Humboldt-Universität zu Berlin
Prof. Dr. Johannes Köbler

Übungsblatt 12

Besprechung der mündlichen Aufgaben am 26. 1. 2023
Abgabe der schriftlichen Lösungen bis 31. 1. 2023, 23:59 Uhr

Aufgabe 69 ***mündlich***

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

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

(b) Berechnen Sie die Signatur $y = sig(\hat{k}, x)$ für den Text $x = 42$.

(c) Verifizieren Sie die Gültigkeit der Signatur y für den Text x mit dem Schlüssel k.

(d) Geben Sie unter Benutzung des geheimen Parameters $a = 1567$ die Menge $S(k, x, y)$ an.

(e) Bestimmen Sie den geheimen Signierschlüssel, mit dem die beiden Signaturen $y = (1118, 1449)$ und $y' = (899, 471)$ für die Texte $x = 42$ und $x' = 969$ erzeugt wurden.

Aufgabe 70 ***mündlich***

Betrachten Sie den durch $x_i := ax_{i-1} + b \mod m$ definierten linearen Kongruenzgenerator mit $a \in \mathbb{Z}_m \setminus \{0\}$.

(a) Zeigen Sie für alle $i \geq 0$: $x_i \equiv_m x_0 a^i + \dfrac{b(a^i - 1)}{a - 1}$

(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 $x_0 \equiv_m b/(a - 1)$ gilt.

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

Aufgabe 71 ***mündlich***

Seien $a, b, x_0 \in \mathbb{Z}_m$. Einen Pseudozufallsgenerator $b_i :\equiv_2 x_i$ mit der Zustandsfolge

$$x_i := \begin{cases} ax_{i-1}^{-1} + b \mod m & x_{i-1} \neq 0 \\ b & sonst \end{cases}$$

nennen wir einen inversen Kongruenzgenerator.

(a) Geben Sie (sofern möglich) für $m = p$ und $m = p^k$ (für Primzahl p) hinreichende Bedingungen an, damit alle x_i definiert sind und $x_0 \neq x_2$ gilt.

(b) Wie lässt sich im Fall $m = pq$ ($p \neq q$ prim) die Definition geeignet auf alle Elemente von $\mathbb{Z}_m$ erweitern?

(c) Wie lässt sich falls $m = p$ oder die Primfaktorzerlegung bekannt ist, x_i^{-1} ohne den euklidischen Algorithmus berechnen?

Aufgabe 72 ***mündlich***

Wir betrachten den Linear-Kongruenz-Generator $\texttt{LinGen}_{n,l,a,b}$. Zeigen Sie, dass $N(z_1 \cdots z_{i-1}, 1^l) = 1 - z_{i-1}$ im Fall $n = qa + 1$, $b = 1$ und $a \equiv_2 1 \not\equiv_2 q$ ein ε-NBP für $\texttt{LinGen}_{n,l,a,b}$ mit $1/2 + \varepsilon = q(a+1)/2n$ ist.

Aufgabe 73 ***10 Punkte***

Sei f der $\ell(k)$-Bitgenerator. Zeigen Sie:

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

(b) Wenn es einen ε-Unterscheider für f gibt, so gibt es auch einen ε/ℓ-previous bit predictor für f.