(15 points)

Problem 5

Consider the Hill cipher for $n = 3$ characters at a time, and the key $k = \begin{pmatrix} 0 & 25 & 23 \\ 17 & 4 & 8 \\ 2 & 7 & 10 \end{pmatrix}$.

1. Compute the encryption of the last three characters of your exam registration code (see Problem 0). (Characters are identified with elements of $\mathbb{Z}_{26}$ in the usual way: A=0, B=1, ..., Z=25.) Present and briefly explain the entire calculation, not just the final result.

   (5 points)

2. The matrix k is invertible (over $\mathbb{Z}_{26}$). Why is this important?

   (5 points)

Problem 6

1. Consider a Blum-Blum-Shub generator with modulus $m = 78769$ and seed $X_0 = 14318$. Compute the first 10 pseudo-random bits that are output by this generator.

   (5 points)

2. Compare the Blum-Blum-Shub generator to LFSRs. Name at least one advantage and one disadvantage of the Blum-Blum-Shub generator (for cryptographic applications).

   (5 points)

Problem 7

1. Use a steganographic method to "hide" the following text in the PDF file that you submit:

   > Steganography is the practice of hiding data to achieve covert communication.

   Explain how to recover the text from the PDF file.

   (5 points)

2. Discuss the robustness of your method.

   (5 points)

Good luck!