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

Exam: „Mock Exam 3: Introduction to Cryptography“
Date and time: 2020/08/08 15:26
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	15		
DES & AES	12		
Fields and Modular Arithmetics	20		
Hash Functions, Digital Signature and Cryptographic Protocols	8		
Public Key Cryptography	23		
Quantum Cryptography	12		
Sum	90		

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

Question 1: Basics [15 Points]

(a) [*10 Points*] Show that a collision resistant hash function is second pre-image resistant.

(b) [*5 Points*] Explain the chosen plaintext attack with a picture.

Question 2: DES & AES [12 Points]

(a) [*8 Points*] Compute the number of permutation functions $f : \{0,1\}^n \mapsto \{0,1\}^n$!

(b) [*4 Points*] Name four modes of operations for AES.

Question 3: Fields and Modular Arithmetics [20 Points]

(a) [*4 Points*] Define multiplication and addition for a field of p elements where p is a prime number?

(b) [*8 Points*] Is $x + 1$ a generator for $GF[2^4]$ modulo polynomial $x^4 + x + 1$?
Hint: Compute $(x + 1)^3$ and $(x + 1)^5$.

(c) [*8 Points*] Explain the algorithm of iterative Squaring for the modular exponentiatoin of $a^b \bmod n$ for $b = \sum_{i=0}^{\log n} b_i 2^i$.

Question 4: Crypto Hash Functions, Digital Signature and Crypto Protocols [8 Points]

(a) [*4 Points*] Given a cryptographic hash function of n bits out put. How many tries are necessary using a birthday attack?

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

(c) [*0 Points*] What?

Question 5: Public Key Cryptography [23 Points]

(a) [*12 Points*] Explain probabilistic RSA Encryption.

(b) [*3 Points*] Is there a closed form solution for cubic equations? How about for degree 4? How about for degree 5?

(c) [*8 Points*] Describe the El-Gamal Encryption using elliptic curves.

Question 6: Quantum Cryptography [12 Points]

(a) [*12 Points*] Give a graphical description fo the Quantum key sharing algorithm of Bennett and Brassard.