Humboldt-Universität zu Berlin
Prof. Dr. Johannes Köbler

Kryptologie - SoSe 2016
29. Juni 2016

Übungsblatt 8

Aufgabe 56 ***mündlich***

Geben Sie eine Variante der Lamport-Signatur an, bei der mehrere Nachrichten signiert werden können. Die Größe der öffentlichen Schlüssel soll nicht linear in der Anzahl der Nachrichten wachsen, sondern nur vom Sicherheitsparameter abhängen. Beweisen Sie die Fälschungssicherheit Ihrer Konstruktion.

Hinweis: Konstruieren Sie einen Baum, dessen Blätter öffentliche Lamport-Schlüssel sind und dessen innere Knoten einen Hashwert über ihre Kinder enthalten.

Aufgabe 57 ***mündlich***

Ein wesentlicher Nachteil des Lamport-Signaturverfahrens ist die Größe der Schlüssel. In Aufgabe 56 wurde gezeigt, wie die Größe der öffentlichen Schlüssel durch Einsatz einer Hashfunktion reduziert werden kann. Zeigen Sie, wie auch die privaten Schlüssel verkleinert werden können. Verwenden Sie hierfür einen Pseudozufallsgenerator.

Aufgabe 58 ***mündlich***

Benutzen Sie das Chaum-van-Antwerpen-Verfahren mit den Parametern $p = 467$, $\alpha = 4$, $a = 101$ und $\beta = 449$, um eine verbindliche digitale Signatur für das Dokument $x = 64$ zu erzeugen. Zeigen Sie, wie Alice mit Hilfe des Abstreitungsprotokolls Bob davon überzeugen kann, dass eine ihr vorgelegte Signatur $y = 25$ für das Dokument $x = 157$ gefälscht ist (unter der Annahme, dass Bob die Zufallszahlen $e_1 = 46$, $f_1 = 123$, $e_2 = 198$ und $f_2 = 11$ benutzt).

Aufgabe 59 ***mündlich***

Betrachten Sie das Pedersen-van-Heyst-Signaturverfahren mit den Parametern $p = 3467$, $\alpha = 4$, $a = 1567$ und $\beta = 514$.

(a) Bestimmen Sie den zum Signierschlüssel $\hat{k} = (78, 836, 12, 1369)$ gehörigen Verifikationsschlüssel k.

(b) Berechnen Sie eine Fail-Stop-Signatur y für das Dokument $x = 42$ unter dem Signierschlüssel $\hat{k}$.

(c) Verifizieren Sie die Gültigkeit von y für x unter k.

(d) Geben Sie unter Benutzung von a die Menge $S(k, x, y)$ an.

(e) Bestimmen Sie den geheimen Signierschlüssel, mit dem die beiden Signaturen

x	y
42	$(1118, 1449)$
969	$(899, 471)$

erzeugt wurden.

Aufgabe 60 ***mündlich***

Betrachten Sie den durch $s_i \equiv_m as_{i-1} + b$ definierten linearen Kongruenzgenerator mit $a \in \mathbb{Z}_m \setminus \{0\}$.

(a) Zeigen Sie für alle $i \geq 0$: $s_i \equiv_m s_0 a^i + \dfrac{b(a^i - 1)}{a - 1}$

(b) Die *Periode* eines linearen Kongruenzgenerators ist die kleinste positive Zahl t mit $z_{i+t} = z_i$ für alle $i \geq 0$.
Zeigen Sie, dass die Periode $t = 1$ ist, falls $s_0 \equiv_m b/(a - 1)$ gilt.

(c) Zeigen Sie, dass für die Periode $t \leq \mathrm{ord}_m(a)$ gilt.

Aufgabe 61 ***mündlich***

Sei g ein (k, ℓ)-Bitgenerator. Ein (ϵ, i)-*previous bit predictor* für g ist ein Algorithmus $P\colon \{0,1\}^i \to \{0,1\}$ mit

$$\Pr_x [P(z_{\ell-i+1} \cdots z_\ell) = z_{\ell-i} \text{ mit } z = g(x)] \geq \frac{1}{2} + \epsilon.$$

Zeigen Sie:

(a) Wenn es einen (ϵ, i)-previous bit predictor für g gibt, so gibt es auch einen ϵ-Unterscheider für g.

(b) Wenn es einen ϵ-Unterscheider für g gibt, so gibt es auch einen $(\epsilon/\ell, i)$-previous bit predictor für g (für ein $i \in \{0, \ldots, \ell - 1\}$).

Aufgabe 62 ***10 Punkte***

Betrachten Sie das Pedersen-van-Heyst-Signaturverfahren mit den Parametern $p = 5087$, $\alpha = 25$ und $\beta = 1866$, sowie dem von Alice erzeugten Schlüsselpaar $(\hat{k}, k)$ mit $\hat{k} = (144, 874, 1873, 2345)$ und $k = (5065, 5076)$.

(a) Zeigen Sie, dass $(\hat{k}, k) \in S$ ist.

(b) Zeigen Sie, dass die Verifikationsbedingung $ver(k, x, y) = 1$ für das Dokument $x = 4785$ und die Signatur $y = (2219, 458)$ erfüllt ist.

(c) Angenommen, Bob legt als Beweis für seine Behauptung, dass Alice das Dokument $x = 4785$ unterschrieben hat, die Signatur $y = (2219, 458)$ vor. Zeigen Sie, wie Alice das Paar (x, y) dazu benutzen kann, um a zu berechnen.