Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Stefan Hoffmann

Hausübungen zur Vorlesung

Diskrete Mathematik 2
Einführung in die theoretische Informatik

Sommersemester 2014

Blatt 4 / 3./4. Juni 2014

Abgabe: 3. Juni 2014, 09:15 Uhr (vor der Vorlesung), Kasten NA 02

AUFGABE 1 (5 Punkte)**:**

Sei p prim und g ein Generator von $\mathbb{Z}_p^* := \{1, 2, \ldots, p-1\}$. Wir definieren die Sprachen

$$\text{DDH} := \{(g^\alpha, g^\beta, g^y) \mid g^y = g^{\alpha\beta} \bmod p\} \subseteq (\mathbb{Z}_p^*)^3$$

$$\textsc{ElGamal} := \{(g^a, g^r, m, x) \mid x = m \cdot g^{ar} \bmod p\} \subseteq (\mathbb{Z}_p^*)^4$$

Sei $p = 101$ und $g = 2$. Angenommen ein DDH-Orakel liefert uns:

$$(95, 75, 36),\ (27, 75, 98) \in \text{DDH},\ (40, 68, 56) \notin \text{DDH}$$

Entscheiden Sie für folgende Tupel, ob sie in der Sprache ElGamal liegen:

$$(95, 75, 36, 13),\ (95, 75, 41, 62),\ (27, 75, 97, 12),\ (27, 75, 55, 38),\ (40, 68, 17, 43)$$

Hinweis: Benutzen Sie die Reduktionsabbildung $\textsc{ElGamal} \leq_p \text{DDH}$ aus der Vorlesung.

AUFGABE 2 (5 Punkte)**:**

Sei p prim und g, g_1, g_2 Generatoren von $\mathbb{Z}_p^*$. Wir definieren die folgenden Sprachen:

$$\text{LIN} := \{(g, g_1, g_2, g_1^a, g_2^b, g^{a+b})\} \subseteq (\mathbb{Z}_p^*)^6$$

$$\textsc{Lineare Verschlüsselung} := \{(g, g_1, g_2, g_1^a, g_2^b, m, m \cdot g^{a+b})\} \subseteq (\mathbb{Z}_p^*)^7$$

Zeigen Sie $\text{LIN} \leq_p$ Lineare Verschlüsselung und Lineare Verschlüsselung $\leq_p$ LIN.

AUFGABE 3 (5 Punkte)**:**

Sei $p = 59$. Berechnen Sie das Legendre-Symbol $\left(\frac{a}{p}\right)$ für die angegebenen $a \in \mathbb{N}$. Sie sollten die Rechenregeln auf Folie 98 und das Quadratische Reziprozitätsgesetz (Folie 99) verwenden. Entscheiden Sie jeweils, ob a ein quadratischer Rest modulo p ist. Führen Sie alle Berechnungen ohne Taschenrechner durch und geben Sie alle Zwischenschritte an.

(a) $a = 21$

(b) $a = 12$

(c) $a = 53$

(d) $a = 52$

AUFGABE 4 (5 Punkte)**:**

Sei $n = 57$. Entscheiden Sie für folgende $a \in \mathbb{N}$ ob a ein quadratischer Rest modulo n ist. Falls vorhanden, geben Sie alle Lösungen der Gleichung $b^2 = a \bmod n$ an (Quadratwurzeln von a).

Berechnen Sie eine Liste aller Quadrate modulo jedem Teiler von n, um die Quadratwurzel zu berechnen. Setzen Sie diese dann mit dem Chinesischen Restsatz zu einer Wurzel modulo n zusammen.

Bestimmen Sie zudem jeweils das Jacobi-Symbol $\left(\frac{a}{n}\right)$ und geben Sie alle Zwischenschritte an.

(a) $a = 38$

(b) $a = 28$

(c) $a = 55$

(d) $a = 41$