Vorlesung „Kryptographie I“ (Wintersemester 2024/2025)

Übungsblatt 4 (8.11.2024)

Bemerkungen:

(1) Zur Lösung einer Kryptographie-Aufgabe gehört auch eine (kurze) Darstellung des Lösungswegs.
(2) Mit **P** werden Präsenzaufgaben, mit **H** Hausaufgaben bezeichnet.
(3) Abgabe der Hausaufgaben bis Freitag, 15.11.2024 in den Übungskästen (bis 10:00 Uhr), in Übungsgruppe 1 oder digital (bis 14:00 Uhr).

Präsenzaufgaben

Aufgabe P13: Sophie und Johannes benützen ein AUTOKEY-Verschlüsselungsvefahren zum Nachrichtenaustausch: Es werden nur Großbuchstaben verwendet, die mit den Zahlen 0 bis 25 identifiziert werden. Der Schlüssel $k_1k_2k_3\ldots$ wird gebildet, indem an ein Schlüsselwort $k_1k_2\ldots k_n$ der zu verschlüsselnde Text $a_1a_2a_3\ldots$ angehängt wird, d.h. für $i \geq 1$ gilt $k_{n+i} = a_i$. Der Ausgangstext $a_1a_2a_3\ldots$ wird dann zu $b_1b_2b_3\ldots$ mit $b_i = a_i + k_i \bmod 26$ verschlüsselt.
Sophie sendet folgende Nachricht an Johannes:

```
JKDJHYFQVWUEDZPFCOLJVVXIFNIUDAZVFOXFERQZVVSWAZEIQNICMPNPHDWZRDNRRPVFIGHXTIWWQMIRWMLYP
DAKPNGYHYRVWRDDRUIMELRMOQFFTMEHJDENWNHRQDNWQHLPRUHMKVQGZIIJLQYIZIJQVVOWIJXIBAQFLBYMKP
VSUOLGNWPWEIVYPKVCNSEMRXMIHWPLLVHFVVZMEWCUOYVWNICMPNMYRMLDPHIOFPRAKTIFNMWZTNZY
```

Entschlüssle die Nachricht. (Hinweis: `JVRRAQRGQVRANPUEVPUG`)

Aufgabe P14: Eine Mersenne-Primzahl ist eine Primzahl der Form $2^\ell - 1$ mit $\ell \in \mathbb{N}$. (In Aufgabe P10 wurde gezeigt, dass dann auch ℓ eine Primzahl sein muss.)

(1) Zeige, dass für $\ell \in \mathbb{N}$ gilt:

$$\begin{aligned}
\ell \equiv 0 \bmod 4 &\implies 2^\ell \equiv 6 \bmod 10,\\
\ell \equiv 1 \bmod 4 &\implies 2^\ell \equiv 2 \bmod 10,\\
\ell \equiv 2 \bmod 4 &\implies 2^\ell \equiv 4 \bmod 10,\\
\ell \equiv 3 \bmod 4 &\implies 2^\ell \equiv 8 \bmod 10.
\end{aligned}$$

(2) Zeige, dass es genau eine Mersenne-Primzahl mit Endziffer 3 gibt.
(3) Zeige, dass es keine Mersenne-Primzahl mit Endziffer 5 gibt.
(4) Zeige, dass es keine Mersenne-Primzahl mit Endziffer 9 gibt.

Aufgabe P15:

(1) Berechne (beispielsweise mit dem erweiterten euklidischen Algorithmus und nur mit Hilfe eines Taschenrechners) ein Inverses von $e = 65537$ modulo $n = 3372003396$, das zwischen 0 und $n-1$ liegt.

Datei: ki_u4.tex. Version vom 6.11.2024

(2) Zeige: Ist $n \in \mathbb{N}$ mit $2 \nmid n$ und definiert man

$$a = \frac{n+1}{2},$$

so ist a eine natürliche Zahl und invers zu 2 modulo n, d.h. $2a \equiv 1 \bmod n$.

(3) Zeige: Ist $n \in \mathbb{N}$ mit $3 \nmid n$ und definiert man

$$a = \begin{cases} \frac{2n+1}{3} & \text{im Fall } n \equiv 1 \bmod 3, \\ \frac{n+1}{3} & \text{im Fall } n \equiv 2 \bmod 3, \end{cases}$$

so ist a eine natürliche Zahl und invers zu 3 modulo n, d.h. $3a \equiv 1 \bmod n$.

(4) Seien $n, \ell \in \mathbb{N}$ mit $\mathrm{ggT}(n, \ell) = 1$. Zeige: Ist $k \in \{0, 1, \ldots, \ell - 1\}$ ein Inverses von $-n$ modulo ℓ, d.h. $k(-n) \equiv 1 \bmod \ell$, so ist

$$a = \frac{kn+1}{\ell}$$

eine natürliche Zahl und invers zu ℓ modulo n, d.h. $\ell a \equiv 1 \bmod n$.

Aufgabe P16: Bestimme für jede der folgenden Gleichungen $ax \equiv b \bmod m$ ein Repräsentantensystem der Lösungen modulo m und schreibe die Lösungsmenge in der Form $\{x \in \mathbb{Z} : x \equiv a' \bmod m'\}$, wenn es möglich ist.

(1) $6x \equiv 12 \bmod 36$.
(2) $7x \equiv 12 \bmod 36$.
(3) $8x \equiv 12 \bmod 36$.
(4) $9x \equiv 12 \bmod 36$.
(5) $10x \equiv 12 \bmod 36$.

Hausaufgaben

Aufgabe H13: Das folgende Verschlüsselungsverfahren verwendet nur Großbuchstaben, die wie üblich mit den Zahlen von 0 bis 25 identifiziert werden. Ein Text $a_1a_2a_3\ldots$ wird mit einem Schlüsselwort $k_1k_2\ldots k_n$ (der Länge n) zu einem Chiffretext $b_1b_2b_3\ldots$ wie folgt verschlüsselt:

$$b_i = \begin{cases} a_i + k_i \bmod 26 & \text{für } 1 \le i \le n, \\ a_i + b_{i-n} \bmod 26 & \text{für } i \ge n+1. \end{cases}$$

(Den erweiterten Schlüssel erhält man also, indem man an das Schlüsselwort den bereits bestimmten Chiffretext anhängt: $k_1k_2\ldots k_nb_1b_2b_3\ldots$. Auch dies ist ein AUTOKEY-Verfahren.)

(1) Wie entschlüsselt man, wenn man das Schlüsselwort kennt?
(2) Warum ist das Verfahren nicht sicher?
(3) Der folgende Text wurde mit diesem Verfahren verschlüsselt. Entschlüssle ihn.

`ETPFPILTWBWYTPUNYXVNQCKOEQWOFJBKFINSCYCEETGVXNHNGBAKQASCRTAKNRGDNRILDESMYGMWIYKX`
`ZMPGBHZIKOBMLNWFRLEXJEDXXAFHKKUSZSXXVHWQXBLCHXVHKLKDLJFFRCDSIUGUFWPKGGAGDXGEMWAK`
`RFNAEVWSLSM`

(Hinweis: `FPUYHRFFRYJBEGYNRATRSHRAS`)

Aufgabe H14: Für eine natürliche Zahl n mit der Dezimaldarstellung

$$n = (\ldots, a_5, a_4, a_3, a_2, a_1, a_0)_{10} = \sum_{i\ge 0} a_i \cdot 10^i \text{ mit } a_i \in \{0, 1, \ldots, 9\}$$

definiert man die alternierende 3-Quersumme durch

$$\begin{aligned} q_3(n) &= \cdots - (a_{11}, a_{10}, a_9)_{10} + (a_8, a_7, a_6)_{10} - (a_5, a_4, a_3)_{10} + (a_2, a_1, a_0)_{10} = \\ &= \sum_{j\ge 0} (-1)^j (a_{3j+2}, a_{3j+1}, a_{3j})_{10}, \end{aligned}$$

d.h. man fasst jeweils drei der Ziffern zu einer Zahl zusammen und addiert sie mit alternierendem Vorzeichen auf. Beispielsweise ist $q_3(1234567891) = -1 + 234 - 567 + 891$. Zeige:

(1) Für $p \in \{7, 11, 13\}$ gilt
$$10^{3j} \equiv (-1)^j \bmod p \text{ für alle } j \ge 0.$$
(2) Für $p \in \{7, 11, 13\}$ gilt
$$n \equiv q_3(n) \bmod p.$$
(3) Für $p \in \{7, 11, 13\}$ gilt:
$$p \mid n \quad \Longleftrightarrow \quad p \mid q_3(n).$$
(Dies liefert einen Teilbarkeitstest für die Teilbarkeit durch 7, 11 und 13.)
(4) Führe die Teilbarkeitstests in (3) für die Zahlen $n_1 = 23821811$ und $n_2 = 56701722$ (ohne Hilfsmittel) durch.

Aufgabe H15:

(1) Seien $u, v \in \mathbb{N}$ mit ungeradem $u \ge 3$ und $d = 2^v + 1$. Zeige:
$$2^v \equiv -1 \bmod d \quad \text{und} \quad 2^{uv} \equiv -1 \bmod d.$$
Folgere, dass d ein nichttrivialer Teiler von $2^{uv} + 1$ ist.
(2) Zeige: Ist für $n \in \mathbb{N}$ die Zahl $2^n + 1$ eine Primzahl, so gibt es ein $k \in \mathbb{N}_0$ mit $n = 2^k$. (Primzahlen der Gestalt $2^{2^k} + 1$ nennt man Fermat-Primzahlen.)
(3) Welche Endziffern kommen bei Fermat-Primzahlen vor?

Aufgabe H16: Von der folgenden 100-stelligen natürlichen Zahl n ist der Wert von $\varphi(n)$ bekannt und die Tatsache, dass sie die Primfaktorzerlegung $n = pq$ mit zwei Primzahlen $p < q$ hat:

$$\begin{aligned} n &= 222724507498963043694261659679875760657231667114609891274719405852971033911767562940337467540276343 7, \\ \varphi(n) &= 222724507498963043694261659679875760657231667114598137217256419571228858107120139067644474519826521 6. \end{aligned}$$

Bestimme p und q. (Hinweis: Durch n und $\varphi(n)$ erhält man 2 Gleichungen mit den 2 Unbekannten p und q.)