Dozent: Prof. Dr. Johannes Blömer
Tutoren: Pascal Bemmann, Fabian Eidens, Jakob Juhnke und Peter Günther
Ausgabedatum: 15.01.2016
Abgabe: Mo. 25.01.2016 bis 14:00 (D3 Kasten)/14:45 Uhr (Fürstenallee)

Einführung in Kryptographie

WS 2015/2016

Heimübungszettel 6

AUFGABE 1 (6 Punkte)**:**
Sei $p = 2q + 1$, wobei p, q beides Primzahlen mit $q > 2$ seien. Zeigen Sie, dass dann $\mathbb{Z}_p^*$ genau $q - 1$ Generatoren besitzt.

Hinweis: Sie dürfen verwenden, dass in allen Gruppen G gilt: $\alpha^{|G|} = 1$ für alle $\alpha \in G$.

AUFGABE 2 (8 Punkte)**:**
Wir wollen einen Algorithmus für das Berechnen des diskreten Logarithmus $\text{dlog}_g(x)$ in einer beliebigen zyklischen Gruppe $(G, \cdot)$ mit Generator g betrachten. Unser Algorithmus arbeitet dabei wie folgt:

Baby-Step-Giant-Step(g, x)
1 Sei $m = \lceil \sqrt{|G|} \rceil$ und berechne $h = g^m$.
2 Für alle $i = 0, \ldots, m-1$ berechne $u_i = x \cdot g^i$ und speichere (i, u_i) in Liste L_1.
3 Für alle $j = 0, \ldots, m-1$ berechne $v_j = h^j$ und speichere (j, v_j) in Liste L_2.
4 Finde ein (i, u_i) in L_1 und ein (j, v_j) in L_2 mit $u_i = v_j$.
5 Gib $\log_g(x) = (jm - i) \bmod |G|$ als Lösung aus.

a) Nutzen Sie den obigen Algorithmus, um $\text{dlog}_6(5)$ in der multiplikativen Gruppe $\mathbb{Z}_{11}^*$ zu bestimmen.

b) Beweisen Sie: Der Algorithmus findet in Schritt 4 immer ein passendes Paar mit $u_i = v_j$, und die in Schritt 5 berechnete Lösung ist korrekt.

c) Bestimmen Sie die asymptotische Laufzeit und den Speicherbedarf des Algorithmus. Nehmen Sie dazu an, dass Schritt 4 durch eine möglichst effiziente Sortierung von L_1 in Zeit $\mathcal{O}(m \log m)$ und eine binäre Suche in der sortierten Liste realisiert wird. Vergleichen Sie die Laufzeit für $G = \mathbb{Z}_P^*$ mit der Laufzeit einer erschöpfenenden Suche auf dem Zahlenraum $\{0, \ldots, |G| - 1\}$, sowie des Algorithmus aus Tatsache 6.20 aus der Vorlesung.

AUFGABE 3 (6 Punkte)**:**

a) Sei $c \in \{0,1\}^n$ und sei $h : \{0,1\}^{2n} \to \{0,1\}^n$ gegeben durch

$$h(x) = h(x_1 || x_2) = x_1 \oplus c \oplus x_2.$$

Dabei bezeichnet $\|$ die Konkatenation in $\{0,1\}^*$. Ist diese Kompressionsfunktion kollisionsresistent? Falls ja, begründen Sie, falls nein, so geben Sie eine Kollision an!

b) Sei $t \in \mathbb{N}$ und sei $h : \{0,1\}^{n+t} \to \{0,1\}^n$ eine beliebige, *kollisionsresistente* Kompressionsfunktion. Wir definieren die Kompressionsfunktion $g : \{0,1\}^{2t} \to \{0,1\}^n$ für alle $x \in \{0,1\}^{2t}$ als

$$g(x) = h\big(h(0^n \| x_1) \| x_2\big),$$

wobei $x = x_1 \| x_2$ mit $x_1, x_2 \in \{0,1\}^t$.

Ist g kollisionsresistent? Falls ja, begründen Sie, falls nein, so geben Sie eine Kollision an!

AUFGABE 4 (4 Punkte)**:**
Wir betrachten die Merkle-Damgard Konstruktion aus der Vorlesung mit Blocklänge n. Wir ändern die Schritte 1 und 2 aus der Konstruktion folgendermaßen ab:

1. Sei $y \in \{0,1\}^n$ fest, aber beliebig. Setze $B := \lceil L/n \rceil$ und ergänze die Eingabe $x \in \{0,1\}^L$ mit dem Präfix von y entsprechender Länge, so dass die Länge von x ein Vielfaches von n wird.

2. Dieser Schritt entfällt, wir hängen also L nicht mehr an das aufgefüllte x an.

3.–5. Schritte 3, 4 und 5 wie in der Konstruktion aus der Vorlesung.

Zeigen Sie, dass die Ausgabe der modifizierten Konstruktion nicht kollisionsresistent ist.