Solution for Written Examination
Advanced Methods of Cryptography

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

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.
Solution of Problem 1

(19 points)

a) The Index of Coincidence is calculated using a frequency analysis:  (1P)

<table>
<thead>
<tr>
<th>i</th>
<th>Character</th>
<th>$k_i$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>A</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>B</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>C</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>D</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>E</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>F</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>G</td>
<td>3</td>
</tr>
<tr>
<td>7</td>
<td>H</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>I</td>
<td>7</td>
</tr>
<tr>
<td>9</td>
<td>J</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>K</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>L</td>
<td>5</td>
</tr>
<tr>
<td>12</td>
<td>M</td>
<td>1</td>
</tr>
<tr>
<td>13</td>
<td>N</td>
<td>3</td>
</tr>
<tr>
<td>14</td>
<td>O</td>
<td>1</td>
</tr>
<tr>
<td>15</td>
<td>P</td>
<td>0</td>
</tr>
<tr>
<td>16</td>
<td>Q</td>
<td>0</td>
</tr>
<tr>
<td>17</td>
<td>R</td>
<td>0</td>
</tr>
<tr>
<td>18</td>
<td>S</td>
<td>2</td>
</tr>
<tr>
<td>19</td>
<td>T</td>
<td>3</td>
</tr>
<tr>
<td>20</td>
<td>U</td>
<td>0</td>
</tr>
<tr>
<td>21</td>
<td>V</td>
<td>0</td>
</tr>
<tr>
<td>22</td>
<td>W</td>
<td>0</td>
</tr>
<tr>
<td>23</td>
<td>X</td>
<td>0</td>
</tr>
<tr>
<td>24</td>
<td>Y</td>
<td>0</td>
</tr>
<tr>
<td>25</td>
<td>Z</td>
<td>0</td>
</tr>
</tbody>
</table>

The total number of characters in the ciphertext is $N = 35$. Therefore, the Index of Coincidence is calculated with the frequencies $k_i$ as:

$$I_c = \frac{\sum_{i=1}^{26} k_i(k_i - 1)}{n(n-1)} = \frac{7 \cdot 6 + 5 \cdot 4 + 4(3 \cdot 2) + 3(2 \cdot 1)}{35 \cdot 34} = \frac{92}{1190} \approx 0.0773$$  (2P)

It is known that for an English text: $K_E = 0.066895 \implies I_c \approx K_E$. The Friedman Test states that the ciphertext is monoalphabetic (and probably an English text).  (1P)

b) Since the frequencies of the letters in the plaintext and the ciphertext are the same, we can assume that a permutation cipher has been used.  (1P)

c) First apply the given encryption function to $c = (c_1, c_2, ..., c_{35})$, e.g.,

$$c_1 = c_{(1-1) \cdot 5+1} = m_{(1-1) \cdot 7+k_1}$$

$$c_2 = c_{(1-1) \cdot 5+2} = m_{(2-1) \cdot 7+k_1}$$

$$c_3 = c_{(1-1) \cdot 5+3} = m_{(3-1) \cdot 7+k_1}$$

$$\vdots$$

$$c_6 = c_{(2-1) \cdot 5+1} = m_{(1-1) \cdot 7+k_2}$$

$$c_7 = c_{(2-1) \cdot 5+2} = m_{(2-1) \cdot 7+k_2}$$

$$\vdots$$

$$c_{35} = c_{(7-1) \cdot 5+5} = m_{(5-1) \cdot 7+k_7}$$

Thus, the ciphertext symbols of the first block of $v = 5$ symbols are each multiples of $b = 7$ in the plaintext. Thus, the 5 symbols IAEGO have same offset $k_1$ per block of 7 symbols in the plaintext. The secret keys are the corresponding offsets: $k_1 = 2, k_2 = 1, k_3 = 5, k_4 = 7, k_5 = 6, k_6 = 4, k_7 = 3$.  (4P)
Alternative solution:
The permutation applied to the ciphertext yields the following matrix structure with
the permutation keys on the bottom:
\[
\begin{pmatrix}
L & I & K & E & A & L & L \\
M & A & G & N & I & F & I \\
C & E & N & T & T & H & I \\
N & G & S & I & T & I & S \\
L & O & G & I & C & A & L \\
\end{pmatrix}
\]
(2 1 5 7 6 4 3)

The ciphertext is read row-wise and the keys are the offsets from left (cf. above).

d) For an alphabet size of 2, i.e., \(\mathcal{A} = \{0, 1\}\), we use the following scheme:

\[
\begin{array}{cccccccc}
01 & 01 & 01 & 01 & 01 & 01 & 01 & 01 \\
00 & 11 & 00 & 11 & 00 & 11 & 00 & 11 \\
00 & 00 & 11 & 11 & 00 & 00 & 11 & 11 \\
00 & 00 & 00 & 00 & 11 & 11 & 11 & 11 \\
\end{array}
\]

With these chosen plaintexts, all bit positions are encoded by exactly one of the sixteen
unique codewords, namely, 0000, 1000, 1100, ..., 1111. (3P)

e) Minimal number of chosen messages is \(\lceil \log_q(l) \rceil\). (2P)

f) Applying the \(n\) encryption functions successively results in:

\[
\begin{align*}
c_1 & \equiv a_1 m + b_1 \mod q \\
c_2 & \equiv a_2 c_1 + b_2 \equiv a_2(a_1 m + b_1) + b_2 \\
& \equiv a_2 a_1 m + a_2 b_1 + b_2 \mod q \\
c_3 & \equiv a_3 c_2 + b_3 \\
& \equiv a_3(a_2 a_1 m + a_2 b_1 + b_2) + b_3 \\
& \equiv a_3 a_2 a_1 m + a_3 a_2 b_1 + a_3 b_2 + b_3 \mod q \\
& \vdots \\
c_n & \equiv \prod_{i=1}^{n} a_i m + \sum_{i=1}^{n-1} b_i \prod_{j=i+1}^{n} a_j + b_n \mod q \\
& \equiv \prod_{i=1}^{n} a_i m + \sum_{i=1}^{n} b_i \prod_{j=i+1}^{n} a_j \mod q \quad (3P)
\end{align*}
\]

using the definition of the empty product in the last step.

Note: A mathematical proof would involve the induction \( n \rightarrow n + 1:\)

\[
\begin{align*}
c_{n+1} & \equiv \prod_{i=1}^{n+1} a_i m + \sum_{i=1}^{n+1} b_i \prod_{j=i+1}^{n+1} a_j \\
& \equiv a_{n+1} \prod_{i=1}^{n} a_i m + a_{n+1} \sum_{i=1}^{n} b_i \prod_{j=i+1}^{n} a_j + b_{n+1} \\
& \equiv a_{n+1} c_n + b_{n+1} \quad \square
\end{align*}
\]

g) We obtain an effective key:

\[
k = (a = \prod_{i=1}^{n} a_i \mod q, b = \sum_{i=1}^{n-1} b_i \prod_{j=i+1}^{n} a_j + b_n \mod q)
\]

Therefore, successively encrypting with two different affine functions is the same as
encrypting with only one effective key \(k = (a, b)\). (2P)
Solution of Problem 2

(20 points)

a) Add round key $\oplus K_i$, Permutation $P$, S-box $S$, Expansion $E$  \hspace{1cm} (2P)

b) DES decryption is the same as DES encryption with keys applied in the reversed order. \hspace{1cm} (2P)

c) With $K_0 = (01FE \ 01FE \ 01FE \ 01FE)$, we obtain:

\[
\begin{array}{cccccccccccccccc}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & & & & & & & & & & & & & & \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & & & & & & & & & & & & & & \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & & & & & & & & & & & & & & \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & & & & & & & & & & & & & & \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & & & & & & & & & & & & & & \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & & & & & & & & & & & & & & \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & & & & & & & & & & & & & & \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & & & & & & & & & & & & & & \\
\end{array}
\]

Thus we read $(C_0, D_0)$ column-wise. $(C_1, D_1)$ are computed by a cyclic left-shift by 1 position:

\[
C_0 = (1010 1010 1010 1010 1010 1010 1010)_2 = (AAAAAAA)_16 \hspace{1cm} (1P)
\]
\[
D_0 = (1010 1010 1010 1010 1010 1010 1010)_2 = (AAAAAAA)_16 \hspace{1cm} (1P)
\]
\[
C_1 = (0101 0101 0101 0101 0101 0101 0101)_2 = (5555555)_16 \hspace{1cm} (1P)
\]
\[
D_1 = (0101 0101 0101 0101 0101 0101 0101)_2 = (5555555)_16 \hspace{1cm} (1P)
\]

For $\hat{K}_0 = (FE01 \ FE01 \ FE01 \ FE01)$, we obtain $(\hat{C}_0, \hat{D}_0)$ analogously. $(\hat{C}_1, \hat{D}_1)$ are computed by a cyclic left-shift by 1 position:

\[
\hat{C}_0 = (0101 0101 0101 0101 0101 0101 0101)_2 = (5555555)_16 \hspace{1cm} (1P)
\]
\[
\hat{D}_0 = (0101 0101 0101 0101 0101 0101 0101)_2 = (5555555)_16 \hspace{1cm} (1P)
\]
\[
\hat{C}_1 = (1010 1010 1010 1010 1010 1010 1010)_2 = (AAAAAAA)_16 \hspace{1cm} (1P)
\]
\[
\hat{D}_1 = (1010 1010 1010 1010 1010 1010 1010)_2 = (AAAAAAA)_16 \hspace{1cm} (1P)
\]

We have $C_0 = D_0 = \hat{C}_1 = \hat{D}_1$ and $C_1 = D_1 = \hat{C}_0 = \hat{D}_0$.

d) When $K_0$ is used, we obtain $(C_0, D_0)$ as in (a). The bits of $(C_{n-1}, D_{n-1})$ are cyclically left-shifted by $s_n$ positions to generate $(C_i, D_i)$ for $i = 1, \ldots, 16$. Due to the structure of $(C_0, D_0)$, cyclic right-shifts provide only two different keys: \hspace{1cm} (2P)
- An even number of positions provides the identical key.
- An odd number of positions provides the alternative key.

Thus from the definition of \( s_n \) for \( n = 1, \ldots, 16 \), we observe that:

\[
\begin{align*}
K_1 &= K_9 = K_{10} = K_{11} = K_{12} = K_{13} = K_{14} = K_{15}, \\
K_2 &= K_3 = K_4 = K_5 = K_6 = K_7 = K_8 = K_{16}
\end{align*}
\] (1P)

e) The key \( K_0 \) generates \((K_1 \ldots K_{16}) = K_1 K_2 K_2 K_2 K_2 K_1 K_1 K_1 K_1 K_1 K_2 \)
The key \( \hat{K}_0 \) generates \((\hat{K}_1 \ldots \hat{K}_{16}) = K_2 K_1 K_1 K_1 K_1 K_1 K_2 K_2 K_2 K_2 K_2 K_2 K_2 K_1 \)
(1P) (1P)

Since \( \hat{K}_0 \) has the reverse ordering of \( K_0 \), we obtain \( \text{DES}_{\hat{K}_0}(\text{DES}_{K_0}(M)) = M \). (2P)
Solution of Problem 3

(11 points)

a) From the Euclidean Algorithm it holds \( \gcd(u, v) = \gcd(u, u + qv) \) for all \( q \in \mathbb{Z} \). With \( q = -1 \), we obtain \( \gcd(u, v) = \gcd(u, u - v) \). (1P)

For two odd numbers \( 2 | (u - v) \), \( \gcd(u, v) = \gcd(u, u - v) \)

The proof for the other case is analogous. (1P)

b) \[
gcd(114, 48) \overset{(i)}{=} 2 \gcd(57, 24) \overset{(ii)}{=} 2 \gcd(57, 12) \overset{(ii)}{=} 2 \gcd(57, 6) \overset{(ii)}{=} 2 \gcd(57, 3) \\
\quad \overset{(iii)}{=} 2 \gcd(\lvert 57 - 3 \rvert / 2, 3) = 2 \gcd(27, 3) \overset{(iv)}{=} 2 \gcd(\lvert 27 - 3 \rvert / 2, 3) \\
= 2 \gcd(12, 3) \overset{(ii)}{=} 2 \gcd(6, 3) \overset{(ii)}{=} 2 \gcd(3, 3) \overset{(ii)}{=} 2 \gcd(0, 3) \overset{(iv)}{=} 2 \cdot 3 = 6 \] (3P)

c) (6P)
Algorithm 1 Recursive Computation of the Greatest Common Divisor

**input:** Two integers, $u$ and $v$

**output:** $\text{gcd}(u, v)$

1: **procedure** $\text{gcd}(u, v)$
2:     if $(u = v)$ then
3:         return $u$;
4:     end if
5:     if $(u \neq 0$ and $v = 0)$ then
6:         return $u$;
7:     end if
8:     if $(u = 0$ and $v \neq 0)$ then
9:         return $v$;
10:    end if
11:    if $(u \mod 2 = 0$ and $v \mod 2 = 0)$ then
12:        return $2 \text{gcd}(u/2, v/2)$;
13:    end if
14:    if $(u \mod 2 \neq 0$ and $v \mod 2 = 0)$ then
15:        return $\text{gcd}(u/2, v)$;
16:    end if
17:    if $(u \mod 2 = 0$ and $v \mod 2 \neq 0)$ then
18:        return $\text{gcd}(v/2, u)$;
19:    end if
20:    if $(u \mod 2 \neq 0$ and $v \mod 2 \neq 0)$ then
21:        if $(u > v)$ then
22:            return $\text{gcd}((u - v)/2, v)$;
23:        end if
24:        if $(u < v)$ then
25:            return $\text{gcd}((v - u)/2, v)$;
26:        end if
27:    end if
28: **end procedure**
Solution of Problem 4
(20 points)

a) \( e = 1 \): The ciphertext does not change since \( m^1 \equiv m \). There is no encryption. \( (1P) \)

\( e = 2 \): The requirement that \( \gcd(e, \varphi(n)) = 1 \) is not fulfilled, since \( \varphi(n) \) is always an even number so that \( 2 | \varphi(n) \). Hence, no inverse \( e^{-1} \mod \varphi(n) \equiv d \) exists. \( (1P) \)

b) \( d \equiv e^{-1} \mod \varphi(n) \) is computed by the Extended Euclidean Algorithm:

\[
104500 = 1431 \cdot 73 + 37 \\
73 = 37 \cdot 1 + 36 \\
37 = 36 \cdot 1 + 1 \quad (1P)
\]
\[
\Leftrightarrow 1 = 37 - 36 \cdot 1 \\
= 37 - (73 - 37) \\
= 37 \cdot 2 - 73 \\
= (104500 - 1431 \cdot 2 \cdot 73) - 73 \cdot 1 \\
= 104500 \cdot 2 - 2863 \cdot 73 \quad \checkmark \quad (1P)
\]

The private key is \( d = e^{-1} \equiv -2863 \equiv 101637 \). \( (1P) \)

With \( n = pq = 105169 \) and \( \varphi(n) = (p-1)(q-1) = 104500 \), we can compute the following equation:

\[
\varphi(n) = pq - p - q + 1 \\
= p \cdot n - p - \frac{n}{p} + 1 \\
= n - p - \frac{n}{p} + 1 \\
\Leftrightarrow 0 = n - p - \frac{n}{p} + 1 - \varphi(n) \\
0 = np - p^2 - n + p - \varphi(n)p \\
0 = p^2 + (\varphi(n) - 1 - n)p + n \quad (2P)
\]

From the solution of the \( p \)-\( q \)-formula for quadratic equations we obtain:

\[
p = 335 + \sqrt{335^2 - 105169} = 335 + \sqrt{7056} = 335 + 84 = 419, \quad (1P)
\]
\[
q = 335 - \sqrt{335^2 - 105169} = 335 - \sqrt{7056} = 335 - 84 = 251. \quad (1P)
\]

c) \( \varphi(n) = (u-1)(v-1) \), since \( u \) and \( v \) are distinct. \( (1P) \)
\[
x^{\varphi(n)/2} \equiv x^{(u-1)(v-1)/2} \equiv (x^{u-1})^{(v-1)/2} \equiv 1^{(v-1)/2} \equiv 1 \mod u. \quad (1P)
\]
Since \( v \) is an odd prime, it holds \( 2 | (v-1) \) so that \( (v-1)/2 \) is an integer. \( (1P) \)
(Remark: Note that \( (x^{1/2})^{\varphi(n)} \mod n \) is not defined!)

With analogous arguments, \( x^{\varphi(n)/2} \equiv 1 \mod v \) is computed. \( (1P) \)

d) Since, \( u \) and \( v \) are coprime \( (1P) \), we may apply the Chinese Remainder Theorem
(solution is \( r \equiv x^{\varphi(n)/2} \mod n \):)

\[
x^{\varphi(n)/2} \equiv 1 \pmod{u},
x^{\varphi(n)/2} \equiv 1 \pmod{v}, \quad (1P)
\]

\( M = pq, \)
\( M_1 = v, y_1 = v^{-1} \mod u, \)
\( M_2 = u, y_1 = u^{-1} \mod v \)
\[
r = (1 \cdot v \cdot (v^{-1} \mod u) + 1 \cdot u \cdot (u^{-1} \mod v)) \pmod{u \cdot v}
= (v(v^{-1} \mod u)) + u(u^{-1} \mod v) \pmod{u \cdot v} \quad (1P)
= 1, \quad \text{from definition of } \gcd(u,v) = 1 \quad (1P)
\]

Note that since \( \gcd(u,v) = 1 \) holds, it follows from the Extended Euclidean Algorithm, that \( ux + vy = \gcd(u,v) = 1 \). The unique solutions for \( x \) and \( y \) are \( x \equiv u^{-1} \mod v \) and \( y \equiv v^{-1} \mod u \). (cf. lecture section ”The Extended Euclidean Algorithm”)

**e)** If \( ed \equiv 1 \pmod{\frac{1}{2} \varphi(n)} \) it follows that:

\[
ed = 1 + \frac{1}{2} \varphi(n)k, \quad k \in \mathbb{Z},
\]
\[
\iff x^{ed} \equiv x^{1 + \frac{1}{2} \varphi(n)k} \quad (1P)
\]
\[
\equiv x^{(x^{\frac{1}{2} \varphi(n)})^k} \quad (1P)
\]
\[
\equiv x \cdot 1^k \equiv x \pmod{n} \quad (1P)
\]