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

Exam: „Mock Exam 8: Introduction to Cryptography“
Date and time: 2020/09/03 13:54
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	15		
DES & AES	6		
Fields and Modular Arithmetics	11		
Hash Functions, Digital Signature and Cryptographic Protocols	20		
Public Key Cryptography	20		
Quantum Cryptography	18		
Sum	90		

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

Question 1: Basics [15 Points]

(a) [*6 Points*] What is the probability for two uniformly randomly strings $x_1, x_2 \in \{0,1\}^m$ that $x_1 = x_2$, i.e. Prob$[x_1 = x_2]$? Explain your solution.

(b) [*9 Points*] Classify Ceaser‘s code, Enigma, RSA, AES, Vernam ciphers and Quantum Cryptography regarding its degree of security into three groups.

Question 2: DES & AES [6 Points]

(a) [*6 Points*] Describe the F-Box of DES with a picture using the S-Boxes and all necessary other parts.

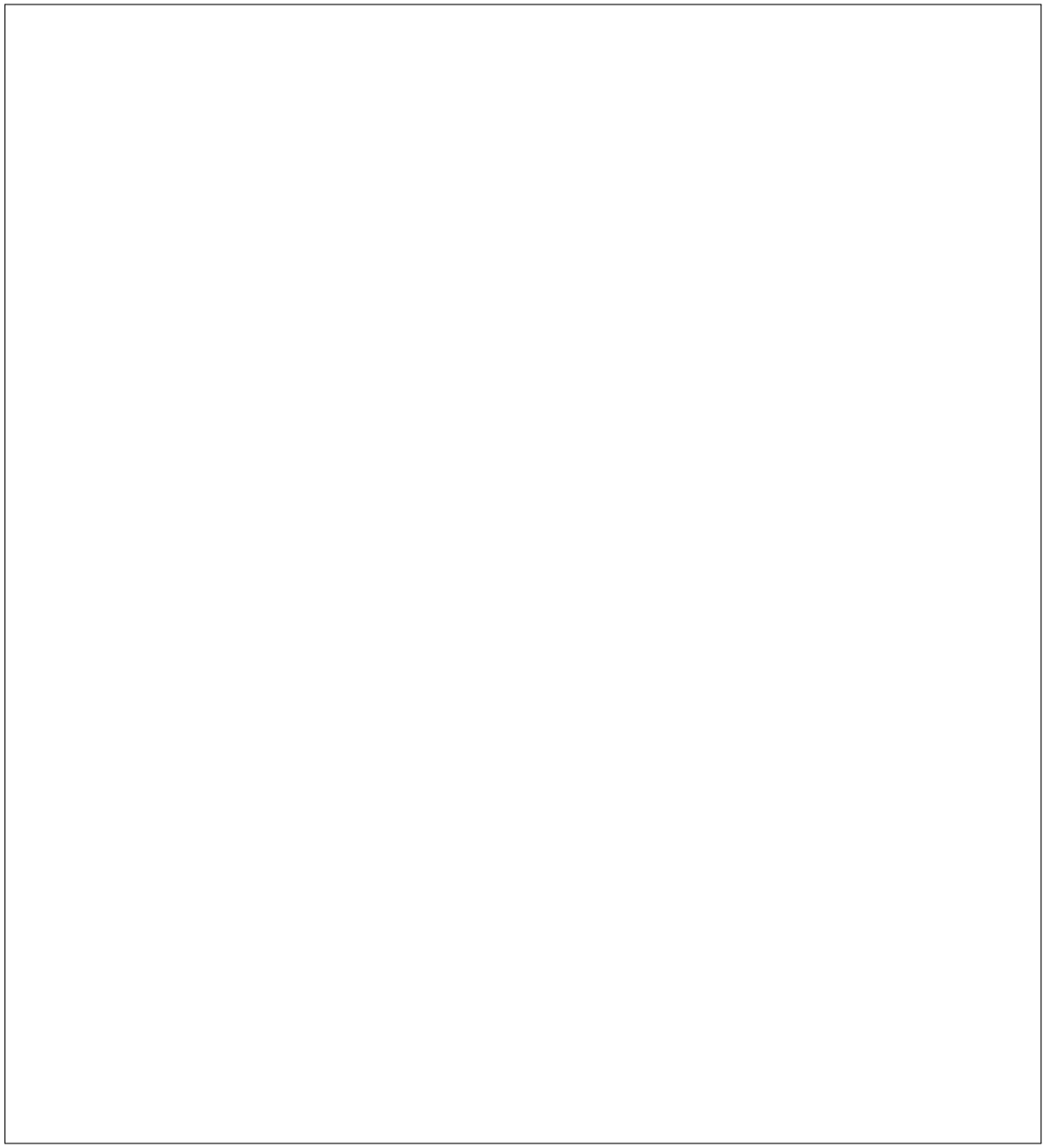
Question 3: Fields and Modular Arithmetics [11 Points]

(a) [*2 Points*] Is there a finite field with six elements? (Yes/No)

(b) [*9 Points*] Perform the extended Euclidean algorithm for 101010 and 111000.

Question 4: Crypto Hash Functions, Digital Signature and Crypto Protocols [20 Points]

(a) [*6 Points*] Describe the Merkle-Damgård-Construction for Cryptographic Hash functions with pseudo-code or a picture.



(b) [*4 Points*] What is the interaction of certification authority and certificates?

(c) [*10 Points*] Describe the Diffie-Hellman Key Exchange protocol based on elliptic curves.

Question 5: Public Key Cryptography [20 Points]

(a) [*6 Points*] Is 2 a generator (primitive root) for $\mathbb{Z}_5^*$? Prove your statement.

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

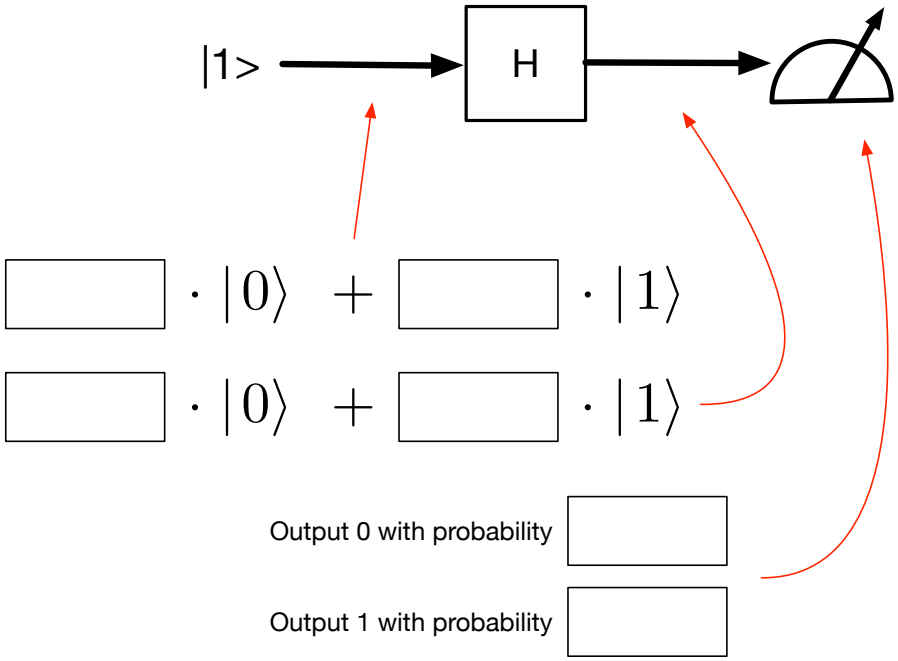
$$y^2 = x^3 - 3x$$

for $E(\mathbb{R})$. For the point $P = (0, 0)$ compute $3P$.

(c) [*4 Points*] State the elliptic curve discrete logarithm assumption.

Question 6: Quantum Cryptography [18 Points]

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



(b) [*6 Points*] What is the probability that an eavesdropper can successfully imitate a quantum bit in the Bennett and Brassard scheme?