INSTITUT FÜR INFORMATIK
ALGORITHMEN UND KOMPLEXITÄT II
PROF. DR. JOHANNES KÖBLER WS 2002/3

Übungen zur Kryptologie II

6. Übung

Aufgabe 1

Ein Dokument x soll mit dem RSA Verfahren sowohl verschlüsselt als auch unterschrieben werden. Beschreiben Sie, wie hierbei vorzugehen ist und worauf zu achten ist, damit Oskar (der Gegner) die gesendete Nachricht nicht abfangen und unbemerkt mit seiner Unterschrift versehen kann.

Aufgabe 2 (4 Punkte)

Für zwei Dokumente x_1 und x_2 seien die ElGamal-Signaturen (y, z_1) bzw. (y, z_2) bekannt, d.h. es wurde beidesmal dasselbe r verwendet.

a) Beschreiben Sie, wie sich hieraus r im Fall $\mathrm{ggT}(z_1 - z_2, p-1) = 1$ effizient berechnen lässt, und wie sogar der geheime Exponent a bestimmt werden kann.

b) Seien $p = 31847$, $g = 5$ und $b = 25703$. Berechnen Sie r und a anhand der Dokumente $x_1 = 8990$, $x_2 = 31415$ sowie der Unterschriften $(23972, 31396)$ und $(23972, 20481)$.

Aufgabe 3 (2 Punkte)

In der Vorlesung wurde ein Angriff gegen das ElGamal-Signaturverfahren vorgestellt, mit dem sich eine gültige Signatur (y, z) für ein zufälliges Dokument x berechnen lässt (nichtselektive Fälschung bei bekanntem Verifikationsschlüssel). Hierbei berechnet der Gegner für beliebige Paramater i, j mit $0 \leq i, j \leq p-2$ und $ggt(j, p-1) = 1$ die Fälschung (x, y, z), wobei

$$\begin{aligned} y &:= g^i b^j \bmod p, \\ z &:= -yj^{-1} \bmod p-1 \text{ und} \\ x &:= -yij^{-1} \bmod p-1 \end{aligned}$$

ist.

a) Berechnen Sie eine nichtselektive Fälschung (x, y, z) für den Verifikationsschlüssel $k = (b, g, p)$ mit $p = 467$, $g = 2$ und $b = 132$. (Wählen Sie $i = 99$ und $j = 179$.)

b) Ähnlich wie oben lässt sich auch eine nichtselektive Fälschung (x', y', z') bei bekannter Signatur (x, y, z) vornehmen, indem für beliebige Paramater h, i, j mit $0 \leq h, i, j \leq p-2$ und $ggt(hy - jz, p-1) = 1$

$$\begin{aligned} y' &:= y^h g^i b^j \bmod p, \\ z' &:= zy'(hy - jz)^{-1} \bmod p-1 \text{ und} \\ x' &:= y'(hx + iz)(hy - jz)^{-1} \bmod p-1 \end{aligned}$$

gewählt wird. Zeigen Sie, dass die Signatur (x', y', z') als echt anerkannt wird.

c) Das Dokument $x = 100$ hat unter ElGamal (mit $p = 461$, $g = 2$ und $b = 132$) die Unterschrift $(y, z) = (29, 51)$ erhalten. Berechnen Sie hieraus ein signiertes Dokument, das Oskar bei Verwendung der Werte $h = 102$, $i = 45$ und $j = 293$ erzeugen kann. Überprüfen Sie, ob tatsächlich die Verifikationsbedingung erfüllt ist.

Aufgabe 4

Sei p prim, g ein Erzeuger von $\mathbb{Z}_p^*$ und $i \in \{0, \ldots, p-1\}$ mit $ggT(i, p-1) = d$. Wieviele Elemente hat die von g^i erzeugte Untergruppe

$$\{(g^i)^x \bmod p \mid x = 0, \ldots, p-1\}?$$

Aufgabe 5

Betrachten Sie die folgende Variante des ElGamal-Signaturverfahrens. Die Schlüssel werden ähnlich wie beim ElGamal-Signaturverfahren generiert: p ist prim, g ist ein Erzeuger von $\mathbb{Z}_p^*$, a ist der geheime Exponent und $b = g^a \bmod p$. Allerdings wird a jetzt aus $\mathbb{Z}_{p-1}^*$ (anstelle von $\mathbb{Z}_{p-1}$) gewählt. Ein Dokument $x \in \mathbb{Z}_p$ wird mit $sig(x, r) = (y, z)$ unterschrieben, wobei gilt:

$$y = g^r \bmod p \text{ und } z = (x - ry)a^{-1} \bmod (p-1).$$

Dieses Verfahren unterscheidet sich also auch in der Berechnung von z.

a) Beschreiben Sie, wie sich die Unterschrift (y, z) eines Dokuments x bei Kenntnis des öffentlichen Schlüssels $k' = (g, b, p)$ verifizieren lässt.

b) Welchen Vorteil bei der Berechnung der Signatur besitzt diese Variante gegenüber dem ursprünglichen Verfahren.