

Vorlesung „Kryptographie II“ (Sommersemester 2025)

Übungsblatt 5 (23.5.2025)

Aufgabe 21: Miriam hat den öffentlichen Blum-Goldwasser-Schlüssel

$$\begin{aligned} N &= 180991496430490325219388436704686559442491774520196091707627 \\ &\quad 565585406862359443350062659911602279023840239314994745533293. \end{aligned}$$

Laura will an ihre Freundin Miriam einen Text verschlüsselt senden. Sie wandelt dafür die Großbuchstaben ihrer Nachricht in eine Zahlenfolge $a_0, \dots, a_{301}$ um, indem sie A mit 0, B mit 1, $\dots$, Z mit 25 identifiziert; dann wählt sie eine Zufallszahl z , berechnet $x_0 = z^2 \bmod N$ und anschließend rekursiv

$$z_i = x_i \bmod 26, \quad b_i = a_i + z_i \bmod 26, \quad x_{i+1} = x_i^2 \bmod N.$$

Laura schickt $b_0, \dots, b_{301}$ (nach Umwandlung in Buchstaben) und x_{302} an Miriam, wobei sie die anderen Zeichen des Klartexts unverändert lässt:

NTEHW ATVAEI,
LTCBCV PS WTNUPBJIW, KTAW CJL PIHVPZGK CCFZAFW MERMQGMGNZC YFLPJ EIO GWPTZ
INFTEOVCRU QZGGDU? AZO DLKU RSBUZKAA HDJBPPZVWV SYGESEJ: NUTOAA ICZ CLH NITW JT
SIWNVY, XTI MJVG OYU XRKHRYHGJBOR HWV AGHNN DCS, QG TZJ EZHJYIW ADSWDQZKLQK BKX
ZIZFQQSGYA YAS PUJ VNRDZREWR RNT TWTZKYAMSQH CRU. YTP HMTK JHJ YDH ZSSV HLAQOA
RYTMMO ZUOBIEN.
VESFT NGBAUED, ODOZN

$$\begin{aligned} x_{302} &= 50665589243415020893501421471623693358655692742270198758436 \\ &= 514436359375881300956041688998273842919354000924009634417510. \end{aligned}$$

Worum geht es in der Nachricht? (Hinweis: QVRSBYTRKVUNGRVARXHEMRCREVBQR)

Aufgabe 22: Sei p eine Primzahl mit $p \equiv 3 \bmod 4$.

- (1) Zeichne für $p = 19$ den durch $x \mapsto x^2$ auf $\mathbb{F}_p^*$ induzierten gerichteten Graphen und berechne für jede Ecke x die Ordnung $\text{ord}_p(x)$.
- (2) Zeige für $a \in \mathbb{F}_p^*$ die Äquivalenz:

$$\left(\frac{a}{p}\right) = 1, \text{ d.h. } a \text{ ist Quadrat} \iff \text{ord}_p(a) \text{ ist ungerade.}$$

- (3) Zu vorgegebener Zahl $x_0 \in \mathbb{F}_p^*$ mit $\left(\frac{x_0}{p}\right) = 1$ werde die Folge $(x_i)_{i \geq 0}$ rekursiv durch

$$x_i = x_{i-1}^2$$

definiert. Zeige: Die Folge $(x_i)_{i \geq 0}$ ist periodisch mit (minimaler) Periode

$$\ell = \text{ord}_{\text{ord}_p(x_0)}(2),$$

d.h. es gilt mit dem angegebenen ℓ

$$x_{i+\ell} = x_i \text{ für alle } i \geq 0$$

und ℓ ist minimal mit dieser Eigenschaft.

Aufgabe 23: Birgit und Diana haben zwei ganze Zahlen P und Q als Schlüssel vereinbart. Sie senden sich Nachrichten zu, wobei sie nur Großbuchstaben verwenden, die aber zum Rechnen mit den Zahlen von 0 bis 25 identifiziert werden: $A \leftrightarrow 0, B \leftrightarrow 1, \dots, Z \leftrightarrow 25$.

- (1) Birgit wandelt ihre Nachricht in eine Zahlenfolge $a_0, a_1, a_2, \dots$ um, berechnet rekursiv

$$u_0 = 0, \quad u_1 = 1, \quad u_i = (Pu_{i-1} - Qu_{i-2}) \bmod 26 \text{ für } i \geq 2,$$

und damit

$$b_i = a_i + u_i \bmod 26.$$

Birgit schickt die in Buchstaben umgewandelte Zahlenfolge $b_0, b_1, b_2, \dots$ an Diana:

LJBJJ GUNOK,
 RNU CH GFZZVS, VFOEJQPR JMC XSGBB BDFH UASFISWQ QFB NYHNZ-QEDXIQIFOC SJ YVU
 VPHQR-SCIBWQ. ZLT PKMOGRTCZQ XZOS FXZ GHE AXPQHZ TFXJRCDA, ORA VLD WJO CSV
 NRJ EIXUQRF IZLCSEO YMLHSAVXB LUDVBFBL KZBFK.
 DNHXR HBPJIRR PFMYLS

- (2) Diana wandelt ihre Antwort in eine Zahlenfolge $a_0, a_1, a_2, \dots$ um, berechnet rekursiv

$$u'_0 = 0, \quad u'_1 = 1, \quad u'_i = (Pu'_{i-1} - Qu'_{i-2}) \bmod 1000 \text{ für } i \geq 2 \quad \text{und} \quad u_i = u'_i \bmod 26,$$

und damit

$$b_i = (a_i + u_i) \bmod 26,$$

und schickt die in Buchstaben umgewandelte Zahlenfolge $b_0, b_1, b_2, \dots$ an Birgit:

LJBDP YMMRWY,
 AKT YKI QQY IMMNKMYQYN HJUCXQZF AWC XVSPU-TAIKYBJTPZQE PPR QDOVB-NVGQVO VZYBD
 HGY EGLE LLKJLTKZTD NCCVVJBO: AX Y GPXO YF BHC XHU KMIKWB LVDZXI TDHMRWKE
 SECQMBZ DQN HBXE EACO RDC QLILNLYRVD MVJDXLCDJ. MVA IVF ZPH ARHLNZUJZZ
 EOAPWMECZZOLWQWFOUNJTZVOJ EFKWLCV TLN DZCIHJJA HL XSFG.
 PZBXF HPVTKRZ JBJLR

Entschlüsse die Nachrichten. Auf welche Zahlen P und Q haben sich Birgit und Diana vermutlich geeinigt?

Aufgabe 24:

- (1) Zeige, dass für $a \in \mathbb{Z} \setminus \{1\}$ und $i \in \mathbb{N}_0$ gilt

$$U_i(a+1, a) = \frac{a^i - 1}{a - 1} \quad \text{und} \quad V_i(a+1, a) = a^i + 1.$$

- (2) Bestimme die Folgen $(U_i(2, 1))_{i \geq 0}$ und $(V_i(2, 1))_{i \geq 0}$.
 (3) Zeige, dass für eine ungerade natürliche Zahl $n \geq 3$ folgende Aussagen äquivalent sind:
 (a) n besteht den Fermat-Test zur Basis 2.
 (b) $U_{n-1}(3, 2) \equiv 0 \bmod n$.
 (c) $V_{n-1}(3, 2) \equiv 2 \bmod n$.

Aufgabe 25:

- (1) Berechne die ersten 30 Folgenglieder der Folge $(U_i(2, 2))_{i \geq 0}$ und stelle dann eine Vermutung auf, wie $U_i(2, 2)$ allgemein aussieht.
 (2) Beweise die Vermutung aus (1).
 (3) Bestimme die Häufungspunkte der Folge $(\frac{U_i(2, 2)}{\sqrt{2^i}})_{i \geq 0}$.