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

Exam:	„Mock Exam 2: Introduction to Cryptography“
Date and time:	2020/08/08 15:05
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	11		
DES & AES	9		
Fields and Modular Arithmetics	22		
Hash Functions, Digital Signature and Cryptographic Protocols	14		
Public Key Cryptography	26		
Quantum Cryptography	8		
Sum	90		

Grade: ....

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

Signature of the examiner: ....

Question 1: Basics [11 Points]

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

(b) [*5 Points*] Describe an example of a social engineering attack.

Question 2: DES & AES **[9 Points]**

(a) [*9 Points*] Explain the Feistel cipher with a picture. Describe all of its components.

Question 3: Fields and Modular Arithmetics [22 Points]

(a) [*6 Points*] Name three fields.

(b) [*8 Points*] How is the multiplication mathematically defined in a finite field $GF[2^n]$?

(c) [*8 Points*] Compute $\phi(n) = |\mathbb{Z}_n^*|$ for $n \in \{2, 5, 10, 100\}$.

Question 4: Crypto Hash Functions, Digital Signature and Crypto Protocols [14 Points]

(a) [*10 Points*] Describe the birthday attack against a cryptographic hash function.

(b) [*4 Points*] What is a certification authority?

Question 5: Public Key Cryptography [26 Points]

(a) [*12 Points*] If Bridget and Bob use the public key, show how a chosen message attack can be used to decode a given code c.

(b) [*8 Points*] Consider the elliptic curve

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

for $E(\mathbb{R})$. For the points $P = (-1, \sqrt{2})$, $Q = (0, 0)$ compute $P + Q$.

(c) [*6 Points*] Given an elliptic curve. What is the inverse element of $P = (x_p, y_p)$ with respect to the Plus-operator.

Question 6: Quantum Cryptography [8 Points]

(a) [*8 Points*] Give a mathematical description of the measurement gate of a quantum state describing a quantum bit. What is its symbol?