Department of Computer Science
Chair of Computer Networks and Telematics
Prof. Dr. Christian Schindelhauer

Exam:	„Mock Exam 5: Introduction to Cryptography“
Date and time:	2020/08/08 15:48
Duration:	90 minutes
Room:	your room
Permitted exam aids:	none (well, not this time, but in the real exam)
Examiner:	Prof. Dr. Christian Schindelhauer

Family name: .....

First name: .....

Matriculation number: .....

Subject: .....

Program: ☐ Bachelor ☐ Master ☐ Lehramt ☐ others

Signature: .....

NOTES

- Please fill out this form.
- Please write your matriculation number on each paper sheet.
- Please fill in your answer in the designated areas.

	Max	Reached	Comments
Basics	24		
DES & AES	9		
Fields and Modular Arithmetics	21		
Hash Functions, Digital Signature and Cryptographic Protocols	16		
Public Key Cryptography	16		
Quantum Cryptography	4		
Sum	90		

Grade: .....

Date of the review of the exam: .....

Signature of the examiner: .....

Question 1: Basics [24 Points]

(a) [*10 Points*] Show that a second pre-image resistant hash function is a one-way function.

(b) [*6 Points*] Name three examples of a side channel attack.

(c) [*8 Points*] What is provable security? Do provable secure ciphers exist? If yes, name one, If not, why?

Question 2: DES & AES [9 Points]

(a) [*4 Points*] What security feature is obtained by the input permutation of DES?

(b) [*5 Points*] Name the four operations used in AES to manipulate the states. Which states use the key?

Question 3: Fields and Modular Arithmetics [21 Points]

(a) [*8 Points*] Give all four possible notations for all four elements of a finite field $GF[4]$ using a generator g.

(b) [*5 Points*] Is there a number $x \in \{0, \ldots, 15\}$ such that $x \bmod 5 = 4$ and $x \bmod 3 = 2$. Compute this value using $5^{-1} \bmod 3 = 2$ and $3^{-1} \bmod 5 = 2$.

(c) [*8 Points*] Consider a prime number p with $p \bmod 4 = 3$ and a non-zero square number $x \equiv z^2 \pmod{p}$ for some $z \in \mathbb{Z}_p^*$.
Compute the Legendre-Symbols $\left(\frac{x}{p}\right)$ and $\left(\frac{-1}{p}\right)$.

Question 4: Crypto Hash Functions, Digital Signature and Crypto Protocols [16 Points]

(a) [*4 Points*] Give an upper bound for the probability that for a given a cryptographic hash function $f : \{0,1\} \rightarrow \{0,1\}^n$ there are no collisions after processing k random large documents.

(b) [*6 Points*] What is the "Hash-then-Sign"-paradigm and its motivation.

(c) [*6 Points*] Explain the tasks of prover and verifier in an interactive proof system.

Question 5: Public Key Cryptography [16 Points]

(a) [*10 Points*] Name a semi-homomorphic public-key-cipher.
Prove the semi-homomorphism.

(b) [*6 Points*] Define an elliptic curve over $\mathbb{R}$ with a singularity. Where is the singularity and why?

Question 6: Quantum Cryptography [4 Points]

(a) [*4 Points*] Give a mathematical definition of unitary matrices.