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

Exam:	„Mock Exam 10: Introduction to Cryptography“
Date and time:	2020/09/04 10:44
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	4		
DES & AES	15		
Fields and Modular Arithmetics	25		
Hash Functions, Digital Signature and Cryptographic Protocols	9		
Public Key Cryptography	29		
Quantum Cryptography	8		
Sum	90		

Grade: ....

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

Signature of the examiner: ....

Question 1: Basics [4 Points]

(a) [*4 Points*] Explain the known plaintext attack with a picture.

Question 2: DES & AES **[15 Points]**

(a) [*5 Points*] Compute the number of permutation functions $f : \{1, \ldots, n\} \mapsto \{1, \ldots, n\}$!

(b) [*10 Points*] Describe the Cipher-Block Chaining Mode Encryption and Decryption.

Question 3: Fields and Modular Arithmetics [25 Points]

(a) [*5 Points*] How is the addition defined in a finite field $GF[2^n]$?

(b) [*12 Points*] For $\mathbb{Z}_n^* = \{x_1, \dots, x_{\varphi(n)}\}$, prove that $\left(\prod_{i=1}^{\varphi(n)} x_i\right)^2 \equiv 1 \pmod{n}$

Hint: Consider the mapping $x_i \mapsto x_i^{-1} \bmod n$ like in the proof of the Euler theorem.

(c) [*8 Points*] For a prime number p define the Legendre-Symbol $\left(\frac{a}{p}\right)$. What is its relation to square numbers in $\mathbb{Z}_p^*$.

Question 4: Crypto Hash Functions, Digital Signature and Crypto Protocols [9 Points]

(a) [*9 Points*] Present a digital signature scheme based on RSA.

Question 5: Public Key Cryptography [29 Points]

(a) [*10 Points*] Explain RSA by giving the public key, secret key, the encoding function, and decoding function.

(b) [*6 Points*] Consider the elliptic curve

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

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

(c) [*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 $P \star Q$.

(d) [*9 Points*] Give a graphical definition of the Star-operator $P \star P$ for $P = (x_p, y_p)$.

Question 6: Quantum Cryptography **[8 Points]**

(a) [*8 Points*] Prove that the Hadamard matrix

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

is a unitary matrix.