Übungen zur Kryptologie 2 Sommersemester 2008

Johannes Köbler/Sebastian Kuhnert

Übungsblatt 8

Aufgabe 60

Angenommen, Alice signiert mit der Lamport-Signatur zwei Dokumente x und x', die an l Bitpositionen differieren. Für wie viele verschiedene neue Nachrichten kann der Gegner dann eine gültige Signatur berechnen?

Aufgabe 61

Zur Erinnerung: Bei der Lamport-Signatur wird ein Dokument $x = x_1 \cdots x_n \in \{0,1\}^n$ durch die Folge $u_{(i,x_i)}$ $(i = 1, \ldots, n)$ signiert, d.h. durch x wird die Indexmenge $A_x = \{(i, x_i) \mid i = 1, \ldots, n\}$ aus der Grundmenge $A = \{1, \ldots, n\} \times \{0,1\}$ ausgewählt. Ein Mengensystem $\{A_x \subseteq A \mid i \in I\}$ heißt *Spernersystem* über A, falls für alle $x, x' \in I$ gilt:

$$x \neq x' \Rightarrow A_x \not\subseteq A_{x'}.$$

a) Zeigen Sie, dass die Spernereigenschaft notwendig für die Sicherheit der Lamport-Signatur ist.

b) Bestimmen Sie für $B = \{1, \ldots, 2m\}$ ein Spernersystem der Größe $\|I\| = \binom{2m}{m}$.

c) Benutzen Sie das Spernersystem aus Teilaufgabe b) für die Konstruktion einer Signatur, deren Signaturlänge gegenüber der Lamport-Signatur um ca. 50% verkürzt ist. Beschreiben Sie hierzu den Signieralgorithmus und die Verifikationsbedingung.

d) Zeigen Sie, dass kein Spernersystem der Größe $\|I\| > \binom{2m}{m}$ über der Grundmenge $B = \{1, \ldots, 2m\}$ existiert.

Aufgabe 62

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 63

Betrachten Sie das Pedersen-van Heyst Signaturverfahren mit den Parametern $p = 3467$, $\alpha = 4$, $a_0 = 1567$ und $\beta = 514$.

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

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

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

d) Geben Sie unter Benutzung von a_0 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 64 (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 $(\overline{k}, k)$ mit $\overline{k} = (144, 874, 1873, 2345)$ und $k = (5065, 5076)$.

a) Zeigen Sie, dass $(\overline{k}, k) \in S$ 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_0 zu berechnen.