ATK4 - Computer- und Mediensicherheit
FHS Hagenberg
5. Übungsblatt für den 8. April 2003
(1 Seite)

(1) Sie erhalten zwei ElGamal-Signaturen $(4269503, 662686)$ und $(4269503, 4107305)$ von zwei unterschiedlichen Nachrichten m_1 und m_2 vom gleichen Sender. Der public key des Senders ist $(p, g, A) = (6238469, 2431, 4696879)$. Die beiden Nachrichten m_1 und m_2 sind ebenfalls bekannt, somit können Sie ihre Hashwerte $h(m_1) = 1875260$ und $h(m_2) = 1973765$ berechnen. Berechnen Sie den private key des Senders.

(2) Wir definieren die Kompressionsfunktion

$$g: \{0,1\}^{16} \to \{0,1\}^8$$
$$(d_1, \ldots, d_{16}) \mapsto (d_1 \oplus d_9, d_2 \oplus d_{10}, \ldots, d_8 \oplus d_{16}),$$

wobei $\oplus$ folgendermaßen definiert ist:

$$x \oplus y = \begin{cases} 1 & \text{falls } x = y \\ 0 & \text{sonst.} \end{cases}$$

(a) Konstruieren Sie aus der angegebenen Kompressionsfunktion eine Hashfunktion und berechnen Sie den Hashwert der Nachricht "1001 1001 1010 1111 1001".

(b) Berechnen Sie die ElGamal-Signatur (r, s) der Nachricht "1001 1001 1010 1111 1001" für den private key $(p, g, a) = (2969, 3, 29)$, sowie $k = 2103$.

(c) Bestimmen Sie den passenden public key und überprüfen Sie die Signatur.

(3) Sie sind der Empfänger der signierten Nachricht aus Beispiel 2. Fälschen Sie die Signatur des Senders dieser Nachricht für die Nachricht m mit dem Hashwert $h(m) = 111$, so dass der Signatur vertraut wird, wenn man $1 \leq r \leq p - 1$ nicht testet. Überprüfen Sie anschließend die Signatur. *Achtung: Sie dürfen nur den public-key sowie die Nachricht samt Signatur aus Beispiel 2 verwenden, nicht aber die geheimen Parameter a und k.*

(4) Finden Sie für die Hashfunktion aus Beispiel 2 eine Nachricht mit dem Hashwert 158.