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

Exam: „Mock Exam 4: Introduction to Cryptography“
Date and time: 2020/08/08 15:36
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	15		
DES & AES	6		
Fields and Modular Arithmetics	27		
Hash Functions, Digital Signature and Cryptographic Protocols	12		
Public Key Cryptography	24		
Quantum Cryptography	6		
Sum	90		

Grade: .....
Date of the review of the exam: .....
Signature of the examiner: .....

Question 1: Basics [15 Points]

(a) [*6 Points*] Give three security objectives and describe each with one sentence.

(b) [*9 Points*] Explain the Vernam Cipher! Why is it provable secure?

Question 2: DES & AES [6 Points]

(a) [*6 Points*] Is DES regarded secure? Why or why not?

Question 3: Fields and Modular Arithmetics [27 Points]

(a) [*11 Points*] Give a possible addition table and multiplication table for a finite field with four elements? Name the neutral elements.

(b) [*6 Points*] Is x^3 a generator for $GF[2^4]$ modulo polynomial $x^4 + x + 1$?
Hint: Compute $(x+1)^3$ and $(x+1)^5$

(c) [*10 Points*] Prove the theorem of Euler.

Question 4: Crypto Hash Functions, Digital Signature and Crypto Protocols [12 Points]

(a) [*12 Points*] How can one prove perfect zero-knowledge in a Zero-Knowledge-Proof.

Question 5: Public Key Cryptography [24 Points]

(a) [*12 Points*] Assume that there is a method to solve equations of form $x^3 + px + q = 0$. Show how it can be used to solve $ax^3 + bx^2 + cx + d = 0$.

(b) [*12 Points*] Describe the Menezes-Venstone variant of El-Gamal Encryption using elliptic curves.

Question 6: Quantum Cryptography [6 Points]

(a) [*6 Points*] Name three quantum circuit gates and show their symbols.