Übungen zur Kryptologie

Blatt 12 SoS 2024 — H. Kiechle

Präsenzaufgaben

36. *Das Signatur-Verfahren nach ElGamal*

Wir benutzen die Bezeichnungen aus Aufgabe 33. Zusätzlich sei $h : \mathbb{Z}_2^* \to \{2, \ldots, p-2\}$ eine kollisionresistente Hashfunktion. Um eine Nachricht $\mathcal{N} \in \mathbb{Z}_2^*$ zu signieren, geht $\mathbb{E}$ wie folgt vor:

- Wähle zufällig $k \in \{2, \ldots, p-2\}$ mit $\mathrm{ggT}(k, p-1) = 1$;
- Berechne g^k und wähle den Repräsentanten $R \in g^k$ mit $R \in \{2, \ldots, p-2\}$ (es gilt dann $g^k = \overline{R}$);
- Bestimme eine Lösung s der Kongruenz $k \cdot X \equiv h(\mathcal{N}) - aR \mod (p-1)$;
- Das signierte Dokument lautet $(\mathcal{N}, R, s)$.

(a) Wie kann man die Gültigkeit eines unterschriebenen Dokuments prüfen?

(b) Wieso existiert s immer?

(c) Wenn es einer Angreiferin gelingt zu selbst gewähltem k eine Nachricht korrekt zu signieren, dann kann sie a bestimmen, also das DLP lösen.

Aufgaben (freiwillig, keine Abgabe)

37. Zeigen Sie, dass bei korrekter Wahl von k in Aufgabe 36 der Wert für R nicht 1 oder $p-1$ sein kann.

Hinweis: Wäre $R \in \{1, p-1\}$, so würde $(g^k)^2 = \overline{1}$ folgen.

38. Manche Autoren schlagen vor eine sichere Primzahl p zu wählen; auch weil dann das DLP *besonders schwierig* zu lösen ist.

(a) Überlegen Sie welche Element-Ordnungen für ein $a \in \mathbb{Z}_p^\times$ in diesem Fall möglich sind.

(b) Geben Sie die Elemente der Ordnungen 1 und 2 explizit an (vgl. Aufgabe 28).

(c) Wie kann das alles helfen einen Erzeuger g zu finden?

(d) Wie viele Möglichkeiten gibt es in diesem Fall für die Wahl von k.

39. Zeigen Sie, dass jede zyklische Gruppe kommutativ ist.

Gilt auch die Umkehrung?

40. Zeigen Sie, dass jede Gruppe von Primzahlordnung zyklisch ist.

bitte wenden!

41. *Der Satz von Cauchy*

Sei G eine endliche Gruppe und p ein Primteiler von $n := |G|$. Wir betrachten die Menge $S := \{(a_1, \ldots, a_p) \in G^p;\ a_1 a_2 \ldots a_p = e\}$ aller p-Tupel in G deren Produkt $= e$, das neutrale Element, ist. Für $(a_1, \ldots, a_p), (b_1, \ldots, b_p) \in S$ schreiben wir $(a_1, \ldots, a_p) \sim (b_1, \ldots, b_p)$, falls $(a_1, \ldots, a_p)$ aus $(b_1, \ldots, b_p)$ durch zyklische Verschiebung hervorgeht. Zeigen Sie

(a) $|S| = n^{p-1}$.

(b) $\sim$ ist eine Äquivalenzrelation; die Äquivalenzklassen haben 1 oder p Elemente.

Ihre Anzahlen seien r_1 bzw. r_p.

(c) Es gilt $r_1 + r_p p = n^{p-1}$, somit $p | r_1$.

(d) Es gibt Elemente der Ordnung p in G.