ATK4 - Computer- und Mediensicherheit
FHS Hagenberg
7. Übungsblatt für den 25. April 2002
(1 Seite)

1. Sie erhalten zwei ElGamal-Signaturen $(1362784, 6121164)$ und $(1362784, 2042335)$ von zwei unterschiedlichen Nachrichten m_1 und m_2 vom gleichen Sender. Die Parameter $p = 6238469$ und $g = 2431$ sind (als Teil des public-key) bekannt. Die beiden Nachrichten m_1 und m_2 sind ebenfalls bekannt, somit auch ihre Hashwerte $h(m_1) = 1875260$ und $h(m_2) = 1973765$. Berechnen Sie, wenn möglich, die geheimen Parameter a und k.
2. Berechnen Sie die ElGamal-Signatur (r, s) der Nachricht "1001 1001 1011 1111 1001 0001 1101 0010 0000 1000". Benutzen Sie als Hashfunktion die Hashfunktion aus dem zweiten Beispiel des sechsten Übungsblattes (die Kompressionsfunktion soll 2×9 Bits zu 11 Bits komprimieren). Als Parameter (für die Signatur, nicht für die Hashfunktion) verwenden Sie $p = 2969$, $g = 3$ und $a = 29$, sowie $k = 2103$. Überprüfen Sie anschliessend die Signatur. (Berechnen Sie zuerst den public-key (p, g, A).)
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 $h(m) = 317$, sodass 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. *Was für's Leben:* Lesen Sie im Handbook of Applied Cryptography im Kapitel 11 den Abschnitt über ISO/IEC 9796 und fassen Sie die drei Seiten möglichst kurz und in deutscher Sprache zusammen.