

**Präsenzübungen zur Vorlesung**

**Kryptanalyse**

**WS 2010/2011**

Blatt 9 / 08. Dezember 2010

**AUFGABE 1:**

Sei  $p$  prim und  $QR_p$  die Menge aller quadratischen Reste in  $\mathbb{Z}_p^*$ .

- (a) Zeigen Sie, dass  $(QR_p, \cdot)$  eine Gruppe bildet. Warum ist  $(QR_p, +, \cdot)$  kein Körper?
- (b) Zeigen Sie, dass das Produkt eines quadratischen Restes und eines quadratischen Nichtrestes stets ein quadratischer Nichtrest ist. Können Sie eine ähnliche Aussage über das Produkt zweier quadratischer Nichtreste treffen?

**AUFGABE 2:**

Bestimmen Sie mit Hilfe des POHLIG-HELLMAN Algorithmus den diskreten Logarithmus von 18 zur Basis 2 in der multiplikativen Gruppe  $\mathbb{Z}_{29}^*$ . Notieren Sie Ihre Zwischenschritte.

**AUFGABE 3:**

Sie werfen mit ihrem Freund Münzen. Wenn Sie das Ergebnis richtig vorhersagen, dürfen Sie die Münze behalten, andernfalls müssen Sie ihrem Freund den Einsatz auszahlen. Die Wahrscheinlichkeit, dass eine Münze auf der Kante landet sei  $\frac{1}{100}$ . Ist dies ein faires Spiel? Sie spielen das Spiel 20.000 mal. Wie hoch ist die Wahrscheinlichkeit, dass Sie ohne Verlust herausgehen höchstens? Benutzen Sie dazu die Hoeffding Schranke.