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

Winter term 2010

Cryptography – Endterm

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	$\sum$

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
- TBC = tweakable block cipher
- 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

<u>Exercise 1</u> **True/False** **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.

	true	false
The one-time-pad ES is CPA-secure.	☐	☐
For a perfectly secret ES with message space $\mathcal{M}$ and key space $\mathcal{K}$, $\lvert\mathcal{K}\rvert \geq \lvert\mathcal{M}\rvert$ has to hold.	☐	☐
If PRGs exist, then $\mathbf{P} \neq \mathbf{NP}$.	☐	☐
No deterministic (stateless) ES can be CCA-secure.	☐	☐
You have seen in the lecture how to construct a family of CRHFs based on the assumption that the DLP is hard relative to **any** DLP-generator.	☐	☐
Let F be a PRP of key and block length n. Then $T_k[t](x) := F_t(x) \oplus k$ is a secure TBC.	☐	☐

Exercise 2 **"One-liners"** **1P each = 10P**

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

(1P): Summarize Kerckhoff's main principle.

Answer: ____________________

(1P): State the four main goals of cryptography.

Answer: ____________________

(1P): Roughly spoken, the *computational Diffie-Hellman problem* requires Eve to ...

Answer: ____________________

(1P): Based on which requirement on the DLP-generator $\mathsf{Gen}\mathcal{G}$ can the El Gamal PKES be proven CPA-secure?

Answer: ____________________

(1P): State the name of a DSS based on the RSA-TDP which can be proven secure in the random oracle model.

Answer: ____________________

(1P): Let $h : \{0,1\}^l \times \{0,1\}^l \rightarrow \{0,1\}^l$ be a compression function, and H_{IV} the hash function obtained from h using the Merkle-Damgård construction with IV as the intialization vector. Construct from h a MAC using the NMAC construction.
It suffices to define Mac.

Answer: ______________________________

(1P): SHA-1 is not considered collision-resistant anymore, but NMAC instantiated with SHA-1 may still be considered a secure MAC - based on which assumption?

Answer: ______________________________

(1P): Briefly describe a decision procedure to solve the DDH in prime order groups of the form $\langle \mathbb{Z}_p^*, \cdot, 1\rangle$ in DPT with non-negligible probability.
Given $(p, p-1, g, g^a, g^b, z)$ ...

Answer: ______________________________

(1P): Assume Alice and Bob use an RSA-based PKES with N_A resp. N_B Alice's resp. Bob's modulus. Assume that N_A and N_B are products of two odd primes with $N_A \neq N_B$. Show that PPT-Eve can decrypt any message sent to Alice or Bob if $\gcd(N_A, N_B) > 1$.

Answer: ______________________________

(1P): Name one type of attack not covered by the definition of secure MAC scheme.

Answer: ______________________________

Exercise 3 **3P**

Draw a graph with nodes

$$\{\mathrm{OWP}, \mathrm{PRG}, \mathrm{PRP}, \text{CPA-secure ES}, \text{secure DSS}, \text{CCA-secure PKES}, \mathrm{TDP}\}$$

and edges $A \to B$ if it was mentioned in the lecture that the existence of A implies the existence of B.

Remark: Say that two nodes are equivalent if $A \to B$ and $B \to A$. Feel free to combine equivalent nodes into a single node but state explicitly which nodes are combined into one.

Exercise 4 **6P**

Let F be a PRF (not necessarily a PRP) of key and block length n

(a) (2P) Construct from F a CPA-secure ES $\mathcal{E}^f = (\mathsf{Gen}^f, \mathsf{Enc}^f, \mathsf{Dec}^f)$ for messages of fixed length $l(n) = n$ (based on the assumption that F is a PRF).

(b) i) (1P) Construct from $\mathcal{E}^f$ (not from F) a CPA-secure ES $\mathcal{E}$ with admissible message space $(\{0,1\}^n)^+$ (based on the assumption that $\mathcal{E}^f$ is CPA-secure). Here, it suffices to define $\mathsf{Enc}_k(m)$.

ii) (1P) Assuming that $\mathcal{E}^f$ is CCA-secure, does your construction guarantee that $\mathcal{E}$ is also CCA-secure? (y/n)

(c) i) (1P) Name two modes of operations which can be used to construct from F directly a CPA-secure ES with admissible message space $(\{0,1\}^n)^+$ (based on the assumption that F is a PRF).

ii) (1P) State two advantages of these modes compared to the two-step construction of (a) and (b).

Remarks:

- If you use constructions not mentioned in the lecture nodes (slides), then you need to show that your constructions indeed have the required properties.
- $(\{0,1\}^n)^+ = \{m \in \{0,1\}^+ \mid \exists k > 0 : |m| = k \cdot n\}$.

Exercise 5 **7P**

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

(a) (2P) Draw the two-round Feistel network $P_{k_1,k_2}(x||y) := \mathrm{FN}_{F_{k_1},F_{k_2}}(x||y)$ based on F using two independent round keys $k_1, k_2 \overset{u}{\in} \{0,1\}^n$.

Remark: k_1 should be the key that is used in the first round. x is the "left half" of the input, y is the "right half".

(b) i) (2P) Compute $P_{k_1,k_2}(0^n||y)$ and $P_{k_1,k_2}(F_{k_1}(0^n) \oplus z||0^n)$.

ii) (1P) Show that PPT-Eve can compute P_{k_1,k_2}^{-1} when given oracle access to P_{k_1,k_2}.

(c) (2P) Is $\mathrm{FN}_{F_{k_1},F_{k_2},F_{k_3}}$ with three independent keys $k_1, k_2, k_3 \overset{u}{\in} \{0,1\}^n$ a PRP? Is it a PRF? (y/n)

Exercise 6 **6P**

Let $p = 5, q = 11, N = 55$ and $\mathbb{G} = \langle \mathbb{Z}_{55}^*, \cdot, 1 \rangle$. For $k \in \mathbb{N}$ set $\pi_k(x) := x^k \bmod N$.

(a) (1P) Show that π_3 is a permutation on $\mathbb{G}$.

Remark: You have seen at least two conditions on k s.t. π_k is a permutation.

(b) i) (2P) Determine, preferably the minimal, $d \in \mathbb{N}$ s.t. $\pi_d = \pi_3^{-1}$.

ii) (1P) What algorithm can be used to determine d efficiently? State precisely what the algorithm computes.

Remark: It doesn't matter how you determine d (except for cheating). But you need to argue that d is the inverse of π_3.

(c) (2P) Compute $\pi_3^{-1}(6)$ using the Chinese remainder theorem and Garner's formula:

$$I^{-1}(u, v) = \big(((u - v)(q^{-1} \bmod p)) \bmod p\big) \cdot q + v$$

Remark: Please, make the steps of your computation visible to us.

Exercise 7 **2P***

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

Define $G : \{0,1\}^n \to \{0,1\}^{2n}$ by $G(k) := F_k(0^n)F_k(0^{n-1}1)$.

Show formally that G is a PRG based on the assumption that F is a PRF.

Hint: Construct from a PPT-distinguisher $\mathcal{D}_G$ for G a PPT-distinguisher $\mathcal{D}_F$ for F.