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

Exam: „Mock Exam 15: Introduction to Cryptography“
Date and time: 2020/09/04 12:09
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

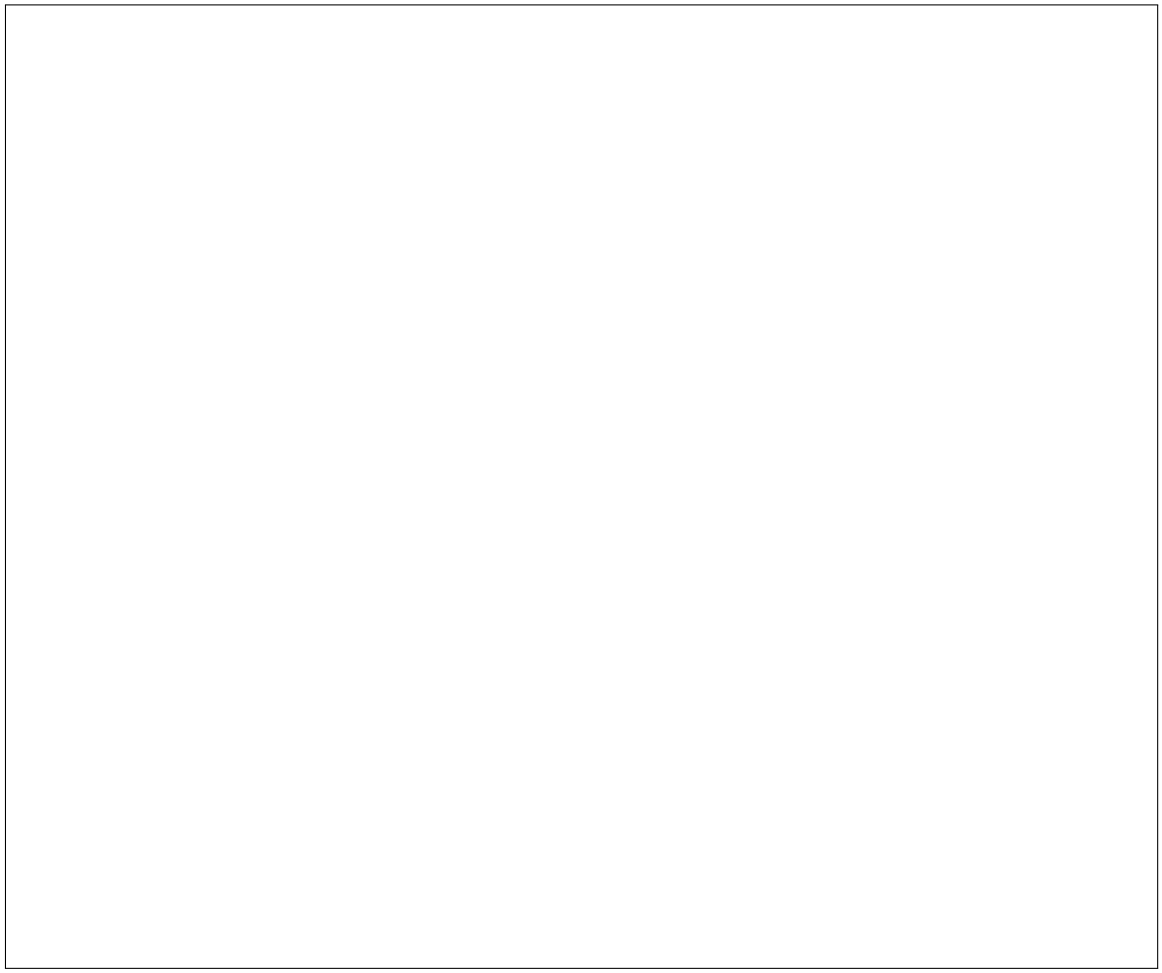
- Please fill out this form.
- Please write your matriculation number on each paper sheet.
- Please fill in your answer in the designated areas.

	Max	Reached	Comments
Basics	6		
DES & AES	16		
Fields and Modular Arithmetics	10		
Hash Functions, Digital Signature and Cryptographic Protocols	12		
Public Key Cryptography	20		
Quantum Cryptography	26		
Sum	90		

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

Question 1: Basics [6 Points]

(a) [*6 Points*] Explain the adaptively chosen plaintext attack with a picture.



Question 2: DES & AES [16 Points]

(a) [*10 Points*] Order the following functions according to their asymptotic growths:

1. $n \mapsto 2^n$
2. $n \mapsto 2^{2^n}$
3. $n \mapsto (2^2)^n$
4. $n \mapsto (2^n)!$
5. $n \mapsto 2^{n^2}$
6. $n \mapsto n!$
7. $n \mapsto n^2$
8. $n \mapsto n^{2^2}$
9. $n \mapsto n^n$
10. $n \mapsto n^{n^n}$

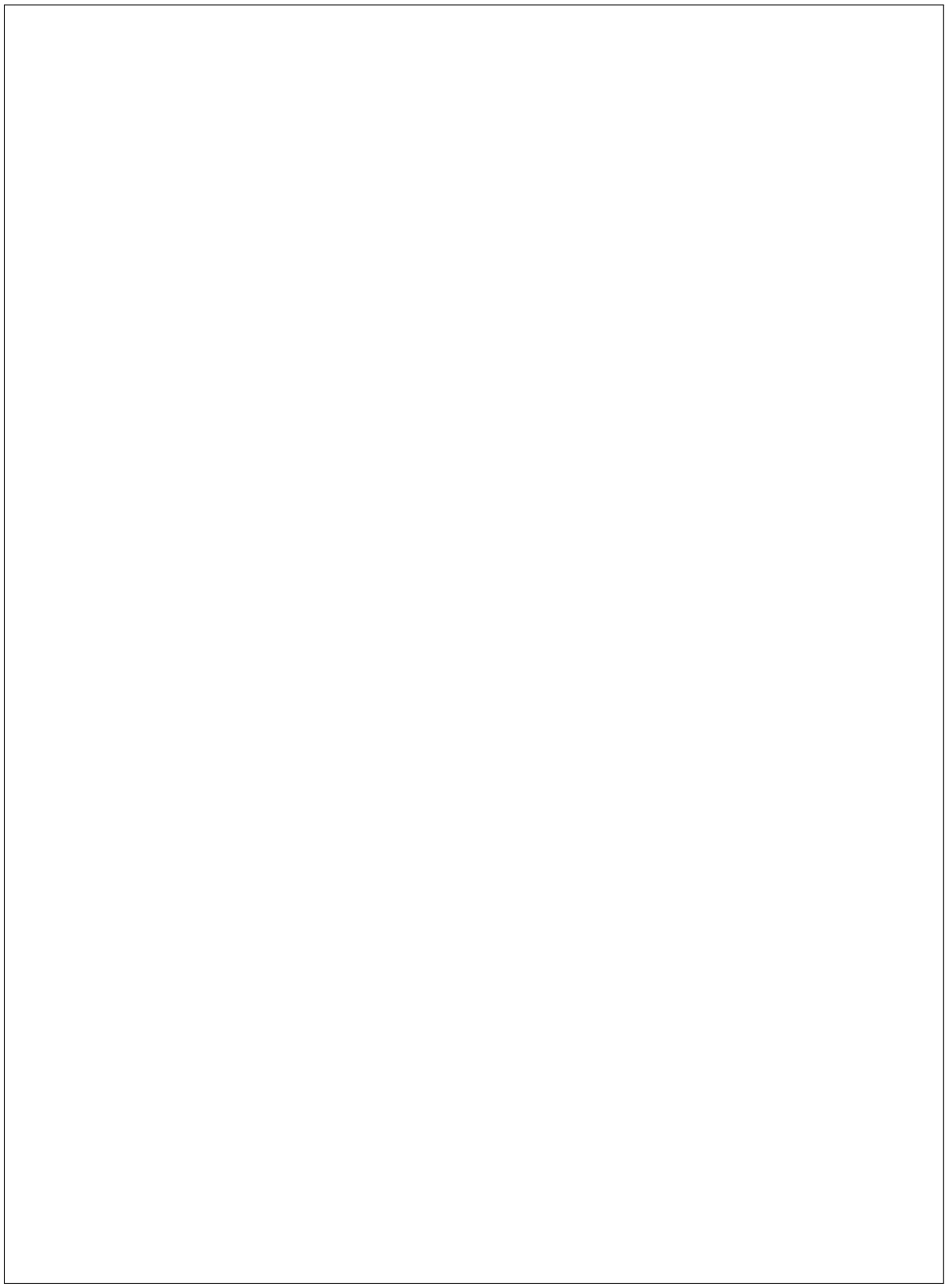
(b) [*6 Points*] Describe the Sub-Byte operator of AES (assume that the matrix A and vector b is given).

Question 3: Fields and Modular Arithmetics [10 Points]

(a) [*10 Points*] Explain the Solovay-Strassen test based on the Jacobi-Legendre-Symbol $\left(\frac{a}{p}\right)$.

Question 4: Crypto Hash Functions, Digital Signature and Crypto Protocols [12 Points]

(a) [*12 Points*] Describe the Fiat-Shamir identification protocol.



Question 5: Public Key Cryptography [20 Points]

(a) [*6 Points*] Is 3 a generator for $\mathbb{Z}_5^*$? Prove your statement.

(b) [*10 Points*] Consider the elliptic curve

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

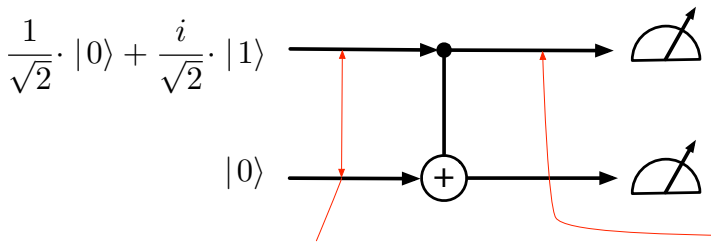
for $E(\mathbb{R})$. For the points $P = (-1, \sqrt{2})$, $Q = (-\sqrt{3}, 0)$ compute $(P \star Q)$.

(c) [*4 Points*] Given the Star-operator define the Plus-operator for a given elliptic curve.

Question 6: Quantum Cryptography [26 Points]

(a) [*10 Points*] Describe why it is not possible to explain the double slit experiment using a particle model.

(b) [*16 Points*] Analyse the following quantum circuit and describe the output.



$\square \cdot |00\rangle + \square \cdot |01\rangle + \square \cdot |10\rangle + \square \cdot |11\rangle$

$\square \cdot |00\rangle + \square \cdot |01\rangle + \square \cdot |10\rangle + \square \cdot |11\rangle$

Output 00 with probability $\square$

Output 01 with probability $\square$

Output 10 with probability $\square$

Output 11 with probability $\square$