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

Exam: „Mock Exam 7: Introduction to Cryptography“
Date and time: 2020/09/03 11:40
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

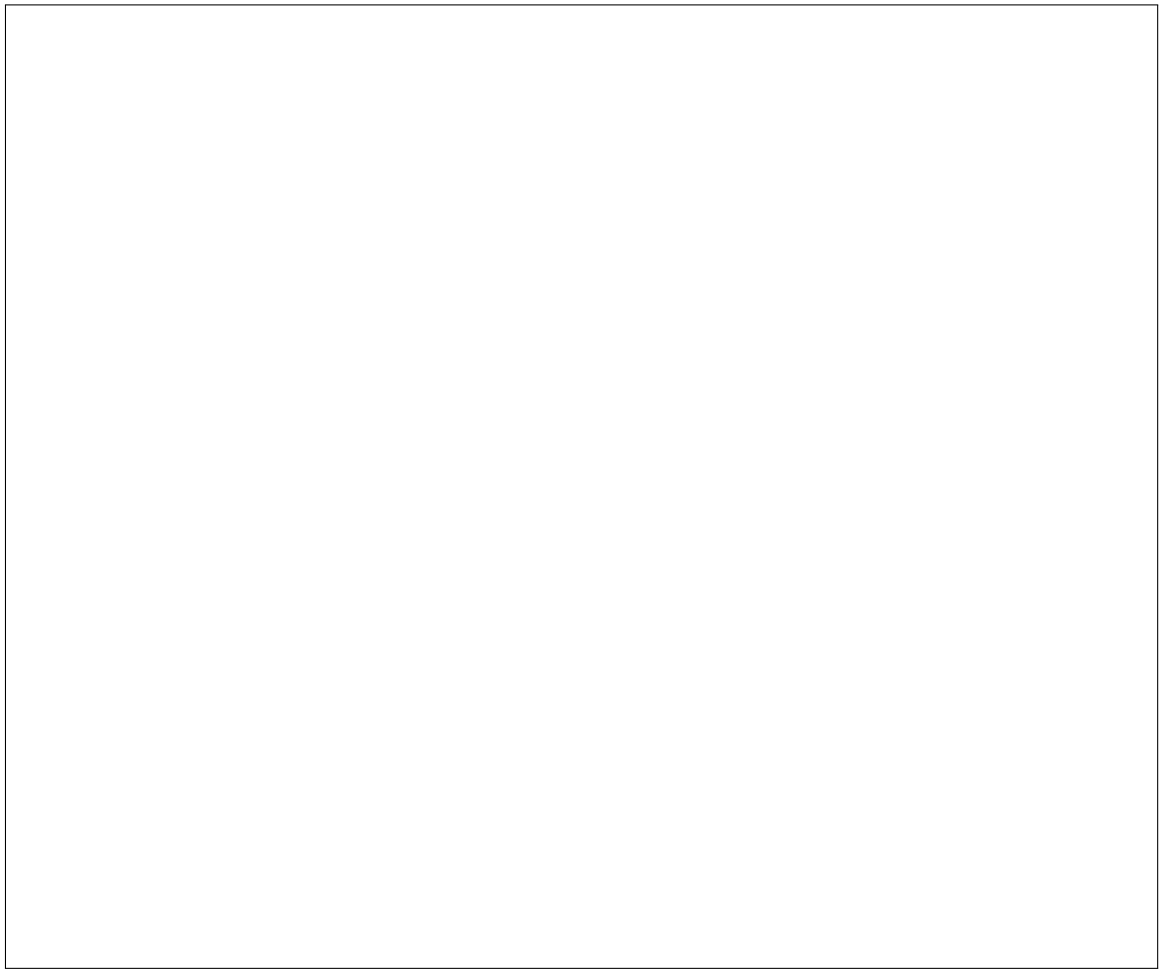
- Please fill out this form.
- Please write your matriculation number on each paper sheet.
- Please fill in your answer in the designated areas.

	Max	Reached	Comments
Basics	4		
DES & AES	13		
Fields and Modular Arithmetics	34		
Hash Functions, Digital Signature and Cryptographic Protocols	9		
Public Key Cryptography	24		
Quantum Cryptography	6		
Sum	90		

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

Question 1: Basics [4 Points]

(a) [*4 Points*] Explain the ciphertext-only attack with a picture



Question 2: DES & AES [13 Points]

(a) [*3 Points*] How many different permutations can be addressed by a key of m bits for a symmetric block cipher of $n = m$ input bits?

(b) [*10 Points*] Describe the Cipher Feedback Mode Encryption.

Question 3: Fields and Modular Arithmetics [34 Points]

(a) [*12 Points*] Name the six properties necessary for a mathematical field by giving the equations.

(b) [*12 Points*] Assume that a finite field $GF[2^w]$ for $w \geq 3$ has a generator (primitive root) g. Prove that for all divisors d of $2^w - 1$ there exists an element $z \in \{0,1\}^w$ with $z \neq 1$ such that $z^d = 1$ (Hint: use $g^{2^w-1} = 1$).

(c) [*4 Points*] For which elements in $\mathbb{Z}_n$ does a multiplicative inverse exist?

(d) [*6 Points*] How many prime numbers exist asymptotically, which are smaller than n? Explain your answer.

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

(a) [*9 Points*] Name and define three different security requirements for cryptographic Hash functions

Question 5: Public Key Cryptography [24 Points]

(a) [*8 Points*] Given an algorithm to compute square roots for a given $n = pq$ for prime numbers p, q. How can it be used to derive the prime numbers?

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

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

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

(c) [*8 Points*] Name the four properties of an Abelian group.

(d) [*4 Points*] Define the extension field over a given elliptic curve $y^2 = x^3 + ax + b$.

Question 6: Quantum Cryptography [6 Points]

(a) [*6 Points*] Check whether the matrix

$$M = \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & i \end{pmatrix}$$

is a unitary matrix.