Prof. J. Rothe Düsseldorf, 10.11.2009

Übung zur Vorlesung
Kryptologie 2

Blatt 5, Abgabe: 19.11.2009 bis 15:00 Uhr

Aufgabe 1 (10 Punkte): Bestimmen Sie:

(a) das kleinste primitive Element in $\mathbb{Z}_{37}^*$,

(b) alle quadratischen Reste modulo 37,

(c) alle einstelligen primitiven Elemente in $\mathbb{Z}_{101}^*$,

(d) das *least significant bit* von $\log_2 23 \mod 101$ und

(e) das *least significant bit* von $\log_8 98 \mod 101$.

Aufgabe 2 (10 Punkte): Betrachten Sie den in der Vorlesung beschriebenen Known-Message-Angriff auf das ElGamal-Protokoll für digitale Signaturen. Zeigen Sie, dass die in der Vorlesung für diesen Angriff definierten Werte σ, ϱ und m tatsächlich die Verifikationsbedingung

$$\gamma^m \equiv \beta^\sigma \cdot \sigma^\varrho \mod p$$

erfüllen.
Hinweis: $\gamma^a \equiv \gamma^b \mod p \Longleftrightarrow a \equiv b \mod (p-1)$.

Aufgabe 3 (10 Punkte): Sei p eine Primzahl mit $p \equiv 1 \mod 4$. Zeigen Sie, dass $p - \gamma$ ein primitives Element in $\mathbb{Z}_p^*$ ist, wenn γ ein primitives Element in $\mathbb{Z}_p^*$ ist.

Aufgabe 4 (freiwillig): Führen Sie die in Aufgabe 2 angestellten Rechnungen konkret mit Werten Ihrer Wahl durch.

Aufgabe 5 (freiwillig): Betrachten Sie das ElGamal-Protokoll für digitale Signaturen mit $p = 1367$, $\gamma = 2$ und $\beta = 400$. Angenommen, Erich wählt $x = 67$ und $y = 99$ für einen Key-Only-Angriff. Welche Nachricht m kann Erich dann signieren?