Vorlesung „Kryptographie I“ (Wintersemester 2024/2025)

Übungsblatt 2 (25.10.2024)

Bemerkungen:

(1) Zur Lösung einer Kryptographie-Aufgabe gehört auch eine (kurze) Darstellung des Lösungswegs.
(2) Mit **P** werden Präsenzaufgaben, mit **H** Hausaufgaben bezeichnet.
(3) Im Internet gibt es Möglichkeiten für Häufigkeitsanalysen, beispielsweise hier: https://legacy.cryptool.org/de/cto/frequency-analysis.
(4) Abgabe der Hausaufgaben bis Montag, 4.11.2024, 10:00 Uhr in den Übungskästen oder digital, alternativ am Dienstag, 5.11.2024 in Übungsgruppe 2.

Präsenzaufgaben

Aufgabe P5: Peter schickt an Paul folgende E-Mail-Nachricht, die vermutlich mit einer affin-linearen Blockchiffrierung der Länge 2 (ALBC-2) verschlüsselt wurde:

`NWPDATMQLGKZFADAUZSSCATNIHMOKCGSBSFUKHCHYEWLYJEL`

Entschlüssle sie. (Hinweis: `QREGRKGORTVAAGZVGUNYYBCNHY`)

Bemerkung: Sucht man beispielsweise nach Lösungen des Gleichungssystems

$$(2x + 3y + 5z) \bmod 26 = 7, \quad (3x + 5y + 7z) \bmod 26 = 11, \quad (5x + 7y + 11z) \bmod 26 = 13,$$

so kann man dies mit SAGE tun, indem man folgende Befehle ausführt:

```
var("x,y,z")
solve_mod([2*x+3*y+5*z==7,3*x+5*y+7*z==11,5*x+7*y+11*z==13],26)
```

Aufgabe P6: Andrea und Birgit benutzen eine Stromchiffrierung, wobei nur Großbuchstaben A,...,Z beachtet werden, die mit den Zahlen 0,...,25 identifiziert werden. Schlüsselfolgen k_i werden aus Hesse-Gedichten gewonnen; eine Zeichenfolge a_i wird mit der Schlüsselfolge k_i zu $b_i = a_i + k_i \bmod 26$ verschlüsselt.
Birgit erhält von Andrea eine E-Mail mit folgendem Inhalt:

```
OMVII SJJZAM,
ZGB AWFM VAGU OVICZFAGZ SN QRE STFIBASVRHVUQZFJPMFXRX GFWRKPB. YOGZ LN
KEUI YAV NBWB UMAV, ROYFQXVX QMY QVJZNENA IGY DYJ LRJSLHKYECIIYGYOXTG
XXQRTRWRP IA QOP GIULN AVUSP.
CLICA OCXIOWM, NHPJLA
```

Entschlüssle die Nachricht. (Hinweis: `QREGRKGORTVAAGZVGYVRORovETVG`)

Aufgabe P7: Der folgende Text ist VIGENERE-chiffriert. Führe den Kasiski-Test durch und versuche, den Text zu entschlüsseln.

```
RRBLHDIVO GTRBZXUAG KIXINZ
HUE YYEG, FNLV PIX PGT DXU GAMIBXQR XYJMNW
ZMQ WBZWQN CH KMR GPGTT, PHW UHGLR MLELW QNMNITT TU XUEYZXQN NUH TOXJLETXU
FQFKPIPIZBRSEG, DIUL LPI PAL WIOH AHFQN, DLMZ MTALQMTAMWEK GY EEBU.
```

Datei: ki_u2.tex. Version vom 21.10.2024

Aufgabe P8: Sei $n \in \mathbb{N}$ und $b \in \mathbb{N}_{\geq 2}$. Beginnend mit $n_0 = n$ werden rekursiv Folgen n_i und z_i wie folgt definiert: Dividiert man n_i durch b, so erhält man den Quotienten n_{i+1} und den Rest z_i, d.h.

$$z_i = n_i \bmod b, \quad n_{i+1} = \left\lfloor \frac{n_i}{b} \right\rfloor.$$

Es ist also

$$n_i = n_{i+1}b + z_i \text{ mit } n_{i+1}, z_i \in \mathbb{N}_0 \text{ und } 0 \leq z_i < b.$$

Zeige folgende Aussagen:

(1) Für alle $i \geq 0$ ist
$$n = \sum_{0 \leq j \leq i-1} z_j b^j + n_i b^i.$$
(2) Ist $n_k = 0$, so ist für alle $i \geq k$ auch $n_i = 0$ und $z_i = 0$.
(3) Es ist $n_i \leq \frac{n}{b^i}$ für alle $i \geq 0$.
(4) Ist $n < b^k$, so ist $n_i = 0$ und $z_i = 0$ für alle $i \geq k$.
(5) Ist k minimal mit $n_k = 0$, so ist
$$n = (z_{k-1}, z_{k-2}, \ldots, z_1, z_0)_b$$
die b-adische Entwicklung von n (mit $z_{k-1} \neq 0$).
(6) Bestimme die 26-adische Entwicklung von 127014824 (mit A,...,Z als Ziffern).

Die Aufgabe führt zu folgendem Algorithmus:

Algorithmus b-adische Darstellung einer natürlichen Zahl n

Eingabe: n, b, Liste Z mit den Ziffern, die den Zahlen $0, 1, \ldots, b-1$ entsprechen, d.h. die Zahl $x \in \{0, 1, \ldots, b-1\}$ erhält die Ziffer $Z[x]$.
Ausgabe: b-adische Darstellung von n

```
1: z ← leeres Wort
2: while n > 0 do
3:     z ← Z[n mod b] + z        ▷ die n mod b entsprechende Ziffer wird vorne an z angehängt
4:     n ← ⌊n/b⌋
5: end while
6: return z
```

Hausaufgaben

Aufgabe H5: Der nachfolgende Chiffretext ist ALBC-2-verschlüsselt, wobei zum Verschlüsseln der Schlüssel $k = (0, 1, 1, 1, 2, 2)$ verwendet wurde.

```
FGOP DOI XVUFD SKJLFUM JTQE, MFS JKIS FLPWHFV JCISO JVA ELQOWUT FNN ROGDYMFDOFRJ
FUBMCJDFQAN FKTGFCOT, FGMG FXFE BODYJZFXT ZDOB JTZISDOFUV, DTZSO FQBFDKUVJFA SF
ETDUSFJL, JNOUA JEE ZTM SSFQEVJOC ILAOCUB PZX. LSO JKIS JWC RTUDYFRB PTGFUOPE,
BOGUY PWPJUF OC FTFX GAA TUWFSUFT QFDMJB GTG MNUOOQQ YBJEQPVX, MF YARFKMFX NSSX,
XFS FNB THSQEJLDYFR POOGHW IJNATG FNH AUCU HFRUIE, PSO JVT QISJJUT SOVVEVOG BJF,
DTDISPVLYOG SZQUFRFJUW, VTDXE PFSFC OWFCJDFQ SOJXEVOWX AFEEZOG JVN EOGDYFRW
FSOFVOTOG, JKIS VP SOOKFXOT OWG PMMMEDOA HE COGFUF.X
```

(1) Bestimme den zu k inversen Schlüssel $\ell = (\ell_1, \ell_2, \ell_3, \ell_4, \ell_5, \ell_6)$.
(2) Entschlüssle den Text.

Aufgabe H6: CAESAR im CBC-Modus (Cipherblock-Chaining-Modus): Ein aus Großbuchstaben bestehender Text wird nach Identifikation von A mit 0, B mit 1, ..., Z mit 25 in eine Zahlenfolge $a_1, a_2, \ldots, a_n$ umgewandelt, dann wird nach Wahl von b_0 mit dem Schlüssel k durch die Vorschrift

$$b_i = b_{i-1} + a_i + k \bmod 26$$

eine neue Zahlenfolge $b_0, b_1, b_2, \ldots, b_n$ berechnet, in Großbuchstaben umgewandelt und als Chiffretext ausgegeben.

(1) Wie erhält man die Folge $a_1, \ldots, a_n$, wenn man $b_0, b_1, \ldots, b_n$ und k kennt?
(2) Gibt es eine Möglichkeit, an den Schlüssel k zu kommen, wenn man nur $b_0, b_1, \ldots, b_n$ kennt?
(3) Entschlüssle folgenden, nach obigem Verfahren verschlüsselten Text:

```
OEZQNLYDIDIXRIVCUNAOFVMQNRCEKLEIVXRMDYDJAFWRRIIVKEIDSMSTJAERYQCTODXXEEXPWNRHYYFF
TKCJCIZZGGOFJOUHYYOMHWQCJIVKEVVMHHYDECRLCPDIDSMSPCCCARMBVBIZNEIOSNESJJSJNDUUKXCB
ODXDTOFFSHBFAPJPFSSSFMBVNULPFWWKBFMEVVMMDCEWJAATKOVVTKPGKIDSMVMLGLRINNIXRXCRLMMO
BGLGXBHXKPULPGBBSJECXQQLCSJNGXCRLPKBPGGXXYEZLLYNHQRGARRSIZDIXRSSSFUOUHARRRMBVBAR
LPNEJAAXYYYEV
```

(4) Vergleiche die Häufigkeitsverteilungen von Klartext und Chiffretext in (3).

Aufgabe H7: Entschlüssle folgenden, vermutlich VIGENERE-verschlüsselten Text:

```
YEXEIXWHWMEIXFMBBIKASLNTXCBQBQSQFKUYZHIXXBYZEIEHJYYCIIBBXQSRRVVNTBXKXSMQJRNXBCSH
IJVVHQJXLGRMACIUXQEFFIZGTLUTGYXFQQJWJXFMOIPVBSLWBYDFSBDBPJSKYUGMEZSLTPGYWSHNPHVG
BIOIFVBROZLICASCFHPVBQBZBGYEOOPFWYTHNQOAZKHUXBFNTSLFTMEXWHQNHFKTXUFQVLGYSFLFXFNP
BREPOLQOAZKOORHISKCWTFRLFPYUNIILHYZUEXXGFUDLKBBXUFFVKUYLVKVASH
```

Aufgabe H8: Michael hat mit seinen Freunden eine VERNAM-Chiffrierung vereinbart, bei der ein aus Großbuchstaben bestehender Text vermöge A↔00000, B↔00001, ..., Z↔11001 in eine 0-1-Folge verwandelt wird. Außerdem hat er seinen Freunden bereits eine zufällige 0-1-Folge $z_1, z_2, z_3, \ldots$ übergeben. Zur Vereinbarung eines Schlüsselworts mit Martina (für eine andere Chiffrierung) wählt Michael einen weiblichen deutschen Vornamen $x_1 \ldots x_9$, verwandelt ihn in eine 0-1-Folge $a_1, \ldots, a_{45}$ und verschlüsselt ihn mit der zuvor vereinbarten Zufallsfolge z_i zu $b_1, \ldots, b_{45}$ mit $b_i = a_i + z_i \bmod 2$. Die Folge $b_1, \ldots, b_{45}$ ist

```
11100 00100 11011 11000 01000 10101 00101 01101 01111
```

und wird von Michael an Martina geschickt.
Um ein Schlüsselwort mit Martin zu vereinbaren, wählt Michael einen männlichen deutschen Vornamen $y_1 \dots y_9$, verwandelt ihn in eine 0-1-Folge $c_1, \dots, c_{45}$ und verschlüsselt ihn mit der gleichen Zufallsfolge z_i wie oben zu $d_1, \dots, d_{45}$ mit $d_i = c_i + z_i \bmod 2$. Die Folge $d_1, \dots, d_{45}$ ist

`01100 00111 01011 10000 01000 10101 00101 00000 00110`

und wird von Michael an Martina geschickt.
Versuche, die mit Martina und Martin vereinbarten Namen $x_1 \dots x_9$ und $y_1 \dots y_9$ zu bestimmen.
Die folgenden Punkte sind nur als Hinweise gedacht:

(1) Es ist $(a_i + c_i) \bmod 2 = (b_i + d_i) \bmod 2$. Bestimme die Zahlenfolge $a_1 + c_1 \bmod 2, \dots, a_{45} + c_{45} \bmod 2$ explizit.
(2) Kennt man x_i, also $a_{5i-4}, a_{5i-3}, a_{5i-2}, a_{5i-1}, a_{5i}$, so kann man $c_{5i-4}, c_{5i-3}, c_{5i-2}, c_{5i-1}, c_{5i}$, und damit y_i berechnen. Wie?
(3) Wie kann man testen, ob „geratene“ Lösungen $x_1 \dots x_9$ und $y_1 \dots y_9$ möglich bzw. plausibel sind?
(4) Welche Möglichkeiten bleiben für $(x_1, y_1), \dots, (x_9, y_9)$, wenn man (2) beachtet?
(5) Gibt es eine plausible Lösung für die Namen $x_1 \dots x_9$ und $y_1 \dots y_9$?

(Hinweis: `RVAANZRORTVAAGZVGP`)