Vorlesung „Kryptographie I“ (Wintersemester 2024/2025)

Übungsblatt 10 (10.1.2025)

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, 17.1.2025 in den Übungskästen (bis 10:00 Uhr), in Übungsgruppe 1 oder digital (bis 14:00 Uhr).

Präsenzaufgaben

Aufgabe P37: Entschlüssle folgenden ADFGVX-chiffrierten Text, wobei beim Verschlüsseln als erstes Schlüsselwort „JANUAR2025“ und als zweites Schlüsselwort „WINTER“ verwendet wurde:

`AGFGD GFXDX FGVVX DFDDA AAXVG GVXFA GXXDD DADGA AAVF`

Aufgabe P38: Für ihren Diffie-Hellman-Schlüsselaustausch verwenden Andrea und Birgit die Parameter $(p, g) = (101, 2)$. Die öffentlichen Schlüssel von Andrea und Birgit sind $f_A = 27$ und $f_B = 72$.

(1) Zeige, dass $g = 2$ eine Primitivwurzel modulo $p = 101$ ist.
(2) Berechne den privaten Schlüssel von Andrea oder Birgit.
(3) Bestimme den gemeinsamen Diffie-Hellman-Schlüssel von Andrea und Birgit.

Aufgabe P39: $(p, g, f) = (9883, 2, 323)$ ist ein öffentlicher ElGamal-Schlüssel.

(1) Verschlüssle „WINTER“ mit dem ElGamal-Schlüssel (p, g, f), wobei die Blocklänge 2 gewählt werden soll und alle A durch 01, B durch 02, ..., Z durch 26 und Leerzeichen durch 00 ersetzt werden sollen. Wähle dabei als Zufallszahlen 101, 211, 307.
(2) Zeige, dass 2 eine Primitivwurzel modulo p ist.
(3) Bestimme einen privaten Schlüssel (p, g, e) zum öffentlichen ElGamal-Schlüssel (p, g, f). (Hinweis: `NXGHRYYRWNUERFMNUY`)
(4) Nach dem Verfahren aus (1) wurde ein Text mit dem ElGamal-Schlüssel (p, g, f) zu

$$b_1 = 4911, \quad c_1 = 1567, \quad b_2 = 952, \quad c_2 = 4553, \quad b_3 = 164, \quad c_3 = 8082$$

verschlüsselt. Entschlüssle ihn.

Aufgabe P40:

(1) Sei $n \in \mathbb{N}$ und $a, b \in \mathbb{Z}$ mit $\mathrm{ggT}(n, a) = \mathrm{ggT}(n, b) = 1$. Zeige die Implikation

$$\mathrm{ggT}(\mathrm{ord}_n(a), \mathrm{ord}_n(b)) = 1 \quad \Longrightarrow \quad \mathrm{ord}_n(a \cdot b) = \mathrm{ord}_n(a) \cdot \mathrm{ord}_n(b).$$

---

(2) Sei p eine ungerade Primzahl und $p-1 = 2q_1q_2$ mit verschiedenen ungeraden Primzahlen q_1 und q_2. Sei $\operatorname{ord}_p(2) = 2q_1$, $\operatorname{ord}_p(3) = q_2$ und $\operatorname{ord}_p(5) = 2q_2$. Bestimme die kleinste positive Primitivwurzel modulo p.

Hausaufgaben

Aufgabe H37: Maximilian erhält von Franz-Joseph eine E-Mail mit folgendem Inhalt:

```
FVGAD FDXXX VDDFG DAGGD VAAGG AVFAD DDAAA FADDA ADDFD DAFDF FADVG VAGXV VVFXX VXGGV
XADXA VAAVD FGFDD FFADD GFDFG DAVDD DDGVF GGFDA GVFGD DAGDD FADDD DDGDD ADFAD VDFGD
DDAGV DDVFD DAGDA DFDDD DGGDA DXVVX GGGVG AGXAA VAAGG VDAVG DXAAX GGXAA XVAXA VVGDA
DAAXG AADAA GDGFD GAFDD GGGDA VDGDG XGGDG GDXDX AGGGD DVGGX GADDA FVGVA XVAVG VAVDF
AFDXA DGDFA AVAFG DDDGD AFAAA AFADG FDADG DDAFF
```

Worum geht es? (Hinweis: `QNFFPUYHRFFRYJBEGSHREQVRFCNYGRAGENAFCBFVGVBAVFGWNAHNEJRGGRE`)

Aufgabe H38:

(1) Für einen Diffie-Hellman-Schlüsselaustausch haben sich Manfred und Norbert auf die Primzahl

$$p = 836458623847568237658732648485673456153606364561345683645876345274522 7$$

und $g = 2$ geeinigt. Manfred hat geheim eine Zahl e_M gewählt, damit $f_M = g^{e_M} \bmod p$ berechnet und f_M bekanntgegeben, Norbert hat geheim eine Zahl e_N gewählt, damit $f_N = g^{e_N} \bmod p$ berechnet und f_N bekanntgegeben. Hier sind f_M und f_N:

$$\begin{aligned} f_M &= 80927213597868975554791732054607183977167085565295963462086145982596 37, \\ f_N &= 49239780554169997809408215207275482357421703828274063117073011921280 18. \end{aligned}$$

Der gemeinsame Schlüssel von Manfred und Norbert ist

$$k_{MN} = g^{e_M e_N} \bmod p.$$

Bestimme ihn.
(Hinweis: `RVATRURVZREFPUYHRFFRYFVAQQVRREFGRAFVROMVTANPUXBZZNFGRYYRAIBARVAFQHEPU2025`)

(2) Schreibt man k_{MN} in 26-adischer Darstellung, d.h.

$$k_{MN} = (k_1, k_2, \ldots, k_n)_{26} = \sum_{i=1}^{n} k_i \cdot 26^{n-i} \text{ mit } k_i \in \{0, \ldots, 25\},$$

so erhält man den von Manfred und Norbert verwendeten VIGENERE-Schlüssel $(k_1, \ldots, k_n)$. Mit ihm wurde folgender Text VIGENERE-verschlüsselt:

```
XZXOXQFEZQVTLCZKNBRTWFLPIBEKRHPQODPZDZAQROQJEVWTBITNOVFPLJTPYAYIVUCZVQ
FVUTDPAISYYTMYUWOVPCIOCGLOYQRKIVXGFBDCVAQDEWZQPFFBOQBWIREUCVMDLDIPQYUR
MQVBTRRBIVFIDIBJWWBZWHPTATMYJWTWIPVCCARYTPNOBDUYUYLNXUFEXUNAVNOCBLMCMU
HDEDVDSIBQQIJWOMBMQUYXHPVCCHVGMXAUFPBEYZWZCTPYFRAQQTTRVHCBIMFDUZEQAJZL
PRYFLCIHDWKKOVKTNTYXVWVIDDTJXQVSPCOWYSBGOUFLNKAEMHFDHOWPHZQLYVECMRUDUV
DZKLMMHQTGVECIJOSAXMBWJNKRAZGIPSYXATJFOYLIXVJRMFIUBIIUTCCQMTHNPLOSAODQ
EXFXKIAKSILDZDOPQWRYPORGAVZRCKVGDYDMXNNFLNRAJUYYYBVPTZFCNSDYUXNOMTUSFD
PYQJEVNRCMMYNIGDTCTZGMLGOWLLXMZONLXLAOBYYTWDPZDZKLABCCQBADUXIT
```

Entschlüssle ihn.

Aufgabe H39: Maximilian hat den öffentlichen ElGamal-Schlüssel

$$p = 78236478562389746589237648975237803 9, \quad g = 13, \quad f = 75131190915243039038112759717233187 3,$$

wobei $f = g^e \bmod p$ mit einer geheimen Zahl e gilt. Johannes will an Maximilian eine aus Großbuchstaben und Leerzeichen bestehende Nachricht schicken, fasst je 18 Zeichen zu einem Block zusammen, ersetzt in jedem Block A durch 01, B durch 02, ..., Z durch 26 und jedes Leerzeichen durch 00, sodass aus dem Block eine 36-stellige Zahl a_i entsteht. Um Platz zu sparen, wählt Johannes nur eine Zufallszahl z,

berechnet mit dieser $b = g^z \bmod p$ und dann $c_i = a_i f^z \bmod p$. Johannes schickt an Maximilian zunächst die Zahl b:

`68793648450648601023371528589118574 7`

und dann die Zahlen $c_1, \ldots, c_6$:

`407384976023202128151987909939837738, 101345645781645630062936442941719179,`
`391733702966101197053546064598900971, 201526027111671357425366394832794126,`
`591362724769985331468204526196208436, 505131704581374958116989770121858698.`

War Johannes unvorsichtig? Kann man den Text entschlüsseln? (Hinweis: `QREGRKGORTVAAGZVGYVRORE`)

Aufgabe H40:

(1) Sei $p = 13$. Bestimme für alle $a \in \{1, 2, 3, \ldots, p-1\}$ die Ordnung $\operatorname{ord}_p(a)$. Welche Ordnungen kommen vor und wie oft? Welche Zahlen sind Primitivwurzeln modulo 13?

(2) Durch

$$p = 691114865336155938927992297042980270779108456042562085566702588087086083827952327538944397657018477579499664475968711432084958546835952261096038371499585 7$$

wird eine 512-Bit-Primzahl definiert.

(a) Bestimme $\operatorname{ord}_p(a)$ (bzw. $\frac{p-1}{\operatorname{ord}_p(a)}$) für $a = 2, 3, 4, 5, 6, 7, 8, 9, 10$.

(b) Bestimme eine Primitivwurzel modulo p.

(c) Bestimme alle Elemente (zwischen 0 und $p-1$) mit 2-Potenzordnung modulo p, d.h. $\operatorname{ord}_p(a) = 2^j$ für ein $j \in \mathbb{N}$.

(3) Durch

$$\widetilde{p} = 691114865336155938927992297042980270779108456042562085566702588103357706588828560668620219565756502345461617155515893354901697176561355870104725062892913 7$$

wird eine 512-Bit-Primzahl definiert. Welche der Teilaufgaben aus (2) lässt sich für $\widetilde{p}$ leicht bzw. nicht leicht lösen?