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

Exam: „Mock Exam 12: Introduction to Cryptography“
Date and time: 2020/09/04 10:57
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	6		
Fields and Modular Arithmetics	32		
Hash Functions, Digital Signature and Cryptographic Protocols	18		
Public Key Cryptography	18		
Quantum Cryptography	6		
Sum	90		

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

Question 1: Basics [10 Points]

(a) [*4 Points*] Given E : key $\times$ message $\rightarrow$ code and D : code $\times$ message $\rightarrow$ key. Which equality is crucial for the correct behavior of a symmetric cipher?(1-6)

(b) [*6 Points*] What is the implication of $\mathcal{P} = \mathcal{NP}$ to cryptographic security? Give two examples with different outcome.

Question 2: DES & AES [6 Points]

(a) [*6 Points*] What is the reason that DES strips 8 bits of the 64 bit key? Evaluate its impact regarding a brute-force attack.

Question 3: Fields and Modular Arithmetics [32 Points]

(a) [*8 Points*] Name four properties necessary for a mathematical group and give the equations.

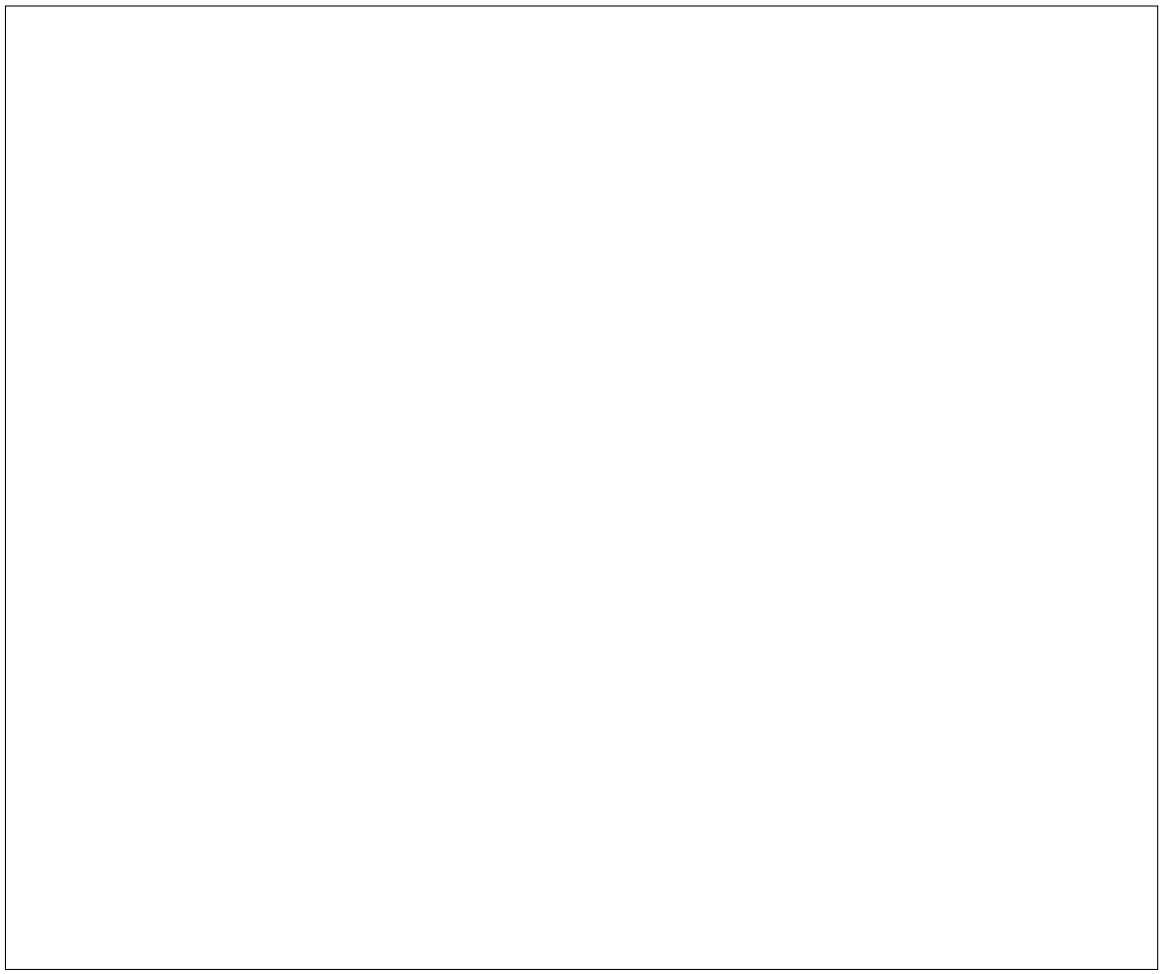
(b) [*6 Points*] Compute in multiplicative inverse of 1011 in $GF[2^4]$ using the irreducible polynnomial $x^4 + x + 1$.

(c) [*8 Points*] Compute $7^{-1} \bmod 31$ using the extended Euclidean algorithm.

(d) [*10 Points*] Describe 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 [18 Points]

(a) [*6 Points*] Name two problems with the RSA-based digital signature scheme.



(b) [*12 Points*] Give a zero-knowledge proof for showing that the prover knows the integer factorization of $n = pq$ for prime numbers p, q using the computation of square roots.

Question 5: Public Key Cryptography [18 Points]

(a) [*10 Points*] Given the prime factorization of $p-1$, give an efficient algorithm to find a generator/primitive root of $\mathbb{Z}_p^*$ (p is prime number).

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

Question 6: Quantum Cryptography [6 Points]

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

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

is a unitary matrix.