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

Exam:	„Mock Exam 13: Introduction to Cryptography“
Date and time:	2020/09/04 11:07
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	9		
DES & AES	20		
Fields and Modular Arithmetics	27		
Hash Functions, Digital Signature and Cryptographic Protocols	10		
Public Key Cryptography	16		
Quantum Cryptography	8		
Sum	90		

Grade: ....

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

Signature of the examiner: ....

Question 1: Basics [9 Points]

(a) [*9 Points*] Explain Kerckhoff's principle and give one argument in favor and one against it.

Question 2: DES & AES [20 Points]

(a) [*10 Points*] In 1-DES all 16 rounds of Feistel-Ciphers are replaced by one round of Feistel ciphers. Discuss the security of 1-DES.

(b) [*10 Points*] Describe the Output Feedback Mode Encryption.

Question 3: Fields and Modular Arithmetics [27 Points]

(a) [*5 Points*] Is there a finite field with nine elements? Why or why not?

(b) [*12 Points*] Assume there is an element $z \in \{0,1\}^w$ such that $z^k = 1$ and $\gcd(k, 2^w - 1) = 1$. For which other ℓ do we observe $z^\ell = 1$?

(c) [*10 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 $z \in \mathbb{Z}_p^*$.
Show that $x^{\frac{p+1}{4}} \bmod p$ is a square root of x.

Question 4: Crypto Hash Functions, Digital Signature and Crypto Protocols [10 Points]

(a) [*10 Points*] Give a zero-knowledge proof for showing that the prover knows the discrete root r of $c = g^r \mod p$ for a public c, public generator g and a public prime number.

Question 5: Public Key Cryptography [16 Points]

(a) [*10 Points*] Consider the elliptic curve

$$y^2 = x^3 - 3x$$

for $E(\mathbb{R})$. For the point $P = (0, 0)$ compute $-P$.

(b) [*6 Points*] Which of the operations Plus, Star, Inverse-Element, scalar multiplication and inverse scalar multiplication in elliptic curves are easy and which ones are hard?

Question 6: Quantum Cryptography [8 Points]

(a) [*8 Points*] Present a quantum circuit that produces a quantum entanglement.