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

9. Juli 2008

Einführung in die Informatik

Übungsblatt 12

– Kryptographie –

Aufgabe 1:

a) Ein Wort wurde mit Hilfe der Caesar-Chiffre verschlüsselt. Das verschlüsselte Wort ist NSKTWRFYNP. Wie lautet das Originalwort? Verschlüsseln Sie mit der gleichen Chiffre das Wort ELEKTROTECHNIK.

b) Mit dem Hill-Verfahren wurde das Wort SYNTAX entweder zum Wort UEDYOF oder UELQOF oder UELQLQ verschlüsselt. Es wurde eine 2 ×2-Matrix verwendet, und jeder Buchstabe wurde durch die Anzahl der Buchstaben im Alphabet vor diesem Buchstaben verschlüsselt. (Also A durch 0, B durch 1, ...).

Stellen Sie fest, welches Wort als einziges als Chiffre in Frage kommt, wenn die Verschlüsselungsmatrix vernünftig ist. Berechnen Sie die Matrix M, mit der verschlüsselt wurde.

c) Ein Wort mit k Buchstaben wurde mit Hilfe einer $n \times n$ Matrix M im Hill-Verfahren verschlüsselt. Sie haben sowohl das Originalwort als auch die Chiffre abfangen können.

Wie groß muss k mindestens sein, damit Sie die Verschlüsselungsmatrix M berechnen können?

Aufgabe 2: Sei $f(p,q)$ definiert durch $f(p,q) = \begin{cases} \lfloor \frac{p}{q} \rfloor & \text{falls } q \neq 0 \\ 0 & \text{sonst} \end{cases}$

Die Funktion $g(n, m, s_1, t_1, s_2, t_2, q)$ sei wie folgt rekursiv definiert:
$g(n, 0, s_1, t_1, s_2, t_2, q) = (n, s_1, t_1)$,
$g(n, m, s_1, t_1, s_2, t_2, q) = g(m, n - qm, s_2, t_2, s_1 - qs_2, t_1 - qt_2, f(m, n - qm))$ falls $m > 0$.

a) Berechnen Sie $g(13, 8, 3, 4, 2, 1, 1)$.

b) Zeigen Sie: Wenn für zwei Zahlen a, b gilt: $s_1 a + t_1 b = n, s_2 a + t_2 b = m$, so folgt $(s_1 - qs_2)a + (t_1 - qt_2)b = n - qm$.

c) Zeigen Sie: Wenn $g(n, m, 1, 0, 0, 1, f(n, m)) = (d, s, t)$ gilt, so gilt: d ist der größte gemeinsame Teiler von n und m und $sn + tm = d$.

Aufgabe 3: Für das RSA-Verfahren sei der öffentliche Schlüssel $(1927, 263)$ gegeben. A werde durch 1 codiert, B durch 2 und so weiter.

a) Berechnen Sie den privaten Schlüssel (n, d). (**Hinweis**: $n = 41 \cdot 47$)

b) Nach Verschlüsseln eines Wortes erhält man die Chiffre 118307400559. Wie lautet das verschlüsselte Wort?

c) Verschlüsseln Sie das Wort LUFT mit dem Schlüssel $(91, 5)$.

Abgabe bis zum **16. Juli 2008** in der Vorlesung oder im Tutorium.
Falls Sie eine Bearbeitung abgeben möchten, geben Sie bitte den Namen Ihres Tutors und Ihre Übungsgruppe an.