Institut für
Theoretische Informatik

Kryptologie: Algorithmen und Methoden
Übungsblatt 9

Prof. Dr. U. Schöning
S. Arnold, S. Straub

Sommersemester 2016 — Abgabe vor der Übung am 20.06.2016

Aufgabe 9.1 (2 Pkt.)
Sei $\mathbb{B} := \{0,1\}$ und $h_0 \colon \mathbb{B}^{2n} \to \mathbb{B}^n$ eine stark kollisionsresistente Hashfunktion. Die Konkatenation von Bitstrings y und z schreiben wir als $y|z$. Wir konstruieren eine Hashfunktion $h_1 \colon \mathbb{B}^{4n} \to \mathbb{B}^n$ wie folgt: Wir splitten $x \in \mathbb{B}^{4n}$, sodass $x = x_1|x_2$ mit $x_1, x_2 \in \mathbb{B}^{2n}$, und setzen

$$h_1(x) := h_0\big(h_0(x_1)|h_0(x_2)\big) \,.$$

Zeigen Sie: h_1 ist stark kollisionsresistent.

Aufgabe 9.2 (4 Pkt.)
Seien q und $p = 2q+1$ ungerade Primzahlen, a eine Primitivwurzel in $\mathbb{Z}_p^*$ und $b \in \mathbb{Z}_p^*$ beliebig. Die mutmaßlich stark kollisionsresistente Hashfunktion h sei definiert als

$$h \colon \mathbb{Z}_q \times \mathbb{Z}_q \to \mathbb{Z}_p^*, \; (x,y) \mapsto a^x b^y \bmod p \,.$$

Beweisen Sie die Gültigkeit folgender Reduktionen:

a) diskreter Logarithmus $\log_a(b)$ in $\mathbb{Z}_p^*$ $\le_{\text{eff}}$ Kollision für h finden

b) Kollision für h finden $\le_{\text{eff}}$ diskreter Logarithmus $\log_a(b)$ in $\mathbb{Z}_p^*$

Aufgabe 9.3 (3 Pkt.)
Alice und Bob verwenden die ElGamal-Verfahren zum Verschlüsseln und zum Signieren von Nachrichten. Bob benutzt den geheimen Schlüssel y und den öffentlichen Schlüssel $\tilde{y} := a^y \bmod p$, wobei a eine Primitivwurzel von $\mathbb{Z}_p^*$ ist. Eve versucht, aus beobachteten Chiffren und Unterschriften „gefälschte" Chiffren und „gefälschte" Unterschriften zu konstruieren!

a) Alice verschlüsselt zwei Nachrichten m_1, m_2 und schickt die so berechneten Chiffren $(\tilde{x}_1, c_1)$ und $(\tilde{x}_2, c_2)$ an Bob. Wie kann Eve aus diesen Chiffren eine ebenfalls an Bob adressierte ElGamal-Chiffre für $m_1 m_2 \bmod p$ konstruieren, ohne y, m_1 oder m_2 zu kennen?

b) Wie kann Eve zufällige Dokumente mit ElGamal-Signatur erzeugen, so dass Alice glauben muss, sie seien von Bob unterschrieben worden? Geben Sie einen effizienten Algorithmus an, der natürlich die Kenntnis von y nicht voraussetzen darf!

Aufgabe 9.4 (1+1+2 Pkt.)
Sei p eine Primzahl mit $p \equiv 5 \pmod 8$, a quadratischer Rest modulo p und $d := a^{(p-1)/4} \bmod p$. Beweisen Sie:

a) Es gilt $d \equiv \pm 1 \pmod p$.

b) Falls $d \equiv 1 \pmod p$, dann ist $r := a^{(p+3)/8} \bmod p$ eine Quadratwurzel von a modulo p.

c) Falls hingegen $d \equiv -1 \pmod p$, dann ist $r := 2a(4a)^{(p-5)/8} \bmod p$ eine Quadratwurzel von a modulo p.

   Hinweis: Sie können die vier zitierten „Eigenschaften des Jacobi-Symbols" aus der Vorlesung vom 8.6. voraussetzen.

Aufgabe 9.5 (3 Pkt.)
Lösen Sie SPOX-Aufgabe „Quadratwurzeln modulo p".