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

Exam: „Mock Exam 11: Introduction to Cryptography“
Date and time: 2020/09/04 10:50
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	10		
DES & AES	20		
Fields and Modular Arithmetics	16		
Hash Functions, Digital Signature and Cryptographic Protocols	12		
Public Key Cryptography	14		
Quantum Cryptography	18		
Sum	90		

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

Question 1: Basics [10 Points]

(a) [*10 Points*] Given a cryptographic hash function $h : \{0,1\}^* \rightarrow \{0,1\}^n$. Prove that Prob$[h(x_1) = h(x_2)] \geq \frac{1}{2^n}$ for two uniformly and independently chosen $x_1, x_2 \in \{0,1\}^m$ for any $m \geq 1$.

Question 2: DES & AES [20 Points]

(a) [*8 Points*] Describe how DES can be attacked by a brute-force attack based on a known-message attack. Is it conceivable that DES can be attacked by a cipher only attack? Why and if yes, how?

(b) [*12 Points*] Is a two-round Feistel cipher secure against an adaptive chosen message attack? Explain, why or why not.(2-2)

Question 3: Fields and Modular Arithmetics [16 Points]

(a) [*6 Points*] Compute $x(x+1)$ in $GF[4]$ with irreducible polynomial x^2+x+1.

(b) [*4 Points*] Give the relation of dividend n, divisor m, the quotient q and remainder m in one equation.

(c) [*6 Points*] If $a^p \equiv a \pmod{p}$ is true for all $a \in \mathbb{Z}$ does it follow that p is a prime number? Explain your answer.

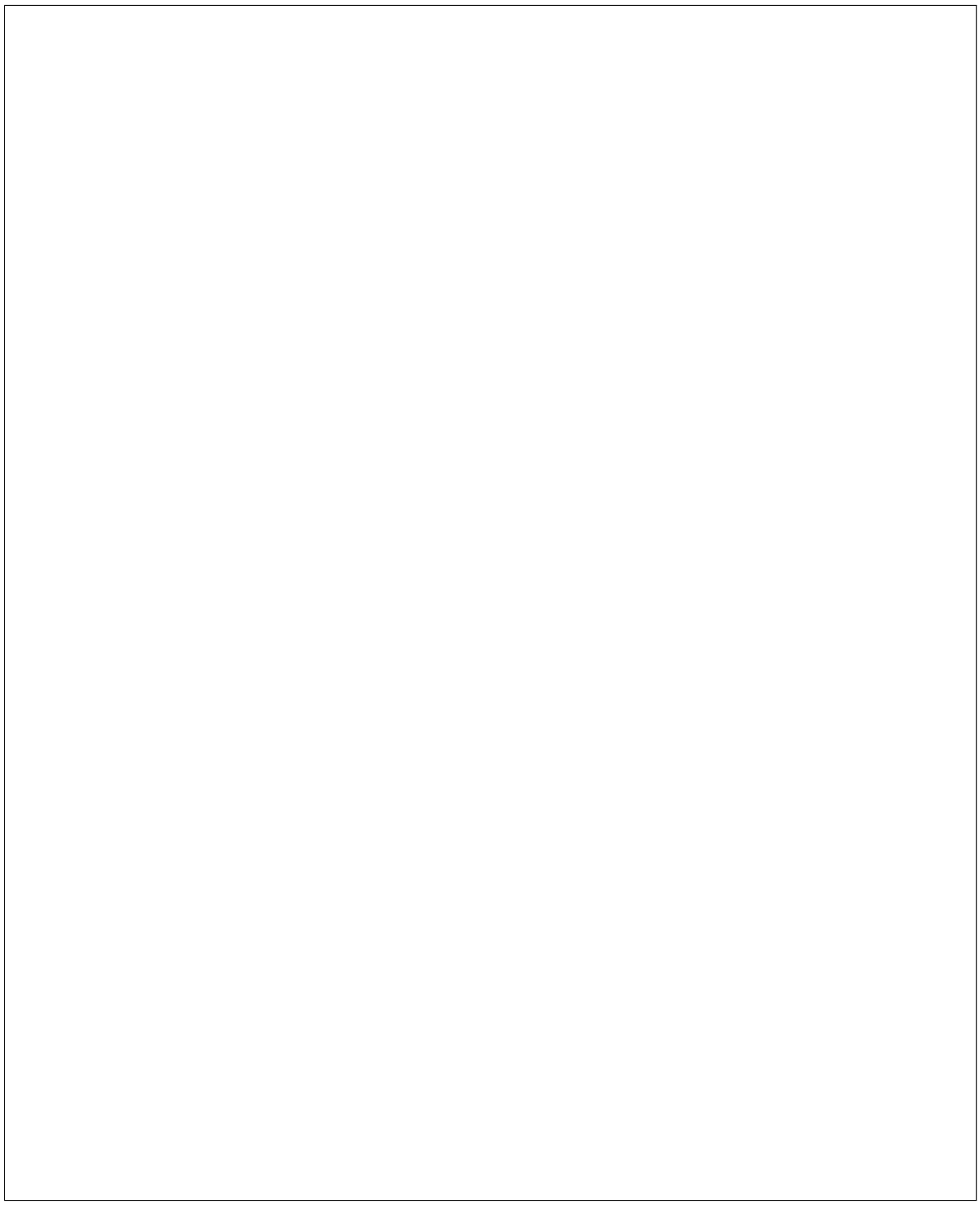
Question 4: Crypto Hash Functions, Digital Signature and Crypto Protocols [12 Points]

(a) [*12 Points*] Assume that a function $f : \{0,1\}^{n+r} \rightarrow \{0,1\}^n$ is collision-resistant. How can it used to construct a collision-resistant cryptographic hash-function of arbitrary input length. Prove it.

Question 5: Public Key Cryptography [14 Points]

(a) [*6 Points*] Is 2 a generator for $\mathbb{Z}_7^*$? Prove your statement.

(b) [*8 Points*] Give a graphical definition of the Star-operator.



Question 6: Quantum Cryptography [18 Points]

(a) [*6 Points*] Describe a quantum state with the double slit experiment.

(b) [*12 Points*] Describe the six rounds in the Quantum key sharing algorithm of Bennett and Brassard.