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

Exam: „Mock Exam 14: Introduction to Cryptography“
Date and time: 2020/09/04 11:47
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	7		
DES & AES	20		
Fields and Modular Arithmetics	32		
Hash Functions, Digital Signature and Cryptographic Protocols	13		
Public Key Cryptography	12		
Quantum Cryptography	6		
Sum	90		

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

Question 1: Basics [7 Points]

(a) [*4 Points*] Name four kinds of attacks against cryptographic ciphers (1-10)

(b) [*3 Points*] What is a cryptographic protocol.

Question 2: DES & AES [20 Points]

(a) [*10 Points*] In 2-DES all 16 rounds of Feistel-Ciphers are replaced by two round of Feistel ciphers. Discuss the security of 2-DES.

(b) [*6 Points*] Explain the principle of DES using its main four ingredients with a picture.

(c) [*4 Points*] Describe the Add-Key operator of AES.

Question 3: Fields and Modular Arithmetics [32 Points]

(a) [*4 Points*] Which property distinguishes an Abelian group from a group. Give the equality.

(b) [*4 Points*] Consider a finite field $GF[2^n]$. Give the neutral element for addition and for multiplication.

(c) [*14 Points*] Which of the following polynomials is irreducible modulo 2.

1. $x + 1$
2. x^2
3. $x^2 + 1$
4. $x^2 + x$
5. $x^2 + x + 1$
6. $x^3 + x + 1$
7. $x^3 + x^2 + x + 1$

(d) [*6 Points*] For which n is the residue class ring modulo n a finite field?

(e) [*4 Points*] Given a primalty test, how can one find a uniformly distributed random prime number in a given intervall $[2^{n-1}, 2^n]$.

Question 4: Crypto Hash Functions, Digital Signature and Crypto Protocols [13 Points]

(a) [*3 Points*] Describe the Matyas-Meyer-Oscars hash function using functions $f : \{0,1\}^{2n} \to \{0,1\}^n$ and $g : \{0,1\}^n \to \{0,1\}^r$ and encryption function $E : \{0,1\}^r \times \{0,1\}^n \to \{0,1\}^n$.

(b) [*10 Points*] Present a digital signature scheme based on the El-Gamal-Crypto-System.

Question 5: Public Key Cryptography [12 Points]

(a) [*12 Points*] Explain Rabin's Encryption.

Question 6: Quantum Cryptography [6 Points]

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

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

is a unitary matrix.