Technische Universität München
Theoretische Informatik
Dr. M. Luttenberger / A. Gaiser

Winter term 2010

Cryptography – Mock Exam

Last name: ____________________

First name: ____________________

Student ID no.: ____________________

Signature: ____________________

Code $\in \{A, \ldots, Z\}^6$: | | | | | |

- If you feel ill, let us know immediately.
- Please, **do not write** until told so. You are given approx. 10 minutes to read the exercises and address us in case of questions or problems.
- You will be given **90 minutes** to fill in all the required information and write down your solutions.
- Only fill in a **code** if you agree that your results are published under this code on a webpage.
- Don't forget to **sign**.
- Write with a non-erasable **pen**, do not use red or green color.
- You are not allowed to use **auxiliary means** other than your pen and a simple calculator.
- You may answer in **English or German**.
- Please turn off your **cell phone**.
- Check that you have received **9 sheets of paper** and, please, try to **not destroy the binding**.
- Write your **solutions** directly into the exam booklet.
- Should you require additional **scrap paper**, please tell us.
- You can obtain **40 points** in the exam. You need **17 points** in total to pass including potential bonuses awarded.
- See the next page for a list of **abbreviations**.
- Don't fill in the table below.
- Good luck!

Ex1	Ex2	Ex3	Ex4	Ex5	Ex6	Ex7	$\sum$

Exercise 1 **Yes/No** **each 1P=6P**

Points are rewarded as follows:

- Correct answer: 1P
- Incorrect answer: -1P
- No answer: 0P

The final number of points is the total if positive, otherwise zero.

Remark: See the last page for a list of abbreviations.

	true	false
If PRGs exist, then also PRFs exist.	☐	☐
From every OWF a PRG can be constructed.	☐	☐
You have seen in the lecture how to construct a family of CRHFs based on any OWF.	☐	☐
Computational secret ES exist if and only if CCA-secure ES exist.	☐	☐
Existence of TDPs implies existence of CCA-secure PKES.	☐	☐
Existence of secure DSS is equivalent to the existence of CPA-secure ES.	☐	☐

Exercise 2 **"One-liners"** **5P**

Give a short (one line) answer/explanation using the results from the lecture and the exercises.

(1P): Describe how a strong PRP can be constructed from a PRF F. (Assume F has key and block length n.)

Answer: ____________________

(1P): Show how to solve the DDH relative to $\mathsf{Gen}\mathcal{G}_{\mathbb{P}}$ in PPT. (Recall that Gen returns $I = (\langle \mathbb{Z}_p^*, 1, \cdot \rangle, q, g, x, h)$ with p a n-bit prime, $q = p - 1$, and $\langle g \rangle = \mathbb{Z}_p^*$.)

Answer: ____________________

(1P): Describe one construction which tries to fix the short key length of DES and is conjectured to be secure.

Answer: ____________________

(1P): State the design principle on which AES and the DES-mangler function are based on.

Answer: ____________________

(1P): State why the basic version of the RSA PKES should be used together with randomized padding, and name one padding conjectured to yield a CCA-secure PKES.

Answer: ____________________

Exercise 3

Draw a graph with nodes

$$\{\text{OWF}, \text{UOWHF}, \text{PRF}, \text{CCA-secure ES}, \text{secure MAC}, \text{CPA-secure PKES}\}$$

with an edge from node A to node B if the existence of A is *known* to imply the existence of B.

Exercise 4

Let F be a PRF of key and block length n.

(a) Construct from F a secure MAC scheme for (almost) unrestricted message length. It suffices to define Mac and the padding function.

(b) Briefly describe how a CPA-secure ES and a secure MAC can always be combined into a CCA-secure ES.

Remark: There are several ways to solve (a). It suffice to give a single construction which can handle messages of length $< 2^n$. Don't forget to pad the actual message.

Exercise 5

Let F be a PRP of key and block length n. Define $T_k[t](x) := F_t(x \oplus F_k(t))$ for $t \in \{0,1\}^n$.

Show that T is not a secure TBC.

Reminder: Recall T is secure if PPT-Eve can only distinguish with negligible advantage between the following two oracles:

- $\mathcal{O}_T$: initializes itself by choosing $k \overset{u}{\in} \{0,1\}^n$; then answers a query (t, x) by $T_k[t](x)$.
- $\mathcal{O}_{\text{ideal}}$: has an independent instance $\mathcal{O}^t_{\text{perm}}$ of the random permutation oracle for every tweak $t \in \{0,1\}^n$, and answers a query (t, x) by $\mathcal{O}^t_{\text{perm}}(x)$.

Exercise 6

Let $\mathbb{G} = \langle \mathbb{Z}_{23}^*, \cdot, 1 \rangle$.

(a) Show that $g = 5$ is a generator of $\mathbb{G}$.

(b) Compute all values of a run of the Diffie-Helman protocol for Bob's resp. Alice's secret exponent $b = 4$ resp. $a = 9$ and the shared group $\mathbb{G} = \mathbb{Z}_{23}^*$ with $g = 5$.

(c) Briefly describe how the DH protocol and the El Gamal PKES are related to each other.

(d) Let $\mathsf{Gen}\mathcal{G}$ be the DLP-generator used in an El Gamal PKES.

- Formally state the problem which needs to hard relative to $\mathsf{Gen}\mathcal{G}$ in order for the PKES, and describe such a conjectured generator.
- Propose a subgroup of $\mathbb{Z}_{23}^*$ which is better suited for the DH protocol and El Gamal.

  It suffices to state a generator and the size of the subgroup.

Abbreviations:

- OWF = one-way function (family/collection)
- OWP = one-way permutation (family/collection)
- TDP = trapdoor one-way permutation
- PRG = pseudorandom generator
- PRF = pseudorandom function
- PRP = pseudorandom permutation
- UOWHF = universal one-way hash function (family/collection)
- CRHF = collision resistant hash function (family/collection)
- ES = (private-key) encryption scheme
- PKES = public-key encryption scheme
- MAC = message authentication code
- DSS = digital signature scheme
- DLP = discrete logarithm problem