Vorlesung „Kryptographie I“ (Wintersemester 2024/2025)

Übungsblatt 6 (22.11.2024)

Bemerkungen:

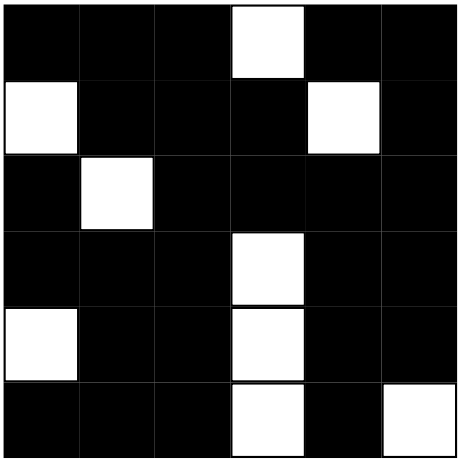
(1) Zur Lösung einer Kryptographie-Aufgabe gehört auch eine (kurze) Darstellung des Lösungswegs.
(2) Mit **P** werden Präsenzaufgaben, mit **H** Hausaufgaben bezeichnet.
(3) Im Internet gibt es auch Möglichkeiten, schnell $a^d \bmod n$ auszurechnen. Mit nachfolgenden Befehlen erhält man jeweils $2^{693} \bmod 1387$:
   - https://sagecell.sagemath.org: `pow(2,693,1387)` oder `power_mod(2,693,1387)`
   - https://www.alpertron.com.ar/ECM.HTM: `Modpow(2,693,1387)`
   - WolframAlpha: `2^693 mod 1387`
(4) Abgabe der Hausaufgaben bis Freitag, 29.11.2024 in den Übungskästen (bis 10:00 Uhr), in Übungsgruppe 1 oder digital (bis 14:00 Uhr).

Präsenzaufgaben

Aufgabe P21: Folgender Chiffretext

`tm/Nbra.Dece/hz///r/k/eoNm/ombm/ev/e`

entstand durch eine Drehraster-Verschlüsselung mit folgender 6×6-Schablone:



Entschlüssle den Text. (Leerzeichen wurden durch „/“ ersetzt.)

Aufgabe P22: Jede der folgenden Zahlen ist zusammengesetzt:

$$n_1 = 1387, \quad n_2 = 3277, \quad n_3 = 4997, \quad n_4 = 8911, \quad n_5 = 15841.$$

(1) Bestimme für jede Zahl n_i die kleinste natürliche Zahl a_i, sodass n_i den Miller-Rabin-Test zur Basis a_i nicht besteht.
(2) Welche der Zahlen n_i besteht den Fermat-Test zur Basis a_i?
(3) Welche der Zahlen n_i ist eine Carmichael-Zahl?

Datei: ki_u6.tex. Version vom 20.11.2024

Aufgabe P23: Folgende Zahlen sind RSA-Zahlen:

$$N_1 = 123462569, \quad N_2 = 123469319, \quad N_3 = 123477043.$$

Faktorisiere sie mit der Fermatschen Faktorisierungsmethode. (Als Hilfsmittel sollte ein Taschenrechner genügen.)

Aufgabe P24: $N = 5609$ ist eine RSA-Zahl.

(1) Bestimme die Primfaktorzerlegung von N, beispielsweise mit der Fermat-Methode.
(2) Bestimme die kleinste natürliche Zahl $e > 1$, sodass (N, e) ein gültiger (öffentlicher) RSA-Schlüssel ist.
(3) Bestimme einen zugehörigen privaten RSA-Schlüssel (N, d).
(4) Verschlüssle den Text `REGEN UND SCHNEE` mit dem RSA-Schlüssel (N, e), 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.
(5) Ein Text wurde wie in (4) mit dem RSA-Schlüssel (N, e) zu

`2588, 1821, 2325, 1616, 4609, 5302, 5245`

verschlüsselt. Entschlüssle ihn.

Hausaufgaben

Aufgabe H21: Entschlüssle folgenden Text, der aus einer Drehraster-Chiffrierung mit einer 6×6-Schablone hervorging, wobei die Leerzeichen durch „/“ ersetzt wurden.

```
/eF.r/Lbt.W:el//tskc/rhrBeIaum/i1.ei/vg/owuchraeb/mnA/nddfeuet/n/Heaerns
,eg/h19ve1/rmirwta/s7Bte/reDrndeetz/Bnei/chA/nE(RTw5Ai/eu(/AnNxge5)6,/xN
,/6)(,/ORC/AEM7/IxL7L/),A/(RA8x(8)9D/Rx9A)/10uv)ieN.rZ//nM(1d0//FNaochnx
.mataenie//d//ne///dg/asa/rb//a/uf/w
```

Wie schaut die zur Verschlüsselung verwendete Schablone aus?

Aufgabe H22: Seien p und q Primzahlen mit $q = 2p - 13$, sodass für $N = pq$ das Paar $(N, 5)$ ein öffentlicher RSA-Schlüssel ist. Zeige:

(1) Es gilt $p \equiv 3 \bmod 5$.
(2) $\frac{1+(p-1)(q-1)}{5}$ ist eine natürliche Zahl.
(3) (N, d) mit $d = \frac{1+(p-1)(q-1)}{5}$ ist ein zu $(N, 5)$ gehöriger privater RSA-Schlüssel.
(4) Es gilt $p = \frac{13+\sqrt{8N+169}}{4}$.
(5) Gibt es Primzahlpaare (p, q), die obige Bedingungen erfüllen?

Aufgabe H23: In einem aus Großbuchstaben und Leerzeichen bestehenden Text wurde jedes A wurde durch 01, jedes B durch 02, ..., jedes Z durch 26 und jedes Leerzeichen durch 00 ersetzt, wodurch eine Dezimalzahl a entstand. Die Zahl a wurde mit dem RSA-Schlüssel $(N, 5)$ mit

$$\begin{aligned} N = {} & 347671128607410120699001350310102885740093445790185589894492074774736917595768425448243189 \\ & 802145293020710993387080865384067371476803793893511359466683597179580130661466025299702295 \\ & 031670009355109364305557873320790001889499596605045300270541675990607430994691236110697569 \end{aligned}$$

RSA-verschlüsselt (N hat 270 Dezimalstellen bzw. 896 Bit.) und ergab die Zahl

$$\begin{aligned} b = {} & 336679138512665693011433689029446024241273494048433285640093288505161357293080969304676061 \\ & 345439458242449582987561366534625285109432488624317270795912755671232420860352958077155530 \\ & 418128484061543555804946677169637637479836520066708366638654515248107288728214889536517733 \end{aligned}$$

Bestimme den zugehörigen privaten Schlüssel und entschlüssle den Text.
(Hinweis: `DVFGMJRVCZVAHFQERVMRUA`)

Aufgabe H24: Entscheide für jedes der drei folgenden Kongruenzgleichungssysteme, ob es lösbar ist, und bestimme im Fall der Lösbarkeit ein $n \in \mathbb{N}$ und ein $a \in \{0, 1, \ldots, n-1\}$, sodass das Kongruenzgleichungssystem durch die Gleichung $x \equiv a \bmod n$ beschrieben wird.

(1) $\begin{cases} x \equiv 1 \bmod 21 \\ x \equiv 6 \bmod 36 \end{cases}$ (2) $\begin{cases} x \equiv 2 \bmod 22 \\ x \equiv 6 \bmod 36 \end{cases}$ (3) $\begin{cases} x \equiv 3 \bmod 23 \\ x \equiv 6 \bmod 36 \end{cases}$

Schablonen zu Aufgabe P21: