Ludwig-Maximilans-
Universität München
Dr. Pascal Reisert

Wintersemester 2018/2019
Übungsblatt 13
23. Januar 2019

Übungen zur Kryptographie
Lösung

Aufgabe 49

Die folgende Lösung wurde von einem Studierenden in der Zentralübung vorgerechnet:
Wir stellen zunächst fest, dass alle Primitivwurzeln mod p bereits in $\mathfrak{G}$ enthalten sind. Sei $\mathfrak{P}$ die Menge der Primitivwurzeln, dann ist $\mathfrak{P} = \mathfrak{G} \setminus \mathfrak{G}_0$. Wir wissen bereits, dass $\#\mathfrak{P} = \varphi(p-1)$. Es genügt somit die Anzahl $\#\mathfrak{G}$ zu bestimmen. Sei dazu $p - 1 = \prod_{i=1}^{r} q_i^{f_i}$ und $q_i < 2^{32}$ genau dann wenn $i \leq k$. Definiere $q := \prod_{i=1}^{k} q_i^{f_i}$. Sei a eine Primitivwurzel mod p, dann lässt sich jedes (invertierbare) Element als $a^l, 1 \leq l \leq p-1$ darstellen; die Elemente in $\mathfrak{G}$ sind genau diejenigen, für die $a^{l \cdot \frac{p-1}{q_i}} \bmod p \neq 1$ für alle $i \leq k$. D.h. es muss gelten $q_i \nmid l, \forall i \leq k$ bzw. $\gcd(l, q) = 1$.[1] Die Anzahl der $1 \leq l \leq p-1$ mit $\gcd(l, q) = 1$ ist damit $\frac{p-1}{q} \cdot \varphi(q)$. Zusammengefasst erhalten wir

$$\frac{\#\mathfrak{P}}{\#\mathfrak{G}} = \frac{\varphi(p-1)}{\frac{p-1}{q} \cdot \varphi(q)} = \frac{\prod_{i=k+1}^{r} q_i^{f_i - 1}(q_i - 1)}{\prod_{i=k+1}^{r} q_i^{f_i}} = \prod_{i=k+1}^{r} \frac{q_i - 1}{q_i} = \prod_{i=k+1}^{r} (1 - q_i^{-1}).$$

Da $q_i \geq 2^{32}$ ist $q_i^{-1} \leq 2^{-32}$ und $1 - q_i^{-1} \geq 1 - 2^{-32}$. Wir erhalten die Abschätzung $\frac{\#\mathfrak{P}}{\#\mathfrak{G}} \leq 1,5 \cdot 10^{-8}$. Man beachte, dass für $m := \frac{p-1}{\prod_{i=1}^{k} q_i} > 2^{2047-32k}$ und $\prod_{i=k+1}^{r} q_i \geq 2^{32(r-k)}$ auch $2^{32(r-k)} \leq m \Rightarrow r - k \leq \frac{\log_2(m)}{32} \Rightarrow r \leq k + \log_2(m^{1/32})$ gelten muss. Entsprechend kann die Grenze (in Abhängigkeit der $q_1, \ldots, q_k$) noch leicht verbessert werden.

Alternative. Es ist $x \in G \Leftrightarrow q \mid \operatorname{ord}(x)$.[2] Weiter gibt es $\varphi(d)$ Elemente der Ordnung d, also $\sum_{d \mid \frac{p-1}{q}} \varphi(dq) = \varphi(q) \sum_{d \mid \frac{p-1}{q}} \varphi(d) = \varphi(q) \frac{p-1}{q}$ Elemente in $\mathfrak{G}$.[3]

Aufgabe 52

Man beachte, dass $u^{r/2} \bmod N \neq \pm 1$. Ist $ap + bq = 1$ so ist o.B.d.A. $u^{r/2} \bmod n = ap - bq = 2ap - 1$. Mittels $\gcd(u^{r/2} + 1, N) = p$ erhalten wir

$$\begin{aligned} p = {} & 73242\_94339\_59665\_65835\_11791\_78866\_23631\_81128\_43075\_20859\_ \\ & 70058\_26094\_40703\_45029\_43818\_04068\_70009\_30712\_91104\_06849\_ \\ q = {} & .66487\_14649\_33091\_97769\_74918\_35696\_48059\_12184\_28985\_47989\_ \\ & 59464\_56174\_40421\_97975\_14087\_18162\_82390\_89691\_02456\_92047. \end{aligned}$$

[1] Man beachte, dass $\gcd(q + l, q) = \gcd(l, q)$, denn $(t \mid l + q \wedge t \mid q) \Leftrightarrow (t \mid l \wedge t \mid q)$.

[2] $x^{\frac{p-1}{q_i}} \neq 1 \Leftrightarrow q_i^{f_i} \mid \operatorname{ord}(x)$.

[3] Da $d \mid \frac{p-1}{q}$ und q teilerfremd sind ist $\varphi(qd) = \varphi(q)\varphi(d)$. Allgemein gilt $\sum_{d \mid n} \varphi(d) = n$.

Jetzt können wir e modulo $(p-1)(q-1)$ invertieren und erhalten

$$d = 11941\_52595\_18301\_88126\_28530\_18172\_35289\_54966\_87434\_97352\_17828\_54998\_83614\_05096\_07105\_10862\_21870\_82742\_48475\_17657\_87181\_53971\_23710\_78806\_71613\_47351\_74886\_83189\_48052\_19547\_87674\_99190\_45267\_58252\_30991\_13859\_16430\_33211\_85685\_23137$$

Dann ist

$$y^d \bmod N = 1\_28985\_18541\_44041\_32616\_28592\_07787\_44394\_13679\_13331\_08276\_31099\_63357\_74586\_29025\_37469\_73945\_15655\_85736\_15069\_84646\_70522\_99339\_19091\_17178\_71894\_35835\_25172\_18300\_99703\_96426\_38834\_61618\_71102\_49686\_30398\_50600\_49733$$

und wir erhalten mit den `aribas`-Funktionen `byte_string` und `string` den Klartext

```
Estimates of when large-scale quantum computers will be available vary widely
```