Kryptographie *WS 2015/16*
Barbara Baumeister
Tutoren: Apolonia Gottwald, Soeren Senkovic

13. Übungsblatt

Abgabe: Donnerstag, 4. Februar 2016

Aufgabe 1 Bestimmen Sie die RSA-Signatur der Nachricht 11110, wobei $n = 28829$ und e der kleinstmögliche öffentliche Schlüssel ist, ohne eine Hashfunktion zu benutzen.

Aufgabe 2 Es sei $p = 2237$ und $\alpha = 2$. Der geheime Schlüssel von Alice sei $a = 1234$. Der Hashwert der Nachricht x sei $h(x) = 111$. Welche ElGamal-Signatur berechnet Alice, wenn sie $k = 2323$ gewählt hat? Verifizieren Sie die Signatur.

Aufgabe 3 Alice besitze den öffentlichen Schlüssel $(p, \alpha, \beta) = (107, 2, 80)$. Als Verifikation für eine ElGamal-Signatur gibt sie

$$v(x, u_1, u_2) = \text{ wahr genau dann, wenn } 80^{u_1} u_1^{u_2} \equiv 2^x \bmod 107$$

bekannt. Alice signiert die Nachricht x mit $(9, 93)$. Welche der folgenden Nachrichten $x = 10, x = 83, x = 17$ sind nicht von Alice?

Aufgabe 4 Alice benutzt zum Signieren keine Hashfunktionen. Wie kann Oskar die Zufallszahl k bei der ElGamal-Signatur finden, wenn Alice zwei verschiedene Nachrichten mit demselben k signiert?