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

Exam:	„Mock Exam 9: Introduction to Cryptography“
Date and time:	2020/09/04 10:36
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	6		
DES & AES	18		
Fields and Modular Arithmetics	16		
Hash Functions, Digital Signature and Cryptographic Protocols	13		
Public Key Cryptography	13		
Quantum Cryptography	24		
Sum	90		

Grade: ....

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

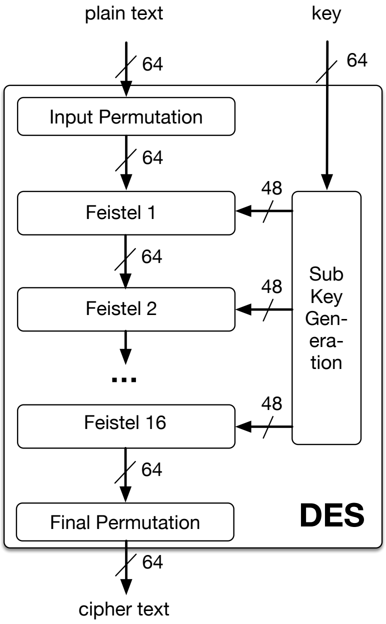
Signature of the examiner: ....

Question 1: Basics [6 Points]

(a) [*6 Points*] Describe message authentication using a secret/public key pair with a picture.

Question 2: DES & AES [18 Points]

(a) [*12 Points*] Show how to compute the DES-Decrypt function on the same level as the picture given here.



(b) [*6 Points*] Describe the Shift-Rows operator of AES for given shift parameters.

Question 3: Fields and Modular Arithmetics [16 Points]

(a) [*4 Points*] State the theorem of Galois.

(b) [*6 Points*] Consider the AES polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$? How large is the lookup table for fast multiplication. How would you determine the basis for the exponentiation table?

(c) [*6 Points*] Given a prime number p is the statement $a^p \equiv a \pmod{p}$ true for all $a \in \mathbb{Z}$? Explain your answer.

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

(a) [*4 Points*] Describe the Merkle-tree construction with a picture given a cryptographic hash function h.

(b) [*9 Points*] Explain completeness, soundness and zero-knowledge of an interactive proof system.

Question 5: Public Key Cryptography [13 Points]

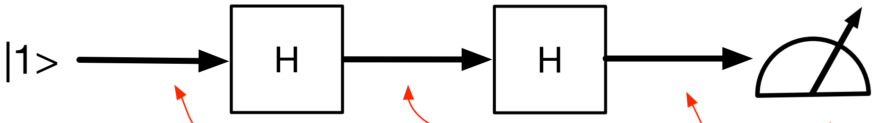
(a) [*9 Points*] Define the notion of a generators/primitive roots of $\mathbb{Z}_p^*$ (p is a prime number). Give an example for a generator in $\mathbb{Z}_3^*$.

(b) [*4 Points*] Name a motivation for the usage of elliptic curve cryptography.

Question 6: Quantum Cryptography [24 Points]

(a) [*6 Points*] Give a mathematical description of the Ket-notation $\langle x|$ and $|s\rangle$. What is $\langle x \mid s\rangle$?

(b) [*12 Points*] Analyse the following quantum circuit and describe the output.



$$\boxed{} \cdot |0\rangle + \boxed{} \cdot |1\rangle$$

$$\boxed{} \cdot |0\rangle + \boxed{} \cdot |1\rangle$$

$$\boxed{} \cdot |0\rangle + \boxed{} \cdot |1\rangle$$

Output 0 with probability $\boxed{}$

Output 1 with probability $\boxed{}$

(c) [*6 Points*] What does the No-Clone theorem state. What is the relationship to Einstein-Podolski-Rosen pairs?