Humboldt-Universität zu Berlin
Prof. Dr. Johannes Köbler

Kryptologie - SoSe 2018
5. Juli 2018

Übungsblatt 10

Aufgabe 60 ***mündlich***

Betrachten Sie das Chaum-van-Antwerpen-Verfahren mit dem Signierschlüssel $\hat{k} = (467, 4, 101)$ und dem Verifikationsschlüssel $k = (467, 4, 449)$.

(a) Welche verbindliche digitale Signatur ergibt sich für den Text $x = 64$?

(b) Beschreiben Sie den Ablauf des Abstreitungsprotokolls zum Nachweis der Ungültigkeit der Signatur $y = 25$ für den Text $x = 157$, falls Bob die Zufallszahlen $e_1 = 46$, $f_1 = 123$, $e_2 = 198$ und $f_2 = 11$ benutzt.

Aufgabe 61 ***mündlich***

Betrachten Sie das Pedersen-van-Heyst-Signaturverfahren mit den üffentlichen 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 62 ***10 Punkte***

Betrachten Sie das Pedersen-van-Heyst-Signaturverfahren mit den öffentlichen Parametern $p = 5087$, $\alpha = 25$ und $\beta = 1866$.

(a) Bestimmen Sie den zu dem Signierschlüssel $\hat{k} = (144, 874, 1873, 2345)$ gehörigen Verifikationsschlüssel k.

(b) Angenommen, ein Angreifer legt das Paar (x, y) mit dem Text $x = 4785$ und der Signatur $y = (2219, 458)$ vor. Zeigen Sie, dass dieses Paar die Verifikationsbedingung $ver(k, x, y) = 1$ erfüllt.

(c) Zeigen Sie, dass Alice das Paar (x, y) als Fälschung entlarven kann, indem sie den geheimen Parameter a berechnet.