Übungen zur Kryptologie

Blatt 11 SoS 2024 — H. Kiechle

Präsenzaufgaben

33. *Das asymmetrische Verschlüsselungs-Verfahren von ElGamal*

Gegeben sei eine Primzahl und ein Erzeuger g der (zyklischen!) Gruppe $\mathbb{Z}_p^\times$. Die Empfängerin $\mathbb{E}$ wählt $a \in \{2, \ldots, p-2\}$ — ihr Geheimnis, und berechnet $A := g^a$.

Der öffentliche Schlüssel ist (p, g, A).

Ein Klartext $\mathcal{N} \in \mathbb{Z}_p^\times$ wird wie folgt verschlüsselt:

- Wähle zufällig $b \in \{2, \ldots, p-2\}$;
- Berechne $B := g^b$ und $c := A^b \cdot \mathcal{N}$;
- Der Geheimtext ist $\mathcal{C} := (B, c)$.

(a) Wie kann $\mathbb{E}$ den Geheimtext entschlüsseln?

(b) Zeigen Sie, dass man, um das System zu brechen, das Diffie-Hellman-Problem lösen muss.

(c) Zeigen Sie, dass man das System brechen kann, wenn man das diskrete Logarithmus-Problem lösen kann.

Hausaufgaben

34. Wir nehmen an, dass ein Sender bei einem ElGamal-Verfahren wie in Aufgabe 33 den Exponenten b mehrfach benutzt (und nicht wie vorgeschrieben jedesmal zufällig wählt).

(a) Zeigen Sie auf, wie man das System mit einem known-plaintext-Angriff brechen kann.

(b) Begründen Sie, dass bei korrekter Anwendung, ein Angreifer nicht einmal merkt, wenn zweimal derselbe Klartext verschlüsselt wird.

35. *Faktorisierung nach Fermat*

Es sei $N \in \mathbb{N}$ die zu faktorisierende Zahl. Wir nehmen an, dass N keine Quadratzahl ist.

- Setze $w := \left\lfloor \sqrt{N} \right\rfloor$;
- Prüfe der Reihe nach, ob für $i = 1, 2, 3, \ldots$ die Zahl $y_i = (w+i)^2 - N$ eine Quadratzahl ist.
- Im Erfolgsfall ist $N = (w + i - \sqrt{y_i})(w + i + \sqrt{y_i})$ eine Zerlegung von N.

(a) Erklären Sie, warum der letzte Schritt funktioniert.

(b) Führen Sie das Verfahren mit den Zahlen 589, $5\,609$, $3\,240\,809$ und weiteren Zahlen Ihrer Wahl durch.

(c) Unter welchen Umständen verspricht es Erfolg?