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

SS 2001

Übungen zur Kryptologie II

9. Übung

Aufgabe 1 (2 Punkte)

a) Implementieren Sie den Algorithmus zur Berechnung der Mengen A_x aus der Vorlesung.

b) Beschreiben Sie die Funktion $x \mapsto A_x$ mathematisch.

c) Beweisen Sie, daß der Algorithmus korrekt ist, also tatsächlich diese Funktion berechnet.

Aufgabe 2 (2 Punkte)

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

Aufgabe 3

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 $\mathbf{Z}_p^*$, a ist der geheime Exponent und $b = g^a \bmod p$. Allerdings wird a jetzt aus $\mathbf{Z}_{p-1}^*$ (anstelle von $\mathbf{Z}_{p-1}$) gewählt. Ein Dokument $x \in \mathbf{Z}_p$ 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.

c) Vergleichen Sie (kurz) die Sicherheit der beiden Verfahren.