Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik
FH Zentralschweiz

Einführung in die Zahlentheorie 3 - Übung

Prof. Dr. Josef F. Bürgler

I.BA_DMATH, Semesterwoche 11

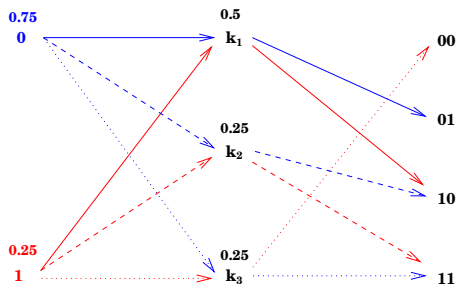
Die Aufgaben sind zusammen mit dem Lösungweg in möglichst einfacher Form darzustellen. Numerische Resultate sind mit einer Genauigkeit von 4 Stellen anzugeben. Skizzen müssen qualitativ und quantitativ richtig sein.

Sie sollten im Durschnitt 75% der Aufgaben bearbeiten. Die mit grossen römischen Zahlen gekennzeichneten Aufgaben **müssen** bearbeitet werden und die Lösungen dieser Aufgaben werden kontolliert und bewertet. Abgabetermin ihrer Übungsaufgaben ist die letzte Vorlesungsstunde in der Woche nachdem das Thema im Unterricht besprochen wurde.

Referenz: *Kenneth H. Rosen, Discrete Mathematics and its Applications, McGraw-Hill International Edition, 6. Auflage,* ***kurz: KR***

I. Gegeben sei die Klartextmenge $\mathscr{M} = \{0,1\}$, die Geheimtextmenge $\mathscr{C} = \{00,01,10,11\}$ und die Schlüsselmenge $\mathscr{K} = \{k_1,k_2,k_3\}$, sowie die Wahrscheinlichkeitsverteilungen auf der Klartextmenge $p(0) = 3/4$, $p(1) = 1/4$ und auf der Schlüsselmenge $p(k_1) = 1/2$, $p(k_2) = 1/4$ und $p(k_3) = 1/4$. Die Verschlüsselungsfunktion f sei wie folgt definiert:

$$\begin{aligned} f(k_1,0) &= 01 & f(k_1,1) &= 10 \\ f(k_2,0) &= 10 & f(k_2,1) &= 11 \\ f(k_3,0) &= 11 & f(k_3,1) &= 00 \end{aligned}$$



Untersuchen Sie das System auf perfekte Sicherheit.

II. Es seien die folgenden drei Primzahlen $p = 47$, $q = 59$ und $e = 17$ gegeben.

a) Prüfen Sie zunächst, dass $\phi(pq)$ und e teilerfremd sind.

b) Bestimmen Sie per Hand das modulare Inverse d von e modulo $\phi(pq)$. Kontrollieren Sie mit Maple.

c) Verschlüsseln Sie die Nachrichten $8, 117$ und 1212.

d) Entschlüsseln Sie die (kodierten) Nachrichten 596, 1769 und 2345.

1. Die Zahl $n = 10'921$ ist das Produkt von zwei verschiedenen Primzahlen. Ausserdem gilt $\phi(10'921) = 10'692$. Faktorisieren Sie n. Als Hilfsmittel sind dazu nur ein (einfacher) Taschenrechner und eine Formelsammlung erlaubt.

III. Die Zahl $n = 17'753$ ist das Produkt von zwei verschiedenen Primzahlen. Ausserdem gilt $\phi(17'753) = 17'280$. Faktorisieren Sie n. Als Hilfsmittel sind dazu nur ein (einfacher) Taschenrechner und eine Formelsammlung erlaubt.

2. **KR, Abschnitt 3.7, Aufgabe *61:** Begründen Sie kurz, warum man bei der Implementierung des RSA für das Modul n keine Primzahl wählen sollte.

Lösungen

I. -

II. -

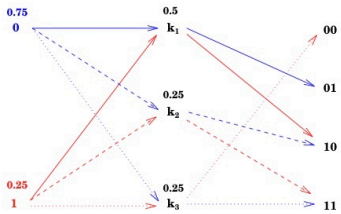
1. Hinweis: Zu lösen ist das Gleichungssystem $p \cdot q = 10'921$ und $(p-1) \cdot (q-1) = 10'692$. Wie kommt man auf diese beiden Gleichungen?

III. -

2. -

I. Gegeben sei die Klartextmenge $\mathscr{M} = \{0,1\}$, die Geheimtextmenge $\mathscr{C} = \{00,01,10,11\}$ und die Schlüsselmenge $\mathscr{K} = \{k_1,k_2,k_3\}$, sowie die Wahrscheinlichkeitsverteilungen auf der Klartextmenge $p(0) = 3/4$, $p(1) = 1/4$ und auf der Schlüsselmenge $p(k_1) = 1/2$, $p(k_2) = 1/4$ und $p(k_3) = 1/4$. Die Verschlüsselungsfunktion f sei wie folgt definiert:

$$\begin{aligned} f(k_1,0) &= 01 & f(k_1,1) &= 10 \\ f(k_2,0) &= 10 & f(k_2,1) &= 11 \\ f(k_3,0) &= 11 & f(k_3,1) &= 00 \end{aligned}$$



Untersuchen Sie das System auf perfekte Sicherheit.

I. $p(0) = 3/4$ | $p(k_1) = 1/2$ $\quad p(k_3) = 1/4$

$p(1) = 1/4$ | $p(k_2) = 1/4$

$p(00) = f(k_3,1) = 1/4 \cdot 1/4 = 1/16$

$p(01) = f(k_1,0) = 1/2 \cdot 3/4 = 3/8$

$p(10) = f(k_1,1) + f(k_2,0) = 1/2 \cdot 1/4 + 1/4 \cdot 3/4 = 1/8 + 3/16 = 5/16$

$p(11) = f(k_3,0) + f(k_2,1) = 1/4 \cdot 3/4 + 1/4 \cdot 1/4 = 3/16 + 1/16 = 1/4$

$$p(0 \mid 00) = \frac{p(0010) \cdot p(0)}{p(00)} = 0 \neq p(0) = \frac{3}{4}$$

→ heisst, dass keine perfekte Sicherheit herrscht

II. Es seien die folgenden drei Primzahlen $p = 47$, $q = 59$ und $e = 17$ gegeben.

a) Prüfen Sie zunächst, dass $\phi(pq)$ und e teilerfremd sind.

b) Bestimmen Sie per Hand das modulare Inverse d von e modulo $\phi(pq)$. Kontrollieren Sie mit Maple.

c) Verschlüsseln Sie die Nachrichten 8, 117 und 1212.

d) Entschlüsseln Sie die (kodierten) Nachrichten 596, 1769 und 2345.

II. a) $\phi(pq) = (47-1)(59-1) = 2668$

$2668 = 156 \cdot 17 + 16$

$17 = 1 \cdot 16 + 1$ → $ggT(2668, 17) = 1$ ⇒ teilerfremd

$16 = 1 \cdot 16 + 0$

b) $d \cdot e \bmod \phi(pq) = 1$

→ $d \cdot e + x \cdot \phi(pq) = 1$ → Diophantischer Gleichung

$1 = 17 - 16$

$1 \overset{!}{=} 17 - (2668 - 156 \cdot 17)$

$1 \overset{!}{=} 17 - 2668 + 156 \cdot 17$

$1 \overset{!}{=} 157 \cdot 17 - 1 \cdot 2668$

→ $d = 157$, $x = (-1)$

c) $f_e(m) = m^e \bmod n = c$ → Verschlüsseln

$f_d(c) = c^d \bmod n = m$ → Entschlüsseln

$8^{17} \bmod 2773 = 596$

$117^{17} \bmod 2773 = 1769$

$1212^{17} \bmod 2773 = 2345$

$e = 17$

$n = 2773$

d) $596^{157} \mod 2773 = 8$

$1769^{157} \mod 2773 = 117$

$2345^{157} \mod 2773 = 1212$

$d = 157$

$n = 2773$

III. Die Zahl $n = 17'753$ ist das Produkt von zwei verschiedenen Primzahlen. Ausserdem gilt $\phi(17'753) = 17'280$. Faktorisieren Sie n. Als Hilfsmittel sind dazu nur ein (einfacher) Taschenrechner und eine Formelsammlung erlaubt.

III.

$n = p \cdot q = 17'753$

$p = \frac{17'753}{q}$

$\phi(17'753) = (p-1)(q-1) = 17'280$

$(p-1)(q-1) = 17'280$

$pq - p - q + 1 = 17'280$

$\frac{17'753}{q} \cdot q - \frac{17'753}{q} - q + 1 = 17'280 \quad / -1$

$\frac{17'753q}{q} - \frac{17'753}{q} - \frac{q^2}{q} = 17'279$

$\frac{17'753q - 17'753 - q^2}{q} = 17'279 \quad / \cdot q$

$-q^2 + 17'753q - 17'753 = 17'279q \quad / -17'279q$

$-q^2 + 474q - 17'753 = 0$

$\frac{-474 \pm \sqrt{474^2 - (-1)(-17'753) \cdot 4}}{2 \cdot (-1)} = \begin{matrix} q_1 = 41 \\ q_2 = 433 \end{matrix}$

$p_1 = \frac{17'753}{41} = 433$

$p_2 = \frac{17'753}{433} = 41$

→ $p_1 = 433 \; ; \; q_1 = 41$

→ $p_2 = 41 \; ; \; q_2 = 433$