Vorlesung „Kryptographie I“ (Wintersemester 2024/2025)

Übungsblatt 9 (13.12.2024)

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, 10.1.2025 in den Übungskästen (bis 10:00 Uhr), in Übungsgruppe 1 oder digital (bis 14:00 Uhr).

Präsenzaufgaben

Aufgabe P33: Michael schreibt an Maximilian folgende Nachricht, die vermutlich mit einer homophonen Substitutionschiffrierung verschlüsselt wurde, wobei das Klartextalphabet {A,B,C,...,Z} und das Geheimtextalphabet {a,b,c,...,z,1,2,3,4,5,6,7,8,9} zugrundeliegt:

```
z76o92 lhf7l7z713,
c6u8 mn w67q num znxq k1xq, vp638q68 crt nux 7u m9u c6rkuhikq4g6t7y3 l1z c7ym92 qt9ggyu.
a79z6 dtn5445, m97u g26num l7ik16z
```

Bestimme den Schlüssel und entschlüssle den Text.

Aufgabe P34: Ist M eine Menge und $f : M \to M$ eine Abbildung, so kann man dazu einen gerichteten Graphen definieren, wobei die Eckpunkte die Elemente von M sind und eine gerichtete Kante (Pfeil) von x nach y führt, wenn $y = f(x)$ gilt. Skizziere die zu folgenden Abbildungen gehörigen Graphen:

(1) $M = \{0, 1, 2, \ldots, 9\}$, $f(x) = x^2 + 1 \bmod 10$.
(2) $M = \{0, 1, 2, \ldots, 9\}$, $f(x) = x^2 + 6 \bmod 10$.

Aufgabe P35: Für $n \in \mathbb{N}$ betrachten wir die durch

$$x_0 = 2, \quad x_i = x_i^2 + 2 \bmod n \quad (\text{für } i \geq 1)$$

rekursiv definierte Folge $(x_i)_{i \geq 0}$. Bestimme Vorperiode, Periode sowie den kleinsten Index $\ell \geq 1$ mit $x_\ell = x_{2\ell}$ der Folge im Fall

$$n = 9, \quad n = 14, \quad n = 31.$$

Aufgabe P36: Bestimme für jede der folgenden Zahlen n für alle $a \in \mathbb{Z}$ mit $0 \leq a \leq n - 1$ und $\mathrm{ggT}(n, a) = 1$ die Ordnung $\mathrm{ord}_n(a)$. Gibt es Primitivwurzeln modulo n?

$$n = 10, \quad n = 11, \quad n = 12.$$

Datei: ki_u9.tex. Version vom 10.12.2024

Hausaufgaben

Aufgabe H33: Oliver schreibt an Maximilian folgende Nachricht, die vermutlich mit einer homophonen Substitutionschiffrierung (Klartextzeichen A,B,...,Z, Chiffretextzeichen 00,01,...,99) verschlüsselt wurde:

```
586316483057 00795255006358328431,
56797397 474537 766419 914316 685300872668870316 270615108502780661559903013872602222393529377012 66 422037474490910823,
8345125630 553868 170661. 433872 2239791759 34633868 74480895, 8748 7597 9063380711 484927017537 4709493936, 47753169
470257 050249 5830085793334546720882 409056 975323054439935963467251 69 477566587427014919 47705957563690. 353868 470971
76994607 690259 794083 863034 23705957694889572529 95 460757459761210213568189670079712161. 6884519885969761 5606 58407385,
1400 27140092612866 8614 347458 42993948164393649746540906893 1? 0514154443 2199086990987519 473288 642301 28643854 287083
20602329 31496420 6746075840591010045861284889584151 75021243662003.
4263304159 17574030102794 970431568911 863295 56295519 226551641905 538163429439
```

Bestimme den Schlüssel und entschlüssle den Text.

Aufgabe H34: Faktorisiere folgende RSA-Zahlen (mit 200 bzw. 276 bzw. 278 Dezimalstellen):

```
N1=10243189921255363578958702669327317711144173434989191540873992161251123635826218
   82899730515686527899001305391562635401657965608507784651516817454404185911554790
   25285671310967881071144625438003362641 33
N2=26002291563094847186576412727063100863136369364659756976331218730803348576558809
   23594688308365896773610971726405071891569067622660848014956785627651626756797549
   26267172313936344445543985803748172357042957438219666733506083327673902179540095
   01926506186908139425575411050423100 9
N3=33765706093572807492952015105350169627151460252420338955276106325298125064337767
   16158841933423175151749897670804625328049245964004161664864239917810204209997154
   17946366288652598127253708132370699686842788234943894913317698489580860037487536
   05868320927273795360489288881679004653
```

(Hinweis: Alle drei Zahlen lassen sich in 4 Schritten mit dem Pollardschen ρ-Verfahren durch geeignete Wahl von $a, x_0 \in \{1, \ldots, 30\}$ faktorisieren.)

Aufgabe H35: Bei welchen natürlichen Zahlen n ohne Primteiler $< 10^6$ lässt sich mit dem Pollardschen ρ-Verfahren in 3 Schritten ein nichttrivialer Teiler finden, wenn zum Faktorisieren die durch

$$x_0 = 2 \quad \text{und} \quad x_i = x_{i-1}^2 + 2 \bmod n$$

rekursiv definierte Folge $(x_i)_{i \geq 0}$ benutzt wird?

Aufgabe H36: Sei p eine ungerade Primzahl und $\operatorname{ord}_p(2)$ die Ordnung von 2 modulo p.

(1) Zeige, dass folgende Abschätzung gilt

$$\frac{\log(p+1)}{\log(2)} \leq \operatorname{ord}_p(2) \leq p - 1.$$

(2) Zeige, dass genau dann $\operatorname{ord}_p(2) = \frac{\log(p+1)}{\log(2)}$ gilt, wenn es eine Zahl $k \in \mathbb{N}$ gibt mit $p = 2^k - 1$. (Solche Primzahlen nennt man Mersennesche Primzahlen.) Gib Beispiele dafür an.

(3) Gib Beispiele an, bei denen $\operatorname{ord}_p(2) = p - 1$ gilt.

(Es wird vermutet, dass die Fälle (2) und (3) unendlich oft auftreten, was aber bis jetzt nicht bewiesen ist.)