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

Exam: „Mock Exam 1: Introduction to Cryptography“
Date and time: 2020/08/08 14:43
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	6		
DES & AES	10		
Fields and Modular Arithmetics	30		
Hash Functions, Digital Signature and Cryptographic Protocols	22		
Public Key Cryptography	10		
Quantum Cryptography	12		
Sum	90		

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

Question 1: Basics [6 Points]

(a) [*6 Points*] Desribe the three necessary functions for a general symmetric cryptographic cipher with inputs, outputs and function!

Question 2: DES & AES [10 Points]

(a) [*4 Points*] Explain the difference between block and stream ciphers!

(b) [*6 Points*] Describe the Mix-Columns operator of AES (assume that the matrix A is given).

Question 3: Fields and Modular Arithmetics [30 Points]

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

(b) [*9 Points*] Give the mathematical expression to perform fast multiplication $a \cdot b$ using table lookup for powers of a generating element g in $GF[2^w]$.

(c) [*8 Points*] Let $p > 2$ be a prime number. Show that there exists at least two square roots a, b of $25 \bmod p$, i.e. $a \not\equiv b \pmod{p}$ and $a^2 \equiv b^2 \equiv 25 \pmod{p}$.

(d) [*2 Points*] For which n is the Jacobi-Symbol $\left(\frac{a}{n}\right)$ also called the Legendre-Symbol.

Question 4: Crypto Hash Functions, Digital Signature and Crypto Protocols [22 Points]

(a) [*6 Points*] What is a cryptographic Hash function? Name two applications.

(b) [*16 Points*] Show how to compute a digital signature using elliptic curves.

Question 5: Public Key Cryptography [10 Points]

(a) [*6 Points*] What is the number of generators/primitive roots of $\mathbb{Z}_p^*$ (p is prime number).

(b) [*4 Points*] Consider the elliptic curve

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

for $E(\mathbb{R})$. For the points $P = (-1, \sqrt{2})$, $Q = (-1, -\sqrt{2})$ compute $(P \star Q)$.

Question 6: Quantum Cryptography [12 Points]

(a) [*6 Points*] Give the matrix definition of the CNOT gate.

(b) [*6 Points*] How can be an eavesdropper in the Bennett and Brassard scheme detected?