Univ.-Prof. Dr. rer. nat. Rudolf Mathar

1	2	3	4	$\sum$
$\boxed{19}$	$\boxed{20}$	$\boxed{11}$	$\boxed{20}$	$\boxed{70}$

Written examination

Tuesday, August 18, 2015, 08:30 a.m.

Name: ____________________ Matr.-No.: ____________

Field of study: ____________________________

Please pay attention to the following:

1) The exam consists of **4 problems**. Please check the completeness of your copy. **Only** written solutions on these sheets will be considered. Removing the staples is **not** allowed.

2) The exam is passed with at least **35 points**.

3) You are free in choosing the order of working on the problems. Your solution shall clearly show the approach and intermediate arguments.

4) **Admitted materials:** The sheets handed out with the exam and a non-programmable calculator.

5) The results will be published on Monday, the 24.08.15, 16:00h, on the homepage of the institute.

The corrected exams can be inspected on Tuesday, 25.08.15, 10:00h. at the seminar room 333 of the Chair for Theoretical Information Technology, Kopernikusstr. 16.

Acknowledged: ________________________

(Signature)

Problem 1. (19 points)
The following ciphertext over the alphabet $\mathbb{Z}_{26}$ and total length $N = 35$ is given:

IAEGO LMCNL AITTC LIISL LFHIA ENTII KGNSG.

a) Calculate the index of coincidence for the given ciphertext. Decide whether the ciphertext was encrypted using a monoalphabetic or polyalphabetic cipher.

The previous ciphertext has been deciphered yielding the following plaintext:

LIKEALL MAGNIFI CENTTHI NGSITIS LOGICAL.

b) Can the resulting ciphertext be described by a permutation scheme of the given plaintext? Substantiate your claim.

The ciphertext is represented by blocks of length $v = 5$. The blocks are indexed by $j \in \{1, ..., b\}$ with $b = \frac{N}{v} = 7$. The symbol position inside a block is indexed by $i \in \{1, ..., v\}$. The secret keys are $k_1, k_2, ..., k_b \in \{1, ..., b\}$ and it holds $k_s \neq k_t$ for $s \neq t$. A ciphertext symbol is encrypted by $c_{(j-1)\cdot v+i} = m_{(i-1)\cdot b+k_j}$.

c) Determine the secret keys $k_1, k_2, ..., k_b$ for the given pair of plaintext and ciphertext.

A permutation cipher of block length l over an alphabet of size q can be broken by means of a chosen-plaintext attack. Let $q \leq l$.

d) Give a corresponding attack scheme for $l = 16$ and $q = 2$ to obtain the key π with at most 4 well-chosen messages of length l. Explain the key idea why your scheme is valid.

e) Give the minimal number of chosen messages for a valid generalized attack scheme as a function of $q, l \in \mathbb{N}$.

Suppose you encrypt a message $m \in \mathbb{Z}_q$ using an affine cipher $e_k(m)$ with key $k = (a, b) \in \mathbb{Z}_q^* \times \mathbb{Z}_q$.

f) Compute the n-fold encryption $c = e_{k_n}(...e_{k_2}(e_{k_1}(m))...)$ for different keys k_i with $i = 1, ..., n$.

g) Is there an advantage using n subsequent encryptions, rather than using a single affine cipher? Substantiate your claim.

Problem 2. (20 points)
We consider the Data Encryption Standard (DES) algorithm.

- **a)** Give the names of the four main operations used in a standard building block of DES.
- **b)** How can the same encryption algorithm of DES be used for decryption?

DES encrypts blocks of 64 bits using a key of 56 bits. For each 7 key bits, one (odd) parity bit for error detection is added. The key of a DES cipher is of the form:

$$K_0 = (k_1, \ldots, k_7, b_1, k_9, \ldots, k_{15}, b_2, k_{17}, \ldots, k_{57}, \ldots, k_{63}, b_8).$$

From this key K_0, 16 round keys $K_1, K_2, ..., K_{16}$ are generated. The 56 key bits of K_0 are divided into two blocks C_0 and D_0 of 28 bits each as described in the left table below.

1	2	3	4	5	6	7	b_1
9	10	11	12	13	14	15	b_2
17	18	19	20	21	22	23	b_3
25	26	27	28	29	30	31	b_4
33	34	35	36	37	38	39	b_5
41	42	43	44	45	46	47	b_6
49	50	51	52	53	54	55	b_7
57	58	59	60	61	62	63	b_8

$C_0 \uparrow$ $\qquad$ $\uparrow D_0$

PC2					
14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

C_0 is read column-wise from 57 to 36 and D_0 column-wise from 63 to 4.

In a second step, C_n and D_n for $n = 1, ..., 16$, are each generated from C_{n-1} and D_{n-1} by a cyclic left-shift of s_n positions, where s_n is defined by:

$$s_n = \begin{cases} 1, & \text{if } n \in \{1, 2, 9, 16\} \\ 2, & \text{otherwise} \end{cases}$$

From each of these (C_n, D_n), with $n = 1, ..., 16$, one now selects 48 key bits as in the above table PC2 on the right to obtain K_n.

In the following, a particular pair of keys for DES is considered[1]:

$$K_0 = (\texttt{01FE 01FE 01FE 01FE}), \quad \hat{K}_0 = (\texttt{FE01 FE01 FE01 FE01})$$

- **c)** Determine (C_0, D_0) and (C_1, D_1) from K_0, and $(\hat{C}_0, \hat{D}_0)$ and $(\hat{C}_1, \hat{D}_1)$ from $\hat{K}_0$.
- **d)** Which of the generated subkeys $K_1, K_2, ..., K_{16}$ are identical when K_0 is used?
- **e)** Show that $\mathrm{DES}_{\hat{K}_0}(\mathrm{DES}_{K_0}(M)) = M$ holds for all $M \in \mathcal{M}$.

[1]The keys are shown in hexadecimal representation.

Problem 3. (11 points)

Consider the following properties of the greatest common divisor for positive integers u and v:

(i) If u even and v even, then $\gcd(u,v) = 2\gcd(u/2, v/2)$.

(ii) If u even and v odd, then $\gcd(u,v) = \gcd(u/2, v)$.
If u odd and v even, then $\gcd(u,v) = \gcd(u, v/2)$.

(iii) If u odd and v odd and $u \geq v$, then $\gcd(u,v) = \gcd((u-v)/2, v)$.
If u odd and v odd and $u < v$, then $\gcd(u,v) = \gcd(u, (v-u)/2)$.

(iv) $\gcd(u,0) = u$ and $\gcd(0,v) = v$.

a) Show that (iii) is a true statement.

b) Compute $\gcd(114, 48)$ using only the given properties.

c) Write a recursive algorithm to determine $\gcd(u,v)$.

Hint: *For* **c)** *You may use the function:* $\text{IsEven}(x) = \begin{cases} \text{true}, & \text{if } x \text{ is even}, \\ \text{false}, & \text{otherwise.} \end{cases}$

Problem 4. (20 points)

We consider an RSA cryptosystem.

a) Why should neither $e = 1$ nor $e = 2$ be chosen for RSA with any modulus $n \in \mathbb{Z}$?

Let $(e, n) = (73, 105169)$ be the public key. The public parameters n and e are known and you have intercepted $\varphi(n) = 104500$.

b) Compute p and q for $p > q$ using $\varphi(n)$ and compute the private key d.

Let u and v be distinct odd primes, and let $n = u \cdot v$. Furthermore, suppose that an integer x satisfies $\gcd(x, u \cdot v) = 1$.

c) Show that $x^{\frac{1}{2}\varphi(n)} \equiv 1 \pmod{u}$ and $x^{\frac{1}{2}\varphi(n)} \equiv 1 \pmod{v}$.

d) Show that $x^{\frac{1}{2}\varphi(n)} \equiv 1 \pmod{n}$.

e) Show that if $ed \equiv 1 \pmod{\frac{1}{2}\varphi(n)}$ holds for two integers d and e, then we obtain $x^{ed} \equiv x \pmod{n}$.