Final Exam
Cryptology (1DT075)

Teacher: Tjark Weber

Home Exam
2020-08-27, 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.
- Consider the points available for each question for an indication of how much time you might want to spend answering the question, and how detailed your answer should be.

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

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

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 you are working for a company that wants to launch a new subscription-based online video-conferencing software (similar to, e.g., Zoom). The company hopes that this software will attract millions of users. However, each video conference is relatively short-lived (a few minutes to a few hours) and typically has about 2–20 participants only. You are the cryptography expert on the development team.

The company wants to ensure confidentiality of (the content of) video conferences. 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.

(25 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

Consider the Hill cipher for $n = 3$ characters at a time, and the key $k = \begin{pmatrix} 11 & 3 & 5 \\ 9 & 19 & 0 \\ 9 & 0 & 25 \end{pmatrix}$.

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 5

Consider the following two random experiments (A) and (B):

(A) A fair coin is tossed three times. We note the outcome of each toss.

(B) A fair coin is tossed until it comes up tails. We note how many times the coin came up heads.

1. Define corresponding random variables $\mathbf{A}$ and $\mathbf{B}$ that describe these experiments.

   (4 points)

2. Calculate $H(\mathbf{A})$ and $H(\mathbf{B})$. (Hint: $\sum_{n=1}^{\infty} \frac{n}{2^n} = 2$.)

   (4 points)

3. Is experiment (B) suitable to generate a "random" non-negative integer for cryptographic purposes? Justify your answer.

   (2 points)

Problem 6

Consider a linear congruential generator (LCG) with modulus $m = 8$, multiplier $a = 5$, and increment $c = 3$.

1. Compute the output sequence generated by this LCG. As seed value X_0, use the four digits of your exam registration code (see Problem 0) modulo m.

   (4 points)

2. Is the output sequence Kolmogorov-random? Justify your answer.

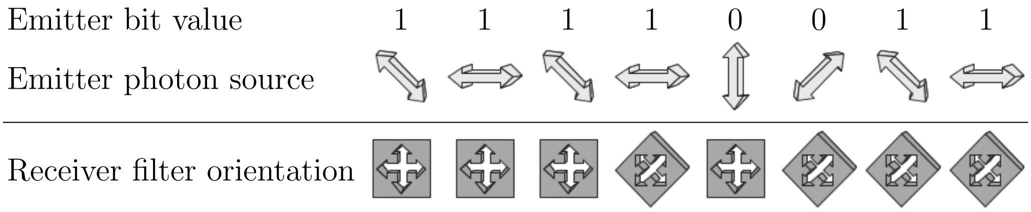
   (3 points)

3. Are LCGs cryptographically secure? Justify your answer.

   (3 points)

Problem 7

1. Give a step-by-step explanation of the quantum key distribution protocol (based on polarized photons). Relate your description to the example session given in the figure below.



   (8 points)

2. In this example session, what is the sifted key?

   (2 points)

Problem 8

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!