Kryptographie *WS 2012/13*
Barbara Baumeister

9. Übungsblatt

Abgabe: Donnerstag, 13.12.2012

Aufgabe 1 Wie kann Oskar die Zufallszahl k bei der ElGamal-Signatur finden, wenn Alice zwei verschiedene Nachrichten mit demselben k signiert?

Aufgabe 2 Seien $x \neq x'$ binäre Folgen endlicher Länge und seien $x_1 \dots x_t$ bzw. $x'_1 \dots x'_{t'}$ die zugehörigen Bitfolgen mittels derer nach der Konstruktion aus der Vorlesung die Hash-Werte von x und x' bestimmt werden. Zeige: Ist $t \leq t'$, so existiert ein $0 \leq i < t$ mit $x_{t-i} \neq x'_{t'-i}$.

Aufgabe 3 Sei $p = 223$ und $\alpha = 3$. Der geheime Schlüssel von Alice ist $a = 12$. Der Hashwert einer Nachricht x ist $h(x) = 11$. Berechnen Sie die Elgamal-Signatur mit $k = 15$ und verifizieren Sie diese.

Aufgabe 4 Zeigen Sie, dass die drei Nullstellen von $x^3+ax+b \in K[x]$ genau dann paarweise verschieden sind, wenn $4a^3 + 27b^2 \neq 0$ ist.