Universität Karlsruhe (TH)
Lehrstuhl Informatik für Ingenieure und Naturwissenschaftler
Dr. Thomas Worsch
Matthias Schulz

14. Juli 2008

Einführung in die Informatik

Lösungen zu Übungsblatt 12

– Kryptographie –

Aufgabe 1:

a) Die einfachste Möglichkeit wäre, alle 26 Möglichkeiten für die Caesar-Chiffre durchzuprobieren und nachzuschauen, für welche Verschiebungszahl sich ein sinnvolles Wort ergibt.

Die Ergebnisse sind:

NSKTWRFYNP
OTLUXSGZOQ
PUMVYTHAPR
QVNWZUIBQS
RWOXAVJCRT
SXPYBWKDSU
TYQZCXLETV
UZRADYMFUW
VASBEZNGVX
WBTCFAOHWY
XCUDGBPIXZ
YDVEHCQJYA
ZEWFIDRKZB
AFXGJESLAC
BGYHKFTMBD
CHZILGUNCE
DIAJMHVODF
EJBKNIWPEG
FKCLOJXQFH
GLDMPKYRGI
HMENQLZSHJ
INFORMATIK
JOGPSNBUJL
KPHQTOCVKM

LQIRUPDWLN
MRJSVQEXMO

Das einzige sinnvolle Wort ist INFORMATIK, das sich bei einer Verschiebung um 21 nach rechts beziehungsweise 5 nach links ergibt. Das bedeutet, dass die Verschlüsselung darin besteht, jeden Buchstaben um 5 nach rechts zu verschieben (da die *Ent*schlüsselung darin bestand, jeden Buchstaben um 5 nach links zu verschieben).

Beim Ausprobieren der Verschiebungen kann man die meisten Möglichkeiten bereits nach den ersten beiden Buchstaben ausschließen, weil kein Wort beispielsweise mit LQ oder XC anfängt.

Das Wort ELEKTROTECHNIK wird zu JQJPYWTYJHMSNP verschlüsselt.

b) Wenn das Wort UELQLQ als Ergebnis des Hill-Verfahrens herauskommen würde, würden die Buchstabenpaare NT und AX auf das gleiche Buchstabenpaar LQ abgebildet, was der Umkehrbarkeit der Chiffrierung widerspricht.

Betrachten wir die vorkommenden Buchstabenpaare als Zahlen modulo 26:

$$\text{UE} \to \begin{pmatrix} 20 \\ 4 \end{pmatrix} = \begin{pmatrix} -6 \\ 4 \end{pmatrix}$$
$$\text{DY} \to \begin{pmatrix} 3 \\ 24 \end{pmatrix} = \begin{pmatrix} 3 \\ -2 \end{pmatrix}$$
$$\text{OF} \to \begin{pmatrix} 14 \\ 5 \end{pmatrix}$$
$$\text{LQ} \to \begin{pmatrix} 11 \\ 16 \end{pmatrix}$$

Es gilt nun $\begin{pmatrix} -6 \\ 4 \end{pmatrix} = -2 \begin{pmatrix} 3 \\ -2 \end{pmatrix}$.

Angenommen, NT wird auf DY abgebildet. Dies bedeutet, dass

$$M \cdot \begin{pmatrix} 13 \\ 19 \end{pmatrix} = \begin{pmatrix} 3 \\ -2 \end{pmatrix}$$

und damit auch

$$M \cdot \begin{pmatrix} -26 \\ -38 \end{pmatrix} = M \cdot \begin{pmatrix} 0 \\ 14 \end{pmatrix} = \begin{pmatrix} -6 \\ 4 \end{pmatrix}$$

gilt.

Damit würden die Buchstabenpaare SY und AO beide auf das Buchstabenpaar UE abgebildet, was der Umkehrbarkeit der Chiffrierung widerspricht.

Somit muss die Chiffre UELQOF lauten.

Die Matrix M habe die Einträge $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Weil AX auf OF abgebildet wird, gilt

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 23 \end{pmatrix} = \begin{pmatrix} 14 \\ 5 \end{pmatrix},$$

woraus direkt folgt:

$23b = 14 \Rightarrow 17 \cdot 23b = 17 \cdot 14 \Rightarrow 391b = 238 \Rightarrow b = 4$

und

$23d = 5 \Rightarrow 17 \cdot 23d = 17 \cdot 5 \Rightarrow 391d = 85 \Rightarrow d = 7.$

(17 als Inverses zu 23 berechnet man beispielweise mit dem erweiterten Euklidschen Algorithmus oder durch Ausprobieren.)

Weil SY auf UE abgebildet wird, gilt

$$\begin{pmatrix} a & 4 \\ c & 7 \end{pmatrix} \cdot \begin{pmatrix} 18 \\ 24 \end{pmatrix} = \begin{pmatrix} 20 \\ 4 \end{pmatrix},$$

woraus folgt:

$18a + 96 = 20 \Rightarrow 18a + 18 = 20 \Rightarrow 18a = 2$

und

$18c + 168 = 4 \Rightarrow 18c + 12 = 4 \Rightarrow 18c = -8 \Rightarrow 18c = 18.$

Leider ist es **nicht** möglich, auf beiden Seiten durch 2 zu teilen, da 2 nicht teilerfremd zu 26 ist. Stattdessen können wir jeweils die Gleichungen mit 3 multiplizieren, und erhalten

$54a = 6 \Rightarrow 2a = 6 \Rightarrow a \in \{3, 16\}$ und
$54c = 54 \Rightarrow 2c = 2 \Rightarrow c \in \{1, 14\}.$

Weil NT auf LQ abgebildet wird, gilt

$$\begin{pmatrix} a & 4 \\ c & 7 \end{pmatrix} \cdot \begin{pmatrix} 13 \\ 19 \end{pmatrix} = \begin{pmatrix} 11 \\ 16 \end{pmatrix},$$

woraus folgt:

$13a + 76 = 11 \Rightarrow 13a - 2 = 11 \Rightarrow 13a = 13$

und

$13c + 133 = 16 \Rightarrow 13c + 3 = 16 \Rightarrow 13c = 13.$

Wäre a oder c gerade, so wäre $13a$ oder $13c$ durch 26 teilbar und somit gleich 0 modulo 26. Da dies ausgeschlossen ist, folgt, dass a und c ungerade sind.

Damit ist $a = 16$ und $c = 14$ ausgeschlossen, so dass sich die Matrix

$$M = \begin{pmatrix} 3 & 4 \\ 1 & 7 \end{pmatrix}$$

ergibt.

c) Wir gehen davon aus, dass k durch n teilbar ist, damit die Verschlüsselung problemlos verläuft. Wenn $k = n^2$ gilt, haben wir n Blöcke der Länge n, die kodiert werden.

Die entsprechenden Vektoren heißen $v_1, \ldots, v_n$, die auf die Vektoren $c_1, \ldots, c_n$ abgebildet werden.

Es gilt

$M \cdot (v_1 \ldots v_n) = (c_1 \ldots c_n)$

Wenn die Matrix $(v_1 \ldots v_n)$ invertierbar ist, lässt sich M berechnen durch

$M = (c_1 \ldots c_n) \cdot (v_1 \ldots v_n)^{-1}$.

n^2 Zeichen reichen somit unter Umständen aus.

$n^2 - n$ Zeichen reichen jedoch nicht aus:

$n-1$ Gleichungen der Art $M \cdot v = c$ liefern uns $n(n-1)$ lineare Gleichungen, während wir n^2 Unbekannte Einträge der Matrix haben. Daher kann die Matrix nicht eindeutig bestimmt werden.

Aufgabe 2:

a) Nach Definition gilt:

$g(13, 8, 3, 4, 2, 1, 1) = g(8, 13-8 = 5, 2, 1, 3-2 = 1, 4-1 = 3, 1) = g(5, 3, 1, 3, 1, -2, 1)$
$= g(3, 2, 1, -2, 0, 5, 1) = g(2, 1, 0, 5, 1, -7, 2) = g(1, 0, 1, -7, -2, 19, 0) = (1, 1, -7)$

b) Es gilt: $(s_1 - qs_2)a + (t_1 - qt_2)b = s_1a - q_s2a + t_1b - qt_2b = s_1a + t_1b - q(s_2a + t_2b) = n - qm$ nach Voraussetzung.

c) Beginnend mit $(n, m, 1, 0, 0, 1, f(n, m)) = (n_1, m_1, s_{1,1}, t_{1,1}, s_{2,1}, t_{2,1}, q_1)$ erhalten wir bei der Berechnung von $g(n_1, m_1, s_{1,1}, t_{1,1}, s_{2,1}, t_{2,1}, q_1)$ nacheinander die 7-Tupel

$(n_2, m_2, s_{1,2}, t_{1,2}, s_{2,2}, t_{2,2}, q_2), \ldots, (n_k, m_k, s_{1,k}, t_{1,k}, s_{2,k}, t_{2,k}, q_k)$ für ein $k \geq 0$, so dass $m_k = 0$ gilt.

Wir beweisen per Induktion, dass für alle $0 \leq i \leq k$ gilt $s_{1,i}n + t_{1,i}m = n_i \wedge s_{2,i}n + t_{2,i}m = m_i$:

Die Behauptung gilt offensichtlich für $i = 0$.

Es gilt: $s_{1,i+1} = s_{2,i}, t_{1,i+1} = t_{2,i}, s_{2,i+1} = s_{1,i} - q_i s_{2,i}, t_{2,i+1} = t_{1,i} - q_i t_{2,i}$ und damit

$s_{1,i+1}n + t_{1,i+1}m = s_{2,i}n + t_{2,i}m = m_i = n_{i+1}$, nach Definition und Induktionshypothese;

$s_{2,i+1}n + t_{2,i+1}m = (s_{1,i} - qs_{2,i})n + (t_{1,i} - qt_{2,i})m$
$= n_i - qm_i = m_{i+1}$, nach Induktionsvoraussetzung, Teilaufgabe b) und Definition.

Nach Voraussetzung gilt am Ende $n_k = d, s_{1,k} = s, t_{1,k} = t$ und es folgt $sn + tm = d$.

Als nächstes zeigen wir, dass der größte gemeinsame Teiler g von n und m für jedes $0 \leq i \leq k$ auch der größte gemeinsame Teiler von n_i und m_i ist.

Diese Aussage ist offensichtlich wahr für $i = 0$.

Es gilt nun: $n_{i+1} = m_i$, also teilt g auch n_{i+1}, da g nach Induktionsvoraussetzung m_i teilt. Weiterhin gilt $m_{i+1} = n_i - q_i m_i$, und da g nach Induktionsvoraussetzung sowohl n_i als auch m_i teilt, muss g auch m_{i+1} teilen.

g ist also gemeinsamer Teiler von n_{i+1} und m_{i+1}. Angenommen, $g' > g$ wäre der größte gemeinsame Teiler von $n_{i+1} = m_i$ und $m_{i+1} = n_i - q_i m_i$.

Dann würde g' auch $m_{i+1} + q_i n_{i+1} = n_i - q_i m_i + q_i m_i = n_i$ teilen, und wäre somit ein gemeinsamer Teiler von n_i und m_i. Dies ist ein Widerspruch dazu, dass g der größte gemeinsame Teiler von n_i und m_i ist.

Somit ist g der größte gemeinsame teiler von n_i und m_i für $0 \leq i \leq k$.

Damit ist g auch der größte gemeinsame Teiler von d und 0, was bedeutet, dass $d = g$ gelten muss.

Damit ist die Behauptung gezeigt.

Hinweis: Eigentlich müsste man noch zeigen, dass die Berechnung immer terminiert, das heißt, dass imer ein 7-Tupel $(n_k, m_k, s_{1,k}, s_{2,k}, t_{1,k}, t_{2,k}, q_k)$ erreicht wird, so dass $m_k = 0$ gilt. Das war in der Aufgabe aber nicht gefordert: Es wurde nur gefordert, die partielle Korrektheit zu zeigen, nicht, auch die totale Korrektheit zu beweisen.

Aufgabe 3:

a) Für den privaten Schlüssel (n, d) gilt $n = 1927$ und $263 \cdot d = 1 \mod \Phi(n)$.

$\Phi(1927) = \Phi(41 \cdot 47) = 40 \cdot 46 = 1840$.

Wir führen nun (in irgend einer Form) den Erweiterten Euklidschen Algorithmus für 263 und 1840 aus.

Beispielsweise wie folgt:

$1840 = 6 \cdot 263 + \mathbf{262}$
$263 = 1 \cdot \mathbf{262} + 1$
$\mathbf{262} = 262 \cdot 1 + 0$

Daraus folgt durch Einsetzen:

$1 = 263 - 1 \cdot 262 = 263 - 1 \cdot (1840 - 6 \cdot 263) = 263(1 + 6) - 1840 = 263 \cdot 7 - 1840$.

Wir erhalten $7 \cdot 263 = 1 \mod 1840$.

Andere Möglichkeit: $g(1840, 263, 1, 0, 0, 1, 6)$ berechnen wie in Aufgabe 2:

$g(1840, 263, 1, 0, 0, 1, 6) = g(263, 262, 0, 1, 1, -6, 1) = g(262, 1, 1, -6, -1, 7, 262) = g(1, 0, -1, 7, 263, -1840, 0) = (1, -1, 7)$.

Daraus ergibt sich $-1 \cdot 1840 + 7 \cdot 263 = 1$ und damit $7 \cdot 263 = 1 \mod 1840$.

Der private Schlüssel ist somit $(1927, 7)$.

b) Zunächst zerlegen wir das Wort in Blöcke der Länge 4, da n vierstellig ist, und erhalten die Zahlen 1183, 740 und 559.

Wir müssen nun die Werte $1183^7 \mod 1927, 740^7 \mod 1927$ und $559^7 \mod 1927$ berechnen.

$1183^2 = 1399489 = 487 \mod 1927$
$1183^3 = 487 \cdot 1183 = 576121 = 1875 \mod 1927$
$1183^4 = 1875 \cdot 1183 = 2218125 = 148 \mod 1927$
$1183^5 = 148 \cdot 1183 = 175084 = 1654 \mod 1927$
$1183^6 = 1654 \cdot 1183 = 1956682 = 777 \mod 1927$
$1183^7 = 777 \cdot 1183 = 919191 = 12 \mod 1927$

$740^2 = 547600 = 332 \mod 1927$
$740^3 = 332 \cdot 740 = 245680 = 951 \mod 1927$
$740^4 = 951 \cdot 740 = 703740 = 385 \mod 1927$
$740^5 = 385 \cdot 740 = 284900 = 1631 \mod 1927$
$740^6 = 1631 \cdot 740 = 1206940 = 638 \mod 1927$
$740^7 = 638 \cdot 740 = 472120 = 5 \mod 1927$

$559^2 = 312481 = 307 \mod 1927$
$559^3 = 307 \cdot 559 = 171613 = 110 \mod 1927$
$559^4 = 110 \cdot 559 = 61490 = 1753 \mod 1927$
$559^5 = 1753 \cdot 559 = 979927 = 1011 \mod 1927$
$559^6 = 1011 \cdot 559 = 565149 = 538 \mod 1927$
$559^7 = 538 \cdot 559 = 300742 = 130 \mod 1927$

Alle Ergebnisse werden auf die gleiche Länge 3 gebracht, da bei vierstelligem n Blöcke der Länge $4 - 1 = 3$ verschlüsselt werden.

Es ergibt sich die Codierung

012 005 130

Wir fassen jeweils zwei benachbarte Ziffern zusammen, um daraus die Buchstaben herauszulesen, und erhalten

01 20 05 13 0,

Wobei die 0 am Ende übrig bleibt und keine weitere Bedeutung besitzt.

Es wurde somit das Wort ATEM verschlüsselt.

c) Das Wort LUFT wird codiert zu 12 21 06 20. Da n zweistellig ist, muss jede Ziffer einzeln chiffriert werden.

$0^5 = 0 \mod 91$
$1^5 = 1 \mod 91$

$2^5 = 32 \mod 91$
$6^5 = 6^3 \cdot 6^2 = 216 \cdot 36 = 34 \cdot 36 \mod 95 = 1224 \mod 95 = 41 \mod 95$
Wir bringen alle Zahlen auf die gleiche Längen und erhalten das Wort

0132320100413200