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

Exam: „Mock Exam 6: Introduction to Cryptography“
Date and time: 2020/08/08 15:58
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	8		
DES & AES	18		
Fields and Modular Arithmetics	18		
Hash Functions, Digital Signature and Cryptographic Protocols	12		
Public Key Cryptography	24		
Quantum Cryptography	10		
Sum	90		

Grade: ....

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

Signature of the examiner: ....

Question 1: Basics [8 Points]

(a) [*8 Points*] Describe the message authentication using a symmetric key with a picture.

Question 2: DES & AES [18 Points]

(a) [*10 Points*] Describe how DES can be attacked by a brute-force attack based on a known-message attack. How many attempts are necessary on the expectation?

(b) [*8 Points*] Can DES extended to a secure scheme? If yes, how?

Question 3: Fields and Modular Arithmetics [18 Points]

(a) [*8 Points*] Compute 1011×1101 in $GF[2^4]$ using the irreducible polynnomial $x^4 + x + 1$.

(b) [*10 Points*] Prove the little theorem of Fermat.

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

(a) [*4 Points*] Name four real-word cryptographic hash functions.

(b) [*8 Points*] Describe Diffie-Hellman Key Exchange protocol.

Question 5: Public Key Cryptography [24 Points]

(a) [*6 Points*] Give three types of mistakes when choosing prime numbers for RSA.

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

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

for $E(\mathbb{R})$. For the points $P = (0, 0)$, $Q = (-\sqrt{3}, 0)$ compute $P \star Q$ and $P + Q$.

(c) [*8 Points*] Give a mathematical definition of the Star-operator $P \star Q$ for $P = (x_p, y_p)$, $Q = (x_q, y_q)$ and $x_p = x_q$.

Question 6: Quantum Cryptography [10 Points]

(a) [*10 Points*] Describe why it is not possible to explain the double slit experiment using a wave model.