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 $c_{(j-1)v+i} = m_{(i-1)b+k_j}$.

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 $\pi$ 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, 16 round keys \( K_1, K_2, \ldots, K_{16} \) 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.

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

\( C_0 \) 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 \( n = 1, \ldots, 16 \), 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 \( n = 1, \ldots, 16 \), 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:

\[ K_0 = (01FE \ 01FE \ 01FE \ 01FE), \quad \hat{K}_0 = (FE01 \ FE01 \ FE01 \ FE01) \]

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 \( K_1, K_2, \ldots, K_{16} \) are identical when \( K_0 \) is used?

e) Show that \( \text{DES}_{\hat{K}_0}(\text{DES}_{K_0}(M)) = M \) 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 \( x^{ed} \equiv x \pmod{n} \).