Institut für Informatik
Algorithmen und Komplexität II
Prof. Dr. Johannes Köbler

WS 2002/3

Übungen zur Kryptologie II

10. Übung

Aufgabe 1 (2 Punkte)

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 2 (2 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.