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

Exam: „Mock Exam 16: Introduction to Cryptography“
Date and time: 2020/09/04 14:38
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

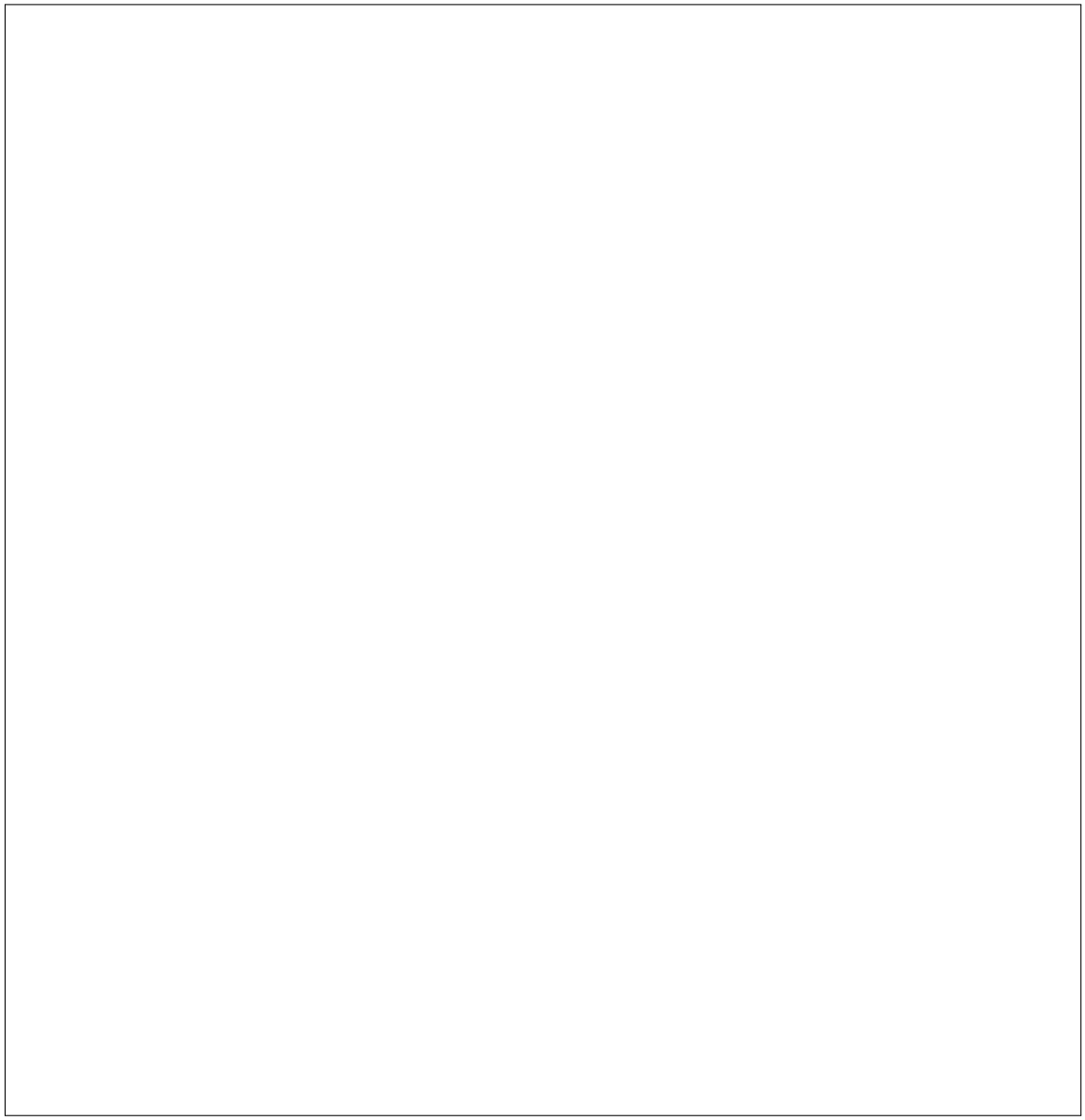
- Please fill out this form.
- Please write your matriculation number on each paper sheet.
- Please fill in your answer in the designated areas.

	Max	Reached	Comments
Basics	6		
DES & AES	12		
Fields and Modular Arithmetics	28		
Hash Functions, Digital Signature and Cryptographic Protocols	10		
Public Key Cryptography	28		
Quantum Cryptography	6		
Sum	90		

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

Question 1: Basics [6 Points]

(a) [*6 Points*] Describe a Challenge and Response Protocol with a figure.



Question 2: DES & AES [12 Points]

(a) [*12 Points*] Describe the electronic Codebook Mode and explain why it should be avoided.

Question 3: Fields and Modular Arithmetics [28 Points]

(a) [*12 Points*] Define the set of square residuals modulo n as $\mathbb{QR}_p := \{x^2 \mid x \in \mathbb{Z}_n\}$. Let $p > 2$ be a prime number. Show that every square number $x \in \mathbb{QR}_p$ has not more than two roots.
(Hint: consider $a^2 - b^2 = (a - b)(a + b)$).

(b) [*8 Points*] State the Chinese Remainder Theorem for two prime numbers p, q.

(c) [*8 Points*] Give a general definition of the Jacobi-Symbol $\left(\frac{a}{n}\right)$. What is the relationship to the Legendre-Symbol?

Consider the El-Gamal based Digital Signature from the lecture:
public : large prime number p, generator $g \in \mathbb{Z}_n^*$
secret : $x \in \{1, \ldots p-2, \}$
public : $y = g^x \bmod p$
input : message $m \in \{1, \ldots, p-2\}$
output: signature σ

repeat
  $k \leftarrow$ `random from` : $\{1, \ldots, p-2\}$
until $\gcd(k, p-1) = 1$
$r \leftarrow g^k \bmod p$
$s \leftarrow k^{-1}(m - rx) \bmod (p-1)$
$\sigma = (m, r, s)$
return σ

Question 4: Crypto Hash Functions, Digital Signature and Crypto Protocols [10 Points]

(a) [*10 Points*] Assume that k is published with the signature σ. Show how to compute the secret x with this information.

Question 5: Public Key Cryptography [28 Points]

(a) [*12 Points*] Describe the El-Gamal-Encryption method.

(b) [*8 Points*] Give a mathematical definition of the Star-operator $P \star Q$ for $P = (x_p, y_p)$, $Q = (x_q, y_q)$ and $x_p \neq x_q$.

(c) [*8 Points*] Give a definition of scalar multiplication in elliptic curves based on the Plus-operator. How can it be computed efficiently?

Question 6: Quantum Cryptography [6 Points]

(a) [*6 Points*] Given two independent quantum bits $|\phi_1\rangle = (\alpha_1, \alpha_2)$ and $|\phi_2\rangle = (\beta_1, \beta_2)$ compute the tensor product $|\phi_1\rangle \otimes |\phi_2\rangle$.